Integración de la tecnología Blockchain con procesos de gestión de registros médicos en la atención y prestación de servicios de salud.

Andrés Favian Cáceres Ramírez

Zaira Sharick Flórez Guadrón

Trabajo de grado presentado para optar al título de Ingeniero Industrial

Director

Néstor Fabian Santos Nova

Máster en Administración y MBA

Universidad Industrial de Santander

Facultad de Ingenierías Físico - mecánicas

Escuela de Estudios Industriales y Empresariales

Bucaramanga

2023

Dedicatoria

Dedicado, en primer lugar, a Dios, quien me ha brindado resiliencia y fortaleza mental. Estoy profundamente agradecido por la sabiduría y la paciencia que me ha impartido, por guiarme por el buen camino y por iluminar mi decisión de elegir la ingeniería industrial como parte de mi proyecto de vida. Asimismo, dedico este trabajo a mi familia: a María del Carmen, mi madre, la mujer que ha cuidado de mí toda la vida, inculcándome ser una persona de bien, con grandes sueños y metas. Sigo esforzándome día a día para hacerlas realidad. A mi padre, Yovanny, por su apoyo constante y por estar siempre pendiente de mí en muchos momentos importantes. A mi hermano, Jhonny Manuel, con quien he compartido y consultado en numerosas etapas de la vida. Extiendo mi agradecimiento a mis tíos Bartolo, Chencha, José, Marcos, Marellys, Ardellys; a mis primos Cristian David, Lesly Marcela, Mateo, Samuel, Luciana, María Luisa, Aradna; y a mis abuelos María Elda y Manuel. Todos ellos me han apoyado en este camino para culminar esta importante etapa. A mi pareja, cuyo apoyo, amor y responsabilidad han sido ejemplares y fundamentales para finalizar esta etapa. Finalmente, quiero agradecer a todos mis demás familiares, amigos, compañeros y profesores que me han apoyado y ayudado a cumplir con esta fase de mi proyecto de vida.

Andrés Favian Cáceres Ramírez

Dedicado a Dios, quien me ha otorgado la perseverancia y la sabiduría necesaria, la salud y la compañía de mis seres queridos. A mis abuelos, mis pilares más sólidos, que con su sabiduría y cariño han sido una fuente inagotable de inspiración y fortaleza. A mis padres, cuyo amor incondicional y constante apoyo han sido la brújula que me ha guiado en mi camino y mis metas. A mi tío, fuente de inspiración y ejemplo de perseverancia, quien me ha enseñado a visualizar y alcanzar sueños. A mis hermanos, cuyo afecto y compañía han hecho más llevadero cada desafío. A mi pareja, cuyo apoyo y cariño inquebrantable han sido pilares fundamentales para culminar esta etapa, eres esa persona que sueña en grande, nunca cambies. A mis amigos docentes y director, quienes con su presencia y consejos han contribuido notablemente en mi crecimiento personal y emocional. A todos ellos,

mi gratitud eterna.

Zaira Sharick Flórez Gualdron

Agradecimientos

Agradezco a Dios por la resiliencia y sabiduría que han hecho de este camino una constante mejora. A mis padres y a mi hermano Jhonny, quienes sin duda han marcado este trayecto con recuerdos significativos que me han convertido en una mejor persona. A mis abuelos, tíos y primos, les estoy agradecido por ser una maravillosa familia para mí y por impulsarme a ser una buena persona, lo cual sé que me ayudará a convertirme en un gran profesional. Por ello, gracias. A mi pareja, le agradezco por sus consejos, apoyo y amor, bajo la única condición de que yo también la ame, la respete y sea una buena persona. Le estoy enormemente agradecido por permitirme soñar sin cortar mis alas y por estar a mi lado en cada proceso y etapa. A mis amigos del barrio, les agradezco, pues sin ellos mi adolescencia no habría sido la misma. Gracias por apoyarme siempre, por entender mis gustos y metas, y por desearme lo mejor. Por esos momentos felices, les doy las gracias. Agradezco a todos mis amigos y compañeros de la universidad que en algún momento me brindaron su apoyo. En especial a Libardo, Christian, Mateo, Daniel y Brayan; amigos del barrio como Brandon, Edgar, Francon y Andrés, quienes también fueron un apoyo en la universidad; a mi hermano, que fue mi sostén en muchos momentos académicos; a mis docentes y al director de mi proyecto de grado. Finalmente, extiendo mis agradecimientos a mis compañeros y amigos de ACEII, que sin duda marcaron una etapa importante de mi vida universitaria. A todos ustedes, les agradezco enormemente. Esto también es para ustedes.

Andrés Favian Cáceres Ramírez

Gracias a Dios, por ayudarme a enfrentar todos los desafíos que se han presentado en mi vida, por mantenerme fuerte y rodeada de personas con un gran corazón. Agradezco a mis padres y abuelos por permitirme siempre elegir qué camino tomar, por apoyarme incondicionalmente, incluso cuando no me fue bien en mis estudios. Este proyecto hace parte de la obtención del título universitario, más que mío, es de ustedes… porque sin ustedes no habría llegado aquí. Agradezco a mis hermanos, quienes compartieron conmigo risas y lágrimas. A mi pareja, por su paciencia, comprensión y amor incondicional, por estar a mi lado durante los momentos difíciles y por celebrar conmigo cada logro alcanzado. También quiero expresar mi profundo agradecimiento a mis amigos, quienes han sido mis confidentes y mis compañeros. Sus palabras de aliento y su compañía han sido esenciales. Y a mis profesores y mentores, por su invaluable orientación académica, por desafiarme a superar mis límites y por brindarme las herramientas necesarias para alcanzar mis metas.

Zaira Sharick Flórez Gualdron

Tabla de Contenido

Pág.

Introducción 13
1. Generalidades del proyecto 14
1.1. Objetivos 15
1.1.1. Objetivo General 15
1.1.2. Objetivos Específicos 15
1.2. Justificación 16
2. Marco de Referencias 17
2.1. Marco de antecedentes 17
2.2. Marco Teórico 22
2.2.1. Tecnología Blockchain 22
2.2.1.1. Criptografía 24
2.2.1.2. Clave pública y privada 24
2.2.1.3 Contratos Inteligentes (Smart contracts) 25
2.2.2. Gestión de registros médicos 25
2.2.2.1. Registros de salud electrónicos (EHR) 26
2.2.2.2. Sistemas de información de salud (HIS) 26
2.2.3. Cloud computing 27
3. Metodología 28
3.1. Fase 1: Revisión de la literatura 28
3.1.1. Análisis bibliométrico 28
3.1.1.1. Ecuación de búsqueda 28
3.1.1.2. Selección de documentos 28
3.1.2. Análisis de literatura 28

3.2. Fase 2: Identificación de posibilidades de integración y de mejora 29
3.2.1. Análisis de posibilidades de integración 29
3.2.2. Mejoras potenciales del sistema actual 29
3.2.3. Soluciones propuestas por Blockchain 29
3.2.4. Consideraciones éticas y legales 30
3.3. Fase 3: Plantear la integración del Blockchain con EHR 30
3.4. Fase 4: Análisis de mejoras y cuantificación de beneficios 31
3.5. Fase 5: Realizar artículo de investigación con carácter publicable 31
4. Revisión de literatura 32
4.1. Análisis bibliométrico 32
4.2. Análisis de literatura 37
5. Identificación de Posibilidades de Integración 41
5.1. Análisis de las Posibilidades de Integración 41
5.1.1. Revisión de Sistemas Actuales de EHR en instituciones de salud 41
5.1.2. Limitaciones y desafíos en la gestión de registros médicos. 43
5.1.3. Casos de implementación exitosa de blockchain 44
5.2. Mejoras potenciales en el sistema actual de salud. 46
5.2.1. Áreas de la salud donde la blockchain aborda problemas existentes 46
5.2.2. Evaluación de Beneficios Potenciales 47
5.3. Soluciones Propuestas con Blockchain. 48
5.3.1. Modelos de Integración blockchain en los procesos de EHR 48
5.4. Consideraciones Éticas y Legales 52
6. Planteamiento de Integración y Análisis de Beneficios 53
6.1. Identificación de Requisitos y Casos de Uso 53

6.2. Explicación de Técnicas para la Gestión de Datos en la Integración 62
6.2.1. Análisis de requisitos de Datos 62
6.2.2. Modelado de Datos 65
6.2.3. Criptografía para Seguridad de Datos 68
6.2.4. Estandarización de Datos 72
6.3. Recomendaciones para Implementaciones Futuras 74
6.3.1. Análisis de Tendencias Tecnológicas 74
6.3.2. Benchmarking de las prácticas actuales con las planteadas 76
6.4. Planteamiento de la Integración de Blockchain y Cloud Computing 77
6.4.1. Diagrama de interacción 78
6.4.2. Modelado de la Integración de Blockchain y Cloud Computing 88
6.5. Análisis de la Gestión del Riesgo 95
6.5.1. Identificación de riesgos potenciales y Evaluación de impacto 96
6.6. Análisis de Mejoras y Cuantificación de Beneficios 98
6.6.1. Identificación de métricas claves 98
7. Conclusiones 105
8. Recomendaciones 108
Referencias Bibliográficas 110

Lista de Figuras

Figura 1. Documentos por tipo 33

Figura 2. Documentos por año de publicación 34

Figura 3. Documentos por país de publicación..... 35

Figura 4. Términos claves por año..... 36

Figura 5. Correlación de términos claves 37

Figura 6. Marco de intercambio de registros médicos BCIF-EHR..... 51

Figura 7. Representación gráfica de interacciones. 82

Figura 8. Arquitectura del sistema. 91

Lista de tablas

Tabla 1. Cumplimiento de objetivos 14

Tabla 2. Benchmarking 77

Lista de Apéndices

Apéndices adjuntos

Apéndice A. Artículo publicable

Resumen/Definición del proyecto

Título: Integración de la tecnología Blockchain con procesos de gestión de registros médicos en la atención y prestación de servicios de salud.*

Autor(es): Andrés Favian Cáceres Ramírez, Zaira Sharick Florez Gualdron**

Palabras clave: Salud, Registros médicos, Blockchain, automatización y Cloud Computing, máquina virtual, interoperabilidad.

Descripción:

La finalidad principal de este proyecto es integrar la tecnología blockchain con los procesos de gestión de registros médicos en entidades prestadoras de servicios de salud. Se abordan problemáticas actuales en la gestión de registros médicos electrónicos tanto en Colombia como a nivel mundial. Entre estos problemas se encuentran la ineficiencia en la gestión y en la seguridad de los registros médicos, así como la falta de interoperabilidad entre sistemas de información, factores que han conducido a violaciones de datos de salud.

Esta integración busca como solución innovadora mejorar la eficiencia, seguridad y privacidad de la historia clínica electrónica. Por medio de la adopción de blockchain y la computación en la nube, el proyecto crea un entorno seguro y eficiente para el almacenamiento, monitoreo y verificación de la información médica, tratando aspectos críticos como la privacidad de los pacientes y la tolerancia a fallas. Permite a los pacientes poseer sus datos, acceder a ellos y gestionar el consentimiento de su historia clínica electrónica (EHR), mediante un sistema integrado moderno y adaptado a las necesidades de la industria.

---

* Trabajo de Grado

** Facultad de Ingenierías Físico-mecánicas. Escuela de Estudios Industriales y Empresariales. Ingeniería Industrial. Director: Néstor Fabian Santos Noba. Máster en Administración y MBA

Abstract

Title: Integration of Blockchain Technology with Medical Record Management Processes in Healthcare Delivery and Services. *

Author(s): Andrés Favian Cáceres Ramírez, Zaira Sharick Florez Gualdron [1]

Keywords: Health, Medical Records, Blockchain, Automation, Cloud Computing, Virtual Machine, Interoperability.

Description:

This project's main purpose is to integrate blockchain technology with medical record management processes in healthcare service providers. It addresses current issues in the management of electronic medical records both in Colombia and globally. Among these issues are inefficiency in management and security of medical records, and the lack of interoperability between information systems, factors that have led to health data breaches.

This integration seeks to innovatively improve the efficiency, security, and privacy of electronic health records (EHR). Through the adoption of blockchain and cloud computing, the project establishes a secure and efficient environment for the storage, monitoring, and verification of medical information, addressing critical aspects such as patient privacy and fault tolerance. It allows patients to own their data, access it, and manage consent for their electronic health record (EHR), through a modern, integrated system tailored to the industry's needs.

---

* Bachelor Thesis

[1] Faculty of Physical-mechanical Engineering. School of Industrial and Business Studies. Industrial Engineering. Director: Néstor Fabian Santos Nova. Master in Administration & MBA

Introducción

El presente trabajo de investigación tiene como objetivo principal analizar la integración de la tecnología Blockchain con los procesos de registros médicos electrónicos, centrándose en instituciones de atención y prestación de servicios en salud. La presente problemática en el sector salud colombiano y la violación de millones datos de salud a nivel mundial, caracterizados por la falta de eficiencia en la gestión de registros médicos y seguridad de estos, la ausencia de interoperabilidad entre sistemas de información motiva la necesidad de buscar soluciones innovadoras para superar estos desafíos.

La justificación de esta investigación se fundamenta en los problemas existentes en el sector salud, incluyendo la escasez de recursos y personal capacitado, lo que afecta la eficacia y eficiencia del sistema de atención médica. La tecnología Blockchain, reconocida por su transparencia y red distribuida segura, surge como una alternativa que podría mejorar la gestión de registros médicos electrónicos, ofreciendo una solución innovadora a los problemas actuales.

La relevancia de este proyecto radica en su contribución al avance y modernización de los registros médicos electrónicos, permitiendo a los usuarios ser dueños y acceder a su propia información para así mejorar la calidad de la atención médica. Con la combinación de Blockchain y tecnologías como Cloud Computing, se busca crear un entorno seguro y eficiente para el almacenamiento, monitoreo y verificación de información, abordando aspectos críticos como la privacidad y la tolerancia a fallas. Este trabajo de investigación busca generar conocimientos que impulsen la adopción de tecnologías innovadoras en la salud y la gestión de sistemas de información, mejorando la gestión de registros médicos y beneficiando a pacientes y profesionales de la salud.

1. Generalidades del proyecto

Tabla de cumplimiento de objetivos

Objetivo específico	Cumplimiento
Realizar revisión bibliográfica de la infraestructura de Blockchain y procesos de automatización e historia clínica en el sector salud.	Capítulo 4
Identificar las posibilidades de integración y de mejora del sistema actual de salud y posibles soluciones con Blockchain.	Capítulo 5
Plantear la integración del Blockchain en el sector salud en los procesos de registros médicos en atención a los pacientes.	Capítulo 6 Numeral 6.1, 6.2, 6.3, 6.4 y 6.5
Realizar un análisis de las mejoras y cuantificación de beneficios para las personas y el sistema de salud. (en eficiencia logística en registros, tiempos de atención y servicio al cliente)	Capítulo 6 Numeral 6.6
Realizar un artículo con carácter publicable que resuma la situación actual, brechas, mejoras e impacto en el sistema de salud por medio de la tecnología Blockchain en los procesos de registros médicos.	Apéndice A

Tabla 1. *Cumplimiento de objetivos*

1.1. Objetivos

1.1.1. Objetivo General

Analizar la integración de la tecnología Blockchain con la automatización de los procesos de registros médicos enfocado en instituciones de atención y prestación de servicios en salud, planteando soluciones por medio de estas tecnologías.

1.1.2. Objetivos Específicos

- Realizar revisión bibliográfica de la infraestructura de Blockchain y procesos de automatización e historia clínica en el sector salud.
- Identificar las posibilidades de integración y de mejora del sistema actual de salud y posibles soluciones con Blockchain.
- Plantear la integración del Blockchain en el sector salud en los procesos de registros médicos en atención a los pacientes.
- Realizar un análisis de las mejoras y cuantificación de beneficios para las personas y el sistema de salud (en eficiencia logística en registros, tiempos de atención y servicio al cliente).
- Realizar un artículo con carácter publicable que resuma la situación actual, brechas, mejoras e impacto en el sistema de salud por medio de la tecnología Blockchain en los procesos de registros médicos.

1.2. Justificación

El sector salud de Colombia tiene diferentes problemas, como la falta de eficiencia en tareas como registros médicos y la falta de interoperabilidad entre los sistemas de información, lo que causa fallas médicas, impuntualidad en la atención a pacientes y sobrecostos. Si a esto se le suma la escasez de recursos y trabajadores capacitados, se convierte en un desafío aún mayor para Colombia superar estas brechas. Por ende, encontrar soluciones e innovadoras para mejorar la eficiencia y eficacia del sector salud colombiano.

El Blockchain es una tecnología que está en auge en distintas industrias, sectores económicos y sociales debido a su capacidad de transparencia y de ser una red distribuida descentralizada de forma segura (Andrew et al., 2023). Al combinar la tecnología Blockchain al Cloud Computing permite mejorar el rendimiento de almacenamiento seguro con una máquina virtual que permita acceder a diferentes inquilinos que trabajen entre sí verificando la confianza de los datos en procesos de almacenamiento, monitoreo y verificación de la información suministrada en cada bloque (Wei et al., 2020). Teniendo en cuenta sistemas de gestión de información de Blockchain médica con tolerancia a fallas bizantinas ya que la seguridad en datos médicos es de gran importancia al igual que su privacidad (Qu, 2022).

En este proyecto de investigación busca proponer soluciones concretas para mejorar los procesos de registros médicos en atención a los pacientes con el fin de mejorar la eficiencia. Este trabajo de grado tiene como propósito aportar al avance y modernización del sector salud colombiano, en pro de la adopción de tecnologías innovadoras siendo esto primordial para garantizar una atención médica de calidad y una buena gestión de los registros médicos.

2. Marco de Referencias

2.1. Marco de antecedentes

La tecnología Blockchain, inicialmente reconocida como la base de las criptomonedas, ha trascendido su papel original y se ha convertido en un paradigma revolucionario con diversas aplicaciones. Este trabajo explorará proyectos e investigaciones que destacan no solo su impacto en la industria en general, sino también su relevancia en los registros médicos electrónicos del sector salud.

La propuesta de Sumathi et al. (2022) aborda el almacenamiento en Blockchain, diferenciando entre almacenamiento en frío (más seguro para datos confidenciales) y en caliente (más expuesto y sujeto a cambios frecuentes). Utilizan dispositivos IoT para recopilar datos de salud, gestionando la seguridad mediante control de acceso y monitorización de datos IoT con Blockchain. Después de la recopilación, los datos se limpian y clasifican con Decision Tree y Fuzzy Rule. Se aplica cifrado basado en atributos a datos confidenciales, creando bloques fuera de la cadena con contratos inteligentes en una red permisiva. Esto reduce el consumo de almacenamiento, mejora el tiempo de acceso y proporciona un control de acceso eficiente en la red Blockchain, permitiendo una gestión más efectiva de indicadores como rendimiento, latencia y capacidad para adaptarse al crecimiento de usuarios y tráfico de red.

Egala et al., en 2021 presentan una arquitectura basada en Blockchain que ofrece un historial médico descentralizado y automatización de servicios mediante Smart Contracts, sin comprometer la seguridad y privacidad del sistema. Incorpora algoritmos de verificación de dispositivos y registros de usuarios de forma anónima para reforzar la seguridad. La herramienta de control de acceso selectivo basado en anillos descentralizado se sometió a pruebas, demostrando que el H-CPS basado en esta cadena fortificada requiere un almacenamiento insignificante y tiene

un tiempo de respuesta rápido en comparación con los H-CPS centralizados tradicionales. Esto proporciona control de acceso automatizado con seguridad y privacidad, cumpliendo con los requisitos de los sistemas de atención médica inteligentes descentralizados.

En respuesta al COVID-19, Bera et al, en 2023 proponen la supervisión remota mediante una red privada Blockchain, respaldada por Fog Computing, análisis de Big Data con inteligencia artificial (AI) y el uso del Internet de las Cosas Médicas (IoMT) para rastrear los datos de pacientes con COVID-19. Se concluye que la combinación de la computación en la niebla y Blockchain ofrece un sistema más seguro en este contexto.

La aplicación de la tecnología Blockchain en el ámbito de la salud promete mejorar la interoperabilidad de datos y fortalecer la seguridad para lograr resultados clínicos óptimos y beneficios operativos y financieros. El enfoque propuesto utiliza un Blockchain privado y autorizado para establecer un ecosistema distribuido de EHR, abordando los desafíos de datos no estructurados en instituciones de atención médica. Con base en la teoría del procesamiento de la información (IPT), el sistema propuesto facilita el almacenamiento y el intercambio de datos entre proveedores de asistencia médica, con posibles aplicaciones en diversos servicios e instituciones del sector (Cerchione et al., 2022).

N. Zhang et al. (2018)presenta "PrivacyGuard" un marco innovador que combina Blockchain y entornos de ejecución confiables, otorgando a los propietarios de datos un control total sobre su información personal. A través de contratos inteligentes en Blockchain y la tecnología de enclave seguro (TEE), los propietarios establecen condiciones de acceso. La arquitectura incluye Blockchain, iDataAgent y almacenamiento cifrado. Esta combinación aborda la protección de la confidencialidad y la verificación del uso previsto de los datos.

Se combina la encriptación basada en atributos (ABE) con la tecnología Blockchain para sistemas de salud electrónica (e-Health), permitiendo búsquedas de palabras clave en datos encriptados y aplicando políticas de acceso granulares. Se resalta la relevancia de la tecnología Blockchain para mejorar la seguridad y privacidad en los sistemas de salud electrónica, enfocándose en proteger la confidencialidad de los datos médicos y asegurar un acceso controlado a la información sensible (Xiang & Zhao, 2022).

En el artículo se presenta EdgeMediChain, un proyecto que combina blockchain y Edge Computing para el intercambio seguro de datos de salud. El objetivo es mejorar el rendimiento y la seguridad del sistema de intercambio de información de salud. Las evaluaciones en un entorno de prueba basado en Ethereum mostraron una reducción del tiempo de ejecución del 84.75% para 2000 transacciones concurrentes, destacando un rendimiento superior a las cadenas de bloques tradicionales y un almacenamiento de registros escalable con crecimiento lineal. El framework demostró capacidad para proporcionar escalabilidad, seguridad y privacidad en el ámbito de la atención médica, facilitando el intercambio de datos mediante contratos inteligentes y control de acceso basado en roles. En conclusión, EdgeMediChain se muestra como una solución efectiva y segura para el intercambio de datos de salud (Akkaoui et al., 2020).

El proyecto se centra en garantizar un intercambio seguro de registros electrónicos de salud (EHR) en el ámbito médico mediante una red de Blockchain centrada en la confianza y la privacidad del paciente. Enfrentando desafíos como la vulnerabilidad a ataques cibernéticos y la alteración de registros, se propone la tecnología de cadena de bloques, específicamente Hyperledger Fabric. Resalta la seguridad y anonimato en el intercambio de datos, la preservación de la privacidad y un sólido control de acceso. Los resultados del proyecto confirman la viabilidad de este enfoque para el intercambio seguro de EHR (Chelladurai & Pandian, 2022).

La arquitectura FogChain, basada en Hyperledger Fabric, brinda un entorno de cadena de bloques seguro y con permisos. Utiliza Fog Computing para procesar datos cerca de dispositivos IoT, evitando puntos únicos de falla. FogChain demuestra la viabilidad del intercambio seguro de registros médicos electrónicos en una red de blockchain confiable, garantizando privacidad y autenticidad. Comparado con infraestructuras de nube basadas en blockchain, FogChain logra un 62,6% más rápido tiempo de respuesta, ofreciendo una solución integral que mejora la seguridad y disponibilidad en tiempo real de la información médica frente a enfoques convencionales en la nube (Mayer et al., 2021).

Ancile utiliza contratos inteligentes en Ethereum para control de acceso y ofuscación de datos en registros médicos electrónicos (EHR). Almacena hashes de referencias en lugar de datos y envía consultas de forma privada, mejorando la escalabilidad. La tecnología blockchain en salud garantiza a los pacientes control sobre sus EHR, facilita transferencias seguras y reduce el riesgo de acceso no autorizado a información de salud protegida bajo HIPAA. Además, permite el intercambio seguro de registros médicos, protegiendo la privacidad de la información del paciente (Dagher et al., 2018).

MedBlock, una propuesta de Fan et al. (2018), busca la interoperabilidad entre sistemas hospitalarios mediante criptografía asimétrica y protocolos de acceso personalizados. Su enfoque garantiza la seguridad y privacidad de la información médica, respaldado por un mecanismo de consenso híbrido eficiente en energía. La función "bread crumbs" facilita la búsqueda en Registros Médicos Electrónicos (EHR), simplificando el acceso a datos cruciales. Esta plataforma ofrece a hospitales y proveedores de atención médica la oportunidad de mejorar la calidad y reducir costos con altos estándares de seguridad .

En 2021, surge appXchain, un sistema que garantiza interoperabilidad entre cadenas mediante el intercambio de documentos EHR mediante aplicaciones descentralizadas. Esta propuesta facilita la comunicación y el intercambio de datos entre distintas arquitecturas blockchain sin alterar la infraestructura central. Nodos verificadores incentivados aseguran la integridad de los datos, y se ilustra la creación de contratos inteligentes en Ethereum para hospitales, detallando roles y requisitos específicos. Esta innovación puede mejorar tanto el intercambio de información como la experiencia del paciente (Madine et al., 2021).

SEMRES consta de tres módulos clave: CEDA (Arquitectura combinada de cifrado y descifrado), DER (Repositorio Descentralizado de Registros Médicos Electrónicos) y una arquitectura blockchain para validar datos. Estos módulos colaboran para brindar un intercambio seguro de registros médicos mediante un sistema de triple seguridad. Ofrece una solución innovadora y prometedora para el intercambio seguro de registros médicos utilizando tecnología blockchain. SEMRES no solo aborda los desafíos de seguridad y privacidad en el intercambio de registros médicos, sino que también se respalda en la sólida estructura de consenso de blockchain para preservar la integridad y autenticidad de los datos (Lee, Y et al., 2022).

Yadav et al. (2023)abordaron la implementación de la tecnología blockchain en la gestión de datos de salud, centrándose en EHR y registros de salud personales (PHR). Destacan la estructura del blockchain, el método de consenso y un sistema de incentivos para proveedores de salud. Utilizaron contratos inteligentes y una aplicación Java para demostrar la viabilidad, mejorando integración, seguridad y privacidad. También consideran la aplicabilidad de IoT para registros inalterables y sistemas de monitoreo de salud inteligente. En resumen, buscan optimizar la gestión de datos de salud mediante la tecnología blockchain.

(Jang et al., 2021) con PDPM emplea la Teoría del Empujón y blockchain para gestionar la privacidad de datos en salud. Incluyen almacenamiento cifrado, clasificación por médicos y filtrado colaborativo que se registra de manera inmutable en la cadena de bloques.

2.2. Marco Teórico

2.2.1. Tecnología Blockchain

Blockchain es un registro inalterable y compartido que simplifica la grabación de transacciones y el seguimiento de activos en redes empresariales. Los activos pueden ser tangibles (casa, coche, dinero en efectivo, tierra) o intangibles (propiedad intelectual, patentes, derechos de autor, marca). En una red blockchain, casi cualquier cosa valiosa puede ser rastreada y transada, disminuyendo riesgos y costos para todas las partes involucradas (*¿Qué Es Blockchain? - IBM*, 2023).

El blockchain funciona e inicia cuando una transacción se registra como un bloque de datos que puede incluir variada información y aspectos específicos de la condición de envío de un producto o del producto en sí. Estos bloques se conectan secuencialmente al anterior y al siguiente, formando una cadena a medida que el activo se traslada o cambia de propietario. La estructura de esta cadena asegura la secuencia y el tiempo exacto de las transacciones y se enlaza de manera segura para prevenir modificaciones indebidas. Así, cada bloque nuevo que se añade valida aún más el anterior, fortaleciendo la cadena completa contra alteraciones. Este mecanismo de encadenamiento no solo impide manipulaciones por parte de actores malintencionados, sino que también establece un registro fidedigno y confiable de las transacciones para todos los participantes de la red involucradas (*¿Qué Es Blockchain? - IBM*, 2023).

Según Tanwar et al. la tecnología blockchain como método de almacenamiento y compartición de datos que es distribuido, confiable e inalterable, lo cual elimina la necesidad de intermediarios o de una autoridad centralizada para verificar las transacciones. Blockchain utiliza diversas técnicas y servicios fundamentales para su aplicación:

- Protocolo de consenso: Permite que ciertos usuarios con derechos de acceso puedan validar y actualizar transacciones en el sistema.
- Criptografía de hash: Utiliza algoritmos de hash, como el SHA256, para añadir transacciones, asegurando que cada una es única y segura.
- Libro mayor inmutable: Todos los registros son permanentes y no pueden ser modificados ni alterados una vez registrados.
- Red P2P distribuida: Las transacciones se difunden a través de una red a todos los usuarios, asegurando que todos tienen la misma versión actualizada de la base de datos.
- Minería: Los mineros contribuyen a la red mediante la resolución de complejos problemas matemáticos para validar bloques, lo cual requiere un alto poder de cómputo y a su vez mantiene la red segura.

Estos componentes hacen que la blockchain sea altamente eficaz en términos de velocidad de procesamiento y seguridad de las transacciones, ofreciendo una plataforma robusta para diversos usos sin la necesidad de un ente central que supervise o controle los datos. (Tanwar et al., 2020)

La robustez de la tecnología blockchain no solo reside en su estructura descentralizada, sino también en su uso intensivo de la criptografía avanzada, que garantiza la seguridad y la

integridad de los datos. Al profundizar en cómo la criptografía sustenta estos sistemas, se puede apreciar su papel indispensable en la protección de la información digital y en la autenticación de transacciones.

2.2.1.1. Criptografía

La disciplina de la criptografía implica salvaguardar datos mediante la implementación de algoritmos cifrados, funciones hash y firmas digitales. Los datos pueden encontrarse en reposo, como archivos almacenados en una unidad de almacenamiento; en tránsito, como comunicaciones electrónicas entre dos o más entidades; en uso, durante la ejecución de operaciones informáticas con la información. (AWS, Amazon)

2.2.1.2. Clave pública y privada

La criptografía de clave pública implica el cifrado o la firma de datos mediante dos claves distintas: la clave pública, accesible para todos, y la clave privada. Solo la clave privada puede descifrar los datos cifrados con la clave pública. Este método, también llamado criptografía asimétrica, se emplea extensamente, especialmente en TLS/SSL, facilitando HTTPS (*¿Cómo Funciona La Criptografía de Clave Pública?*, 2023).

La criptografía, especialmente a través del uso de claves públicas y privadas, establece una base sólida para la seguridad en las tecnologías blockchain. Este método no solo asegura la privacidad de la información, sino que también facilita la verificación de la autenticidad de las transacciones sin intervención externa. Avanzando en la aplicación de blockchain en la gestión de registros electrónicos de salud (EHR), surge el concepto de contratos inteligentes. Estos contratos programables permiten la automatización de procesos y la ejecución de acuerdos predefinidos

dentro de la red de blockchain, lo que promete transformar la manera en que se manejan y se accede a los EHR en entornos sanitarios.

2.2.1.3 Contratos Inteligentes (Smart contracts)

Protocolos computacionales que aseguran la ejecución automática de prestaciones, eliminando intermediarios y garantizando seguridad contra modificaciones o impedimentos en contratos. Aunque prometen revolucionar relaciones industriales y particulares, generan inquietudes en la ciencia del derecho. Aspectos como su validez, naturaleza jurídica, libertad negocial, disciplina normativa, coherencia con el derecho privado, interpretación y revisión judicial son cuestionados y requieren respuestas de la doctrina jurídica (Fuentes Blanco, 2022).

2.2.2. Gestión de registros médicos

Es el proceso de manejo de toda la información relacionada con la salud de los individuos, incluyendo la recolección, almacenamiento, acceso, análisis y protección de los datos. Este proceso puede abarcar una gran variedad de datos, desde registros médicos personales hasta grandes bases de datos poblacionales utilizadas para la investigación y la política de salud pública. Teniendo como propósito mejorar la calidad de la atención médica, facilitar la investigación y el desarrollo de políticas de salud, y optimizar los costos de los servicios de salud a través de un manejo eficiente de la información (Gestión de registros médicos, s.f.).

La gestión efectiva de registros médicos es esencial para mejorar los servicios de salud, asegurando un acceso seguro y ágil a la información del paciente. Los Registros de Salud Electrónicos (EHR) son herramientas vitales que digitalizan datos clínicos importantes, mientras que los Sistemas de Información de Salud (HIS) facilitan la administración y recuperación de estos datos y coordinan las operaciones de los servicios de salud. Conjuntamente, los EHR y los HIS no solo elevan la eficiencia operativa, sino que también fortalecen la calidad del cuidado médico,

permitiendo la incorporación de tecnologías avanzadas como blockchain para proteger la integridad y privacidad de la información médica.

2.2.2.1. Registros de salud electrónicos (EHR)

El Registro Médico Electrónico (EHR) se refiere a un sistema de almacenamiento de datos sobre el estado de salud de una persona en un formato procesable por computadora. Según la norma ISO/TR 20514:2005 de Informática en Salud, este tipo de registro debe ser seguro, accesible para múltiples usuarios autorizados, y mantener un formato estandarizado que sea independiente del sistema de Electronic Medical Records utilizado. Su principal objetivo es apoyar la continuidad del cuidado de manera eficiente y facilitar una atención integral de calidad (Gutiérrez et al., 2020).

Los Registros Médicos Electrónicos (EHR) constituyen un compendio digital de datos de salud de una persona o grupo, registrando el estado de salud en diversos momentos y las intervenciones realizadas para evaluarlo o alterarlo. La Organización Panamericana de la Salud (OPS) reconoce los EHR como elementos clave dentro de su estrategia de e-Salud en las Américas, enfocándose en su potencial para resolver diversas problemáticas de los sistemas de salud actuales. Aunque la adopción de los EHR presenta complejidades y no existe una única forma de implementación que garantice el éxito, la mayoría de los países de la región están fomentando su uso en diferentes niveles. Además, la Red de eSalud de América Latina y el Caribe (RELACSIS) ha integrado en su agenda el fomento y la expansión del uso de los RME, organizando actividades como foros y webinars que son dirigidos por expertos del área *(OPS, s.f.).*

2.2.2.2. Sistemas de información de salud (HIS)

Según la OPS Los Sistemas de Información para la Salud representan una estrategia de manejo que integra sistemas interoperables y datos abiertos de diversas fuentes, utilizados de manera ética mediante herramientas tecnológicas eficaces. Esto se realiza con el objetivo de

producir información estratégica que beneficie la salud pública (*Sistema de información para la salud*, s.f.).

2.2.3. Cloud computing

Cloud Computing se refiere a la disponibilidad inmediata de recursos de computación a través de Internet, evitando la gestión directa de recursos por parte de las empresas y permitiéndoles pagar por el uso. El cloud computing permite a las empresas acceder remotamente a recursos tecnológicos como procesamiento y almacenamiento, operando como si estuvieran localmente presentes, aunque realmente estén distribuidos globalmente. Esta tecnología se divide en frontend, para el acceso de usuarios mediante navegadores o software específico, y backend, que maneja el almacenamiento seguro a través de servidores y bases de datos controlados por un servidor central. Las ventajas incluyen elasticidad, escalabilidad, y seguridad, facilitando el pago por uso y el trabajo colaborativo. Sin embargo, enfrenta desafíos como potenciales tiempos de inactividad, riesgos de seguridad, control limitado sobre la infraestructura y dependencia de proveedores, lo que puede complicar la migración de servicios y generar costos adicionales. Hay tres modelos de despliegue: nube pública, nube privada y nube híbrida. En las nubes públicas, proveedores externos ofrecen recursos compartidos por Internet. Las nubes privadas, gestionadas internamente, ofrecen más control y seguridad. Las nubes híbridas combinan modelos público y privado, permitiendo aprovechar servicios externos y mantener funciones internas de cumplimiento y seguridad. (*Computación en la nube,* 2024).

3. Metodología

3.1. Fase 1: Revisión de la literatura

Ante la necesidad de fundamentar teóricamente la justificación del problema de estudio, se procede a realizar una revisión bibliográfica exhaustiva. Este proceso incluye la identificación de términos clave y documentos esenciales mediante el uso de bases de datos bibliográficas especializadas.

3.1.1. Análisis bibliométrico

Este análisis permite explorar y comprender los documentos obtenidos mediante la aplicación de una ecuación de búsqueda en la base de datos documental.

3.1.1.1. Ecuación de búsqueda

Se seleccionan palabras clave y términos relevantes para recopilar la información adecuada desde la base de datos documental.

3.1.1.2. Selección de documentos

Inicialmente, se revisan los resúmenes y las introducciones de los documentos que estén relacionados con entidades de prestación de servicios de salud. Esta revisión ayuda a seleccionar los documentos que serán incluidos en la revisión bibliográfica y en los planteamientos del estudio, también se descarta tipos de documentos como cartas, notas, revisión de conferencias, encuestas.

3.1.2. Análisis de literatura

Este análisis se centra en profundizar en el estado actual de la tecnología blockchain y su aplicación en la gestión de registros médicos electrónicos a través de los documentos seleccionados. Se evalúan las diversas aplicaciones de esta tecnología para obtener una comprensión integral de sus beneficios y limitaciones. Este entendimiento detallado es crucial para orientar el desarrollo del estudio y asegurar la alineación con los objetivos propuestos.

3.2. Fase 2: Identificación de posibilidades de integración y de mejora

Esta fase se centra en documentar las dificultades actuales en los procesos de prestación de servicios médicos relacionados con la gestión de información, especialmente en lo que respecta a la historia clínica electrónica. Se explora cómo la tecnología blockchain puede contribuir a la mejora de estos procesos, identificando áreas específicas donde la integración podría ser más beneficiosa.

3.2.1. Análisis de posibilidades de integración

Se identificarán y documentarán los desafíos actuales en la gestión de la información médica, enfocándose en cómo la tecnología blockchain puede abordar estos problemas para optimizar la eficiencia, seguridad y transparencia. Se analizarán los sistemas actuales de EHR para determinar las áreas específicas donde la integración con blockchain podría ser más efectiva.

3.2.2. Mejoras potenciales del sistema actual

Se centrará en identificar y discutir las mejoras potenciales que la tecnología blockchain podría aportar al sistema actual de gestión de registros médicos. Se explorarán las ventajas de la descentralización, la seguridad mejorada mediante criptografía, y la transparencia que proporciona la tecnología blockchain, lo cual puede contribuir significativamente a la reducción de fraudes, errores y tiempos de respuesta en el acceso a la información.

3.2.3. Soluciones propuestas por Blockchain

Se describirán soluciones específicas propuestas por la tecnología blockchain para abordar las deficiencias identificadas en los sistemas de EHR. Se discutirá cómo la implementación de contratos inteligentes y la creación de un libro mayor distribuido e inmutable pueden facilitar la gestión automatizada y segura de los registros médicos, mejorando la interoperabilidad entre diferentes proveedores de servicios de salud y asegurando la integridad de los datos médicos.

3.2.4. Consideraciones éticas y legales

Se abordarán las consideraciones éticas y legales asociadas con la integración de blockchain en los sistemas de EHR. Se discutirá la importancia de asegurar la privacidad y el consentimiento del paciente en el uso de sus datos, los desafíos relacionados con la conformidad normativa y la necesidad de establecer marcos legales claros que regulen el uso de blockchain en la gestión de información de salud. También se explorará cómo la tecnología puede ser diseñada para cumplir con las regulaciones vigentes como HIPAA en los EE.UU., y otras normativas internacionales pertinentes.

3.3. Fase 3: Plantear la integración del Blockchain con EHR

En esta fase, se propondrá un modelo de integración del blockchain con los sistemas de registros de salud electrónicos (EHR). Se diseñarán y definirán los requisitos técnicos, tecnológicos y funcionales necesarios para implementar esta integración, asegurando que se alineen con las necesidades específicas de la gestión de información en la atención al paciente.

Para que lo anterior sea posible, se revisan aspectos clave como los requisitos y casos de uso, además de explicaciones sobre técnicas fundamentales para la integración de blockchain y cloud computing. También se incluyen consideraciones y recomendaciones para futuras implementaciones que deberán tenerse en cuenta en investigaciones posteriores. Se propone una integración, considerando las diversas interacciones dentro del sistema y un modelado de la integración con aspectos clave a tener en cuenta al utilizar los EHR en el sistema de salud.

3.4. Fase 4: Análisis de mejoras y cuantificación de beneficios

En la sección "Análisis de Mejoras y Cuantificación de Beneficios", se aborda cómo determinar las métricas clave para evaluar el rendimiento y los beneficios de la implementación de sistemas de registros médicos electrónicos (EHR). Se examinan varios aspectos críticos como el rendimiento del sistema, evaluando factores como la latencia y la capacidad de procesamiento, y la eficiencia en el uso de recursos. También se contempla la sostenibilidad, considerando el consumo de energía y el impacto ambiental de las tecnologías utilizadas. Además, se detallan métricas de gestión de identidades y de interoperabilidad para asegurar una integración efectiva y segura entre diferentes sistemas y plataformas. Importantes también son las métricas centradas en el usuario, que buscan mejorar la experiencia y satisfacción del mismo. Por último, se incluyen consideraciones sobre los costos e inversiones necesarios para la implementación y mantenimiento de estas tecnologías, así como la importancia de la seguridad y la privacidad en el manejo de datos sensibles. Todo esto constituye una base fundamental para la planificación estratégica y la toma de decisiones informadas en el ámbito de la salud digital.

3.5. Fase 5: Realizar artículo de investigación con carácter publicable

Finalmente, se redacta un artículo de investigación destinado a la publicación, que resumirá los hallazgos, resultados y conclusiones del estudio. Este documento incluirá un análisis crítico de los desafíos enfrentados y las ventajas obtenidas a través de la integración del blockchain, la automatización y el cloud computing en los procesos de registros médicos. Además, se revisarán las características que debe tener el artículo para ser aceptado en una revista científica específica, asegurando que cumpla con los estándares y expectativas del ámbito académico.

4. Revisión de literatura

4.1. Análisis bibliométrico

Para comenzar la revisión de la bibliográfica y ubicar referencias bibliográficas relevantes, es primordial llevar a cabo un análisis bibliométrico. Este análisis tiene como objetivo identificar tendencias en el tema de investigación y resaltar las publicaciones más influyentes en el campo. Se presta especial atención a las palabras claves, tipo de documentos, fundamentación teórica y año de publicación, verificando así la idoneidad de la base de datos para la investigación. La ecuación de búsqueda utilizada para este análisis fue la siguiente:

(Blockchain AND Health AND ("Medical records" OR "Clinical history"))

La aplicación de la ecuación de búsqueda generó una base de datos documental compuesta por 674 documentos de Scopus, con una selección inicial limitada a artículos y capítulos de libros, resultando en 312 documentos. Posteriormente, se eligieron 193 documentos para revisión basándose en criterios y relevancia temática, no hubo acceso a 40 documentos y finalmente se escogieron 31 artículos para una revisión exhaustiva mediante un análisis narrativo. Este análisis busca comprender a fondo las tendencias, enfoques y desarrollos clave en el ámbito de investigación identificado, no solo para obtener información relevante, sino también para identificar patrones y perspectivas emergentes. La revisión narrativa se selecciona como enfoque metodológico para proporcionar una visión contextualizada y holística de la literatura encontrada en Scopus relacionada con el campo de investigación. Adicionalmente, se incluyeron 52 documentos, de los cuales 27 son artículos científicos que provienen de investigaciones previas y en el desarrollo del proyecto. Los recursos adicionales consultados incluyen Google Scholar, Elsevier, Proquest, PubMed, páginas web, etc. La Figura 1 revela que una proporción significativa

son documentos de artículos (70%), seguido por páginas web (27%), posteriormente capítulos de libro (2%) y libro (1%).

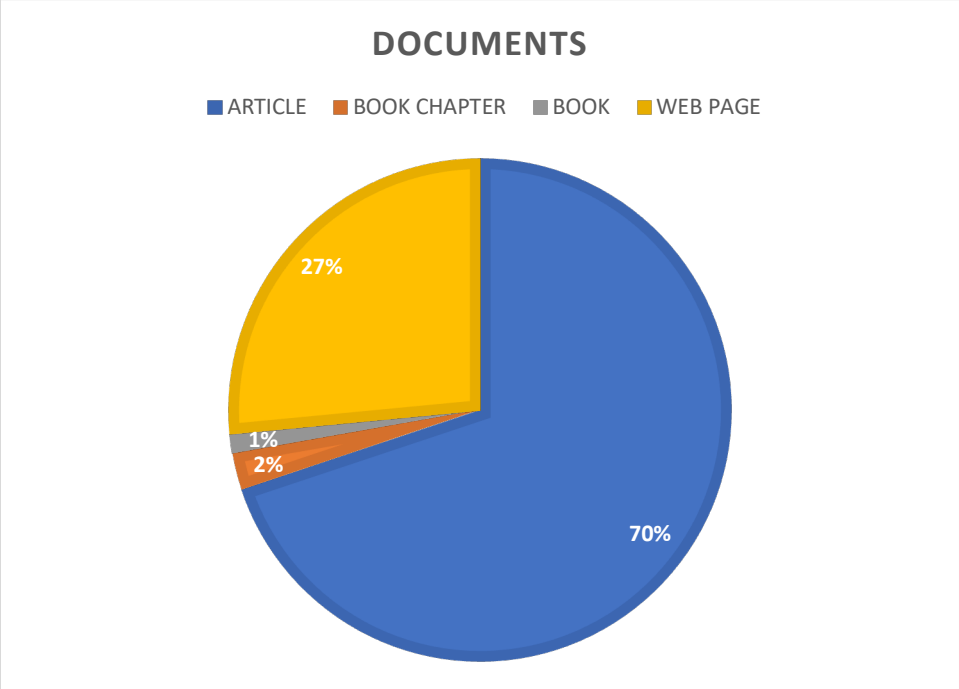

Figura 1. *Documentos por tipo*

La figura 2 muestra la distribución temporal de los documentos seleccionados. Se consideraron artículos, capítulos de libros y libros completos. Las páginas web fueron excluidas del análisis debido a que muchas no especifican el año de publicación o son actualizadas constantemente. Los datos revelan patrones de crecimiento en la producción científica, marcando un aumento significativo en los últimos años. Este análisis temporal proporciona perspectivas clave sobre la evolución y relevancia continua del campo de investigación.

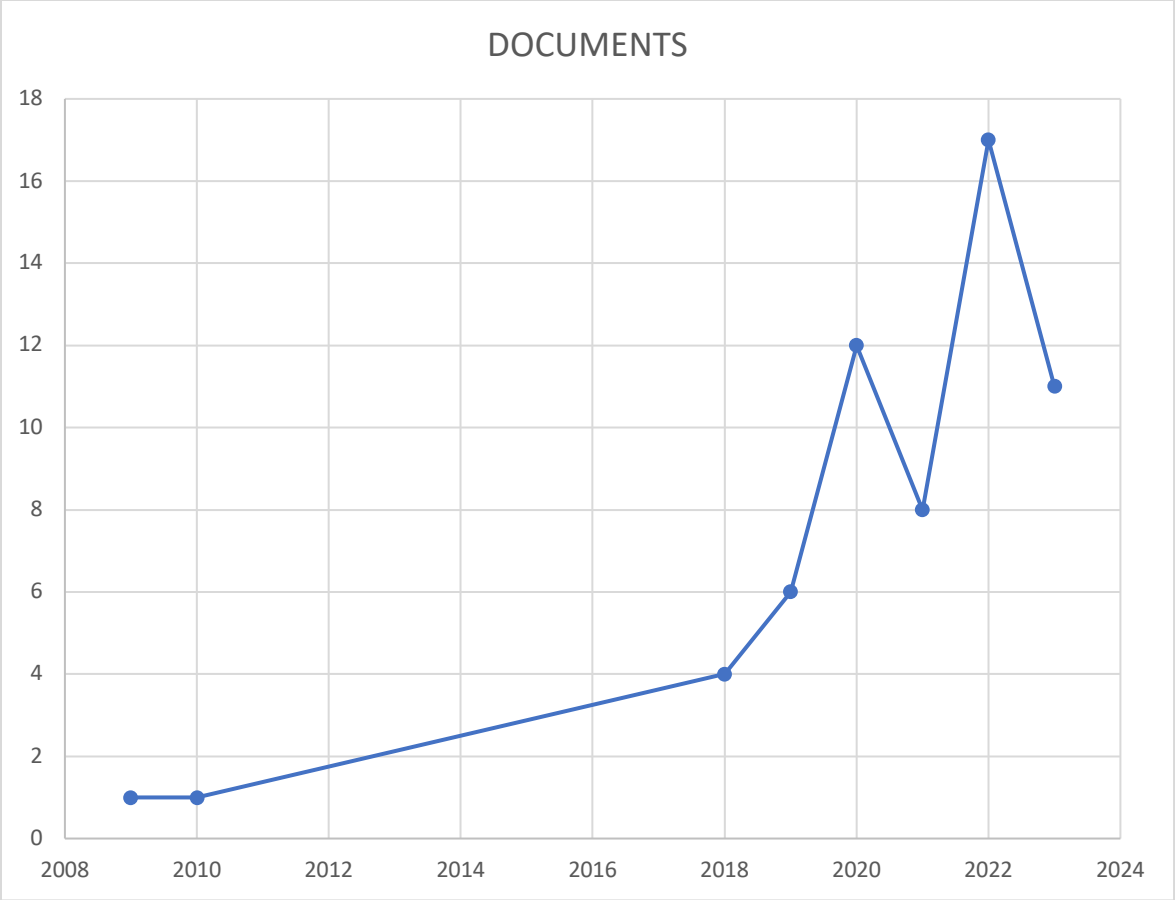

Figura 2. *Documentos por año de publicación*

Un factor crucial en la construcción de fundamentos teóricos es el país de origen de la publicación de los documentos. En el conjunto analizado se destaca India, China, EE. UU. y Arabia Saudita. Permite identificar y valorar las contribuciones de estas regiones en la producción científica relacionada con el Blockchain y el tópico especificado en la ecuación de búsqueda. Ver figura 3.

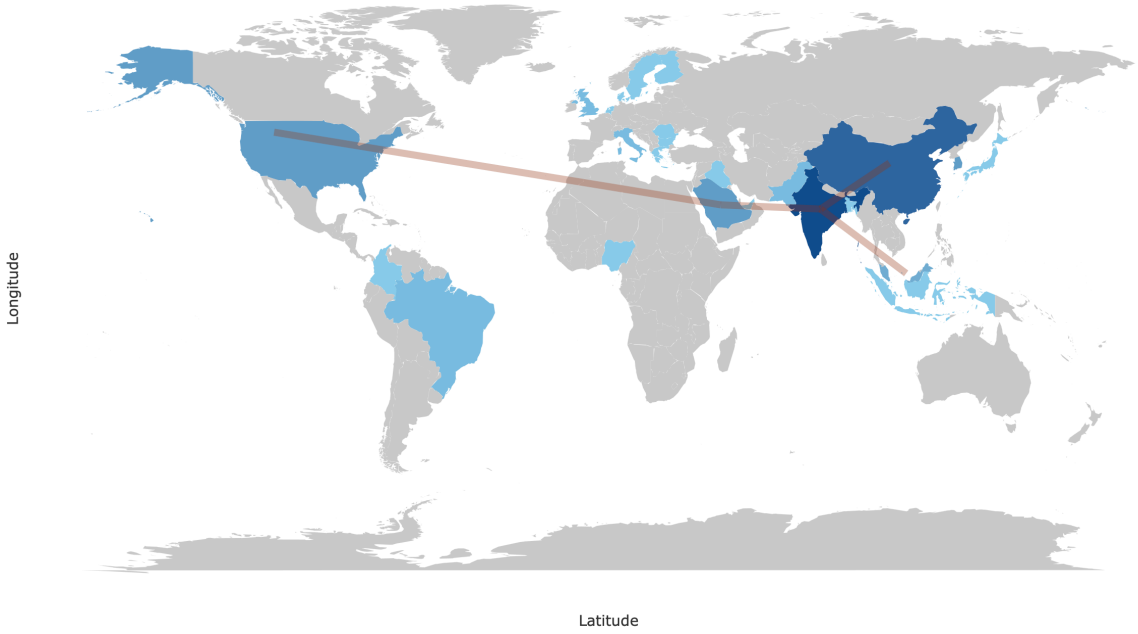

Figura 3. *Documentos por país de publicación*

En la figura 4, se evidencia que los términos más predominantes y vinculados con los documentos a medida que pasan los años son Blockchain, computer security, health care, y en cuarto lugar, Medical record. Estos resultados subrayan la trascendencia de las áreas tecnológicas con la salud y recalcan la importancia de la convergencia interdisciplinaria de estas áreas para el progreso y mejora de la producción científica en este específico campo de estudio.

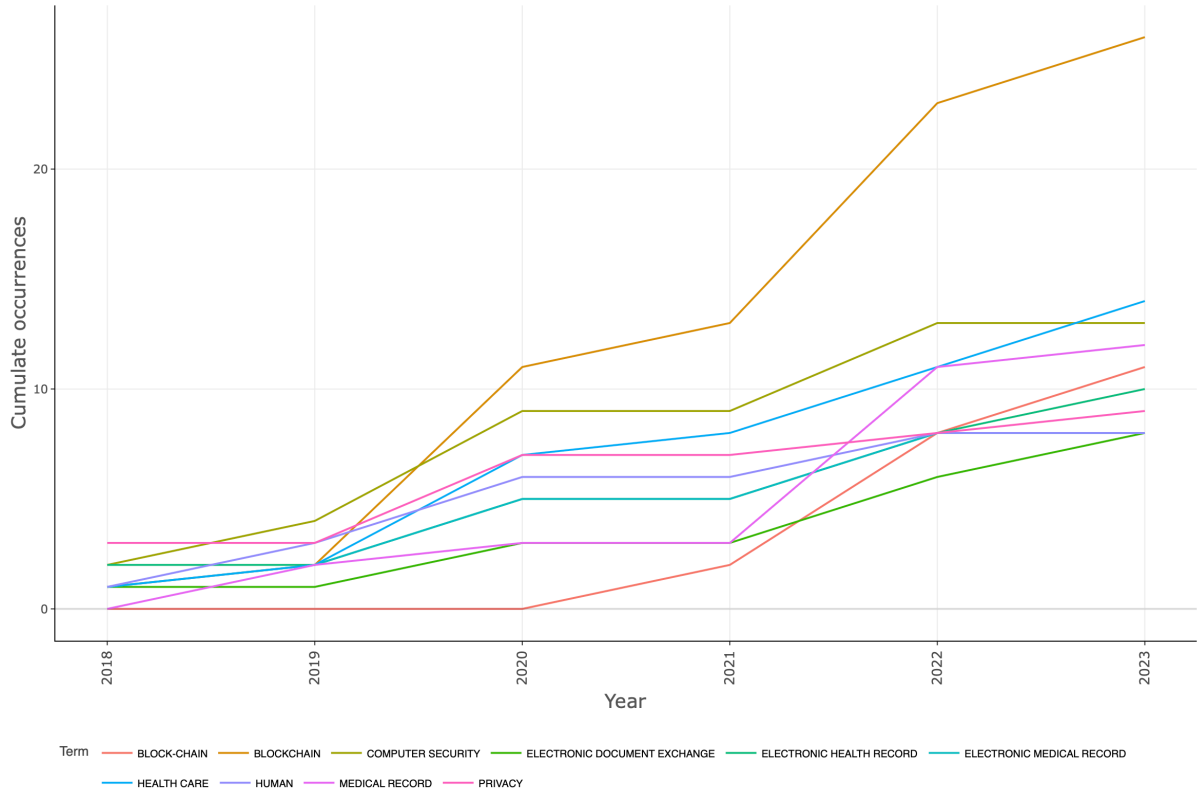

Figura 4. *Términos claves por año*

La Figura 5 muestra que la correlación entre los términos clave de la muestra es congruente con Figura 4 y pertinente para el proyecto en cuestión. Se destacan los términos "blockchain","electronic health record" y "data privacy", que son de suma relevancia para este estudio.

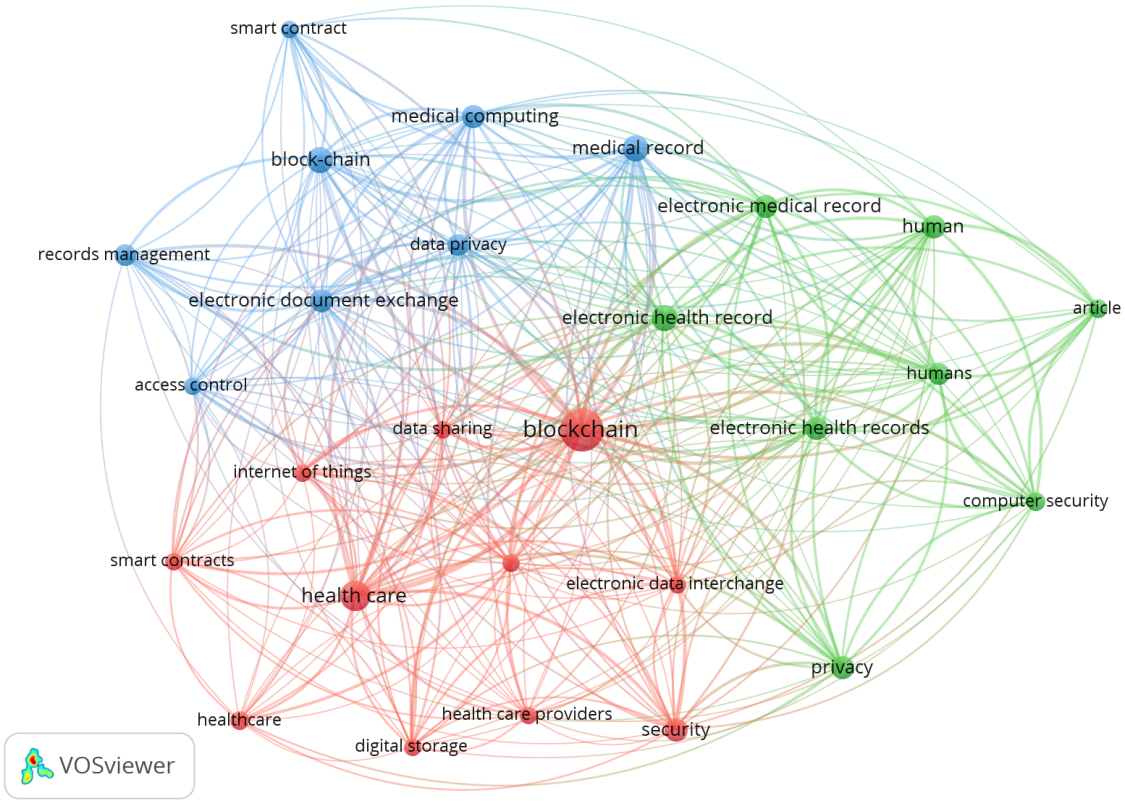

Figura 5. *Correlación de términos claves*

4.2. Análisis de literatura

El Blockchain se ha convertido en una tecnología disruptiva que ha sido de beneficio en diversos ámbitos alcanzando su mayor auge al ser utilizada en un activo digital, pero hoy en día tiene diferentes aplicaciones en sectores de banca y servicios financieros, cadena de suministros, salud, telecomunicaciones, entre otros. Ha tenido impacto positivo en ellos mejorando los procesos, eficiencia, certificación y aduanas. Se quiere indagar que proyectos se han realizado, métodos aplicados y la gestión en su proceso de realización.

Park et al, en 2019 señala que el uso de blockchain en la gestión de registros de salud ofrece ventajas en seguridad y descentralización, permitiendo al paciente controlar sus datos y mejorando

la privacidad. Aunque la implementación de un blockchain privado, controlado por una entidad específica, brinda mayor control sobre el acceso a la información médica sensible, enfrenta desafíos legales y regulatorios, así como obstáculos técnicos y sociales.

Indumathi et al, en 2020 proponen una arquitectura integral basada en blockchain, Internet de las cosas médicas (IoMT) y almacenamiento en la nube para gestionar datos médicos. Enfocándose en una atención médica uno a uno centrada en el paciente, resaltan la importancia de entender los fundamentos de blockchain para su impacto en el futuro de la atención médica. Presentan ejemplos de aplicaciones, como el seguimiento de activos de salud y el intercambio seguro de datos médicos. Validan la arquitectura, destacando su idoneidad para la inspección y revisión de procedimientos en el campo médico.

En 2020, Tanwar et al, abordan a fondo el uso potencial de la tecnología blockchain en la gestión de registros médicos electrónicos, considerando aspectos cruciales como seguridad, facturación de seguros y contratos inteligentes. Destacan beneficios como la interoperabilidad de las bases de datos de salud, el rastreo de dispositivos médicos y mejoras en eficiencia y seguridad en comparación con sistemas convencionales. Aunque se exploran desafíos y limitaciones, la seguridad basada en blockchain recibe atención destacada por su capacidad para ofrecer robustez en el almacenamiento y compartición de datos.

Por otra parte, Poongodi et al, se enfocan en la utilidad de la tecnología Blockchain y el internet de las cosas (IoT) para supervisar la salud de los pacientes. Proponen que incluyen la recolección de datos en tiempo real, la interoperabilidad de los datos y la protección de la privacidad. Esto podría mejorar la eficiencia, la precisión en el diagnóstico y en el tratamiento médico avanzando así en la calidad de la atención médica.

Xu et al. (2023) destaca el papel esencial de la tecnología Blockchain, especialmente en la autenticación de identidad en el hogar inteligente, resalta la función clave de los Smart Contracts de Ethereum, estos contratos ofrecen un nivel adicional de seguridad y confianza en las transacciones e identidad asociadas. La integración de la computación en la niebla complementa esta estrategia, mejorando la eficiencia en tiempo real y fortaleciendo la robustez del sistema.

El sistema propuesto por Akhter Md Hasib et al, redefine la gestión de registros médicos al permitir a los pacientes crear cuentas seguras en línea. Aquí, pueden cargar y almacenar con seguridad datos médicos, con acceso autorizado para los médicos. La privacidad está respaldada por criptografía, y un sistema de pago Ethereum ofrece funciones exclusivas. El estudio destaca los beneficios de un sistema EHR basado en blockchain: mejora en seguridad, privacidad e interoperabilidad. Además, subraya la importancia de abordar desafíos organizativos y éticos, especialmente en entornos de bajos ingresos. La necesidad de capacitación y apoyo técnico adecuados se enfatiza para lograr una adopción exitosa.

La tecnología blockchain, según Reegu et al. (2023), proporciona un sistema seguro y descentralizado para almacenar y compartir datos en entornos de atención médica, asegurando la confidencialidad. Proponen un marco que integra blockchain con el marco robusto HIPAA para abordar problemas de privacidad y seguridad, ofreciendo capas adicionales de protección en el transporte de datos. A pesar de su enfoque transparente y descentralizado, la implementación de blockchain puede enfrentar desafíos en escalabilidad, privacidad y regulaciones, requiriendo posiblemente cambios significativos en los sistemas existentes y una inversión considerable en infraestructura y capacitación para profesionales de la salud.

Jennath et al, en 2020 presentaron un entorno centrado en el paciente para el intercambio seguro de datos médicos mediante tecnología blockchain e inteligencia artificial descentralizada.

En este marco, el proveedor de atención médica clasifica la información del paciente, la envía a un administrador de identidad blockchain para generar un identificador único, y almacena la información personal offline con su hash vinculado a la cadena de bloques. El paciente tiene control sobre los datos compartidos, marcando una lista de verificación, y decide otorgar o no acceso a información adicional. El enfoque parte del supuesto de que los hospitales carecen de infraestructura tecnológica para gestionar los datos del paciente.

Lee, Y. et al, 2022 proponen "medical blockchain", en este caso el usuario también ejerce el control sobre sus datos mediante el uso de una tarjeta inteligente. A través de simulaciones, ilustran cómo la implementación de contratos inteligentes, respaldados por un diseño de criptografía asimétrica de curva elíptica, facilita un mecanismo seguro para compartir registros médicos. Este método demuestra la garantía de precisión en los datos médicos y la preservación de la privacidad del paciente. Además, enfatizan que la integridad de la información de un paciente específico se asegura mediante el control de los contratos inteligentes. Además, se abordan regulaciones y estándares relevantes, como la Ley HIPAA.

Ibor et al, en 2023 proponen el uso de la tecnología blockchain para mejorar la seguridad y privacidad de los registros médicos a través de una plataforma de tres niveles. La blockchain sirve como base de datos para almacenar y autenticar registros médicos, mientras que el cliente permite a los usuarios interactuar con el sistema, brindándoles un mayor control mediante una clave privada. La descentralización elimina administradores y facilita la transferencia eficiente de registros médicos del personal de salud a los pacientes. Se utiliza IPFS para cifrar datos y claves pública/privada para garantizar la seguridad en el intercambio de información. Esta estructura aborda problemas persistentes en la integridad, seguridad y privacidad de los datos médicos, ofreciendo una solución innovadora y prometedora en la gestión de registros médicos.

En la rehabilitación médica, Zhang et al. (2021) proponen abordar los desafíos considerables de los datos del Expediente Médico de Rehabilitación (ERMR) mediante la adopción de una estructura híbrida de red P2P. Utilizan instituciones diversas como super nodos y crean una cadena de bloques de alianza. Se implementa un mecanismo de almacenamiento híbrido que aprovecha el cifrado asimétrico para garantizar el intercambio seguro de datos. La aplicación de firmas digitales y un sólido mecanismo de consenso basado en el algoritmo Raft fortalece la identidad del servidor hospitalario y mejora la tolerancia a fallos del sistema, ofreciendo así una solución integral a los desafíos específicos del intercambio de datos médicos en la rehabilitación.

5. Identificación de Posibilidades de Integración

Se realiza una revisión documental para la identificación de posibilidades de integración.

5.1. Análisis de las Posibilidades de Integración

5.1.1. Revisión de Sistemas Actuales de EHR en instituciones de salud

En la última década, se ha desencadenado a nivel global la incorporación de nuevas tecnologías para la gestión cotidiana de los EHR. La Organización Mundial de la Salud (OMS) ha reconocido los registros médicos como activos que demandan innovación y cuyo intercambio trasciende su utilidad primaria. Estos registros han emergido con el potencial de impactar significativamente en la calidad de vida a nivel mundial (Daraghmi et al., 2019).

Debido al vasto volumen diario de datos, el procesamiento, análisis y almacenamiento eficaz a nivel local se vuelve casi imposible. Por ello, muchos proveedores de atención médica optan por trasladar sus datos al ámbito público. Sin embargo, la falta de interoperabilidad en la información médica representa una amenaza, dificultando los análisis y tratamientos, ya que los

datos están dispersos en lugares como hospitales, farmacias y clínicas. Se destaca la necesidad de una infraestructura más integrada para permitir la interoperabilidad y el intercambio seguro de información médica entre diversos dominios de atención. (Jamil et al., 2020).

En Turquía, se ha evaluado la adopción de Historias Clínicas Electrónicas (EHR) a nivel nacional para mejorar la calidad de los servicios de salud. Entre 2014 y 2017, EE. UU. experimentó un aumento en hospitales con funciones integrales de EHR (25,5% al 39,1%) y una disminución en funciones básicas (58,9% al 41,4%). En Turquía, durante el mismo período, el 63,1% de los hospitales tenía funciones básicas y el 36% funciones integrales. Estudios comparativos destacan un significativo aumento en la adopción de EHR en China, del 18,6% al 85,3% de 2017 a 2018, y en EE. UU., del 9,4% al 96% de 2008 a 2017 (Köse et al., 2023).

Sin embargo, según Daraghmi et al. en la gestión de registros médicos electrónicos, surge una problemática palpable: la carencia de una coordinación fluida y el acceso simultáneo a estos registros. Esta situación genera obstáculos sustanciales en la prestación de servicios de salud, afectando la eficacia y la calidad de la atención médica.

Egala et al.,afirma que la asignación anticipada de recursos, gestionada a partir de predicciones basadas en datos en tiempo real, se ha vuelto esencial para el seguimiento de contactos, cuarentena y automatización de la distribución de vacunas durante pandemias. La digitalización de la información médica, aunque eficaz en la gestión de crisis sanitarias, plantea preocupaciones sustanciales sobre la seguridad y privacidad de los datos. La centralización en un único servidor, aunque simplifica las medidas de seguridad, también implica la pérdida de derechos del propietario de los datos y genera incertidumbres relacionadas con la intervención de terceros, afectando la privacidad y la seguridad de la información.

Los actuales Sistemas de Salud Inteligentes (SHS) enfrentan deficiencias en la preservación de la apertura y privacidad de los registros médicos a nivel sistémico. A pesar de la implementación de medidas de mitigación como pruebas, seguimiento y tratamiento (3T), las arquitecturas informáticas centralizadas muestran vulnerabilidades frente a ataques de denegación de servicio, filtración de datos confidenciales y falta de control absoluto por parte de los propietarios de datos. Abordar estas vulnerabilidades se presenta como un requisito esencial para la evolución efectiva de los sistemas de salud, demandando enfoques innovadores que aseguren la integridad y privacidad de los registros médicos electrónicos a nivel sistémico (Egala et al., 2022).

5.1.2. Limitaciones y desafíos en la gestión de registros médicos.

Las limitaciones en la gestión de registros médicos electrónicos (EHR) se centran en su impacto negativo en la atención personalizada y la interacción médico-paciente. La dinámica médico-computadora-paciente ha reemplazado la atención cara a cara, afectando el razonamiento clínico y perdiendo la narrativa humana. Informes indican que, en promedio, personal médico dedica alrededor del 50% de su tiempo laboral interactuando con la pantalla del EHR en lugar de atender directamente a los pacientes. La introducción de información en la computadora, con múltiples clics del ratón, representa una carga significativa, consumiendo más del 40% de un turno típico de 10 horas y generando más ruido que información clínica relevante. Esto impacta negativamente la eficiencia y calidad de la atención médica. (Honavar, 2020).

La concentración de información en un solo servidor presenta la amenaza del Punto Único de Fallo (SPoF), comprometiendo la certeza sobre la disponibilidad de datos. Este desafío en la gestión de registros médicos electrónicos sugiere que la interrupción o fallo del servidor podría llevar a la inaccesibilidad total de información crítica. Este riesgo plantea dudas sobre la

continuidad y accesibilidad de datos cruciales, resaltando la necesidad de enfoques más resilientes y distribuidos en el diseño de sistemas de gestión de EHR (Egala et al., 2022).

Continuando con las limitaciones de los EHR, según el metaanálisis realizado por Windari et al., en 2023 otros desafíos como los altos costos de implementación, especialmente en áreas rurales, preocupaciones sobre la seguridad de los datos ante ciberataques, resistencia de usuarios y falta de experiencia informática en profesionales de la salud. Se proponen soluciones como un liderazgo efectivo, un ambiente positivo, y una educación y capacitación integral.

Peterson et al., definen la interoperabilidad de los registros sanitarios, destacando desafíos en la estructura y semántica. La complejidad y heterogeneidad de los datos sanitarios dificultan la implementación de estándares propuestos, tanto por la falta de consenso como por la alineación con diversos estándares. La semántica requiere un consenso en esquemas de codificación para garantizar un intercambio efectivo de datos sanitarios. La limitación principal radica en la dificultad para establecer un estándar autorizado y alcanzar consenso en la codificación semántica.

5.1.3. Casos de implementación exitosa de blockchain

Hai et al. (2022), proponen el marco BVFLEMR, que integra blockchain y aprendizaje federado para mejorar la seguridad y ofrecer recomendaciones de tratamientos personalizados en la gestión de EHR. Utilizan Hyperledger Fabric para el almacenamiento en blockchain, abordando desafíos de privacidad en la descentralización de datos de salud. El marco consta de dos partes esenciales: almacenamiento seguro en blockchain y recopilación de datos mediante aprendizaje federado para procesamiento distribuido sin compartir datos crudos. Proporciona una solución integral para mejorar la eficiencia y privacidad en la gestión de datos de salud y la recomendación de tratamientos personalizados, fundamentado en una implementación de tecnología blockchain.

En 2022 Tuler De Oliveira et al. propone SmartAcces, como una solución para el intercambio seguro de información médica entre organizaciones. Abordando desafíos cruciales como políticas de acceso compartido, adaptabilidad dinámica en el control de acceso y la transparencia en el manejo de datos. SmartAccess utiliza contratos inteligentes que imitan la granularidad del modelo de control de acceso basado en atributos (ABAC). En la red blockchain, los responsables del tratamiento definen políticas de acceso en consenso, respaldadas por atributos validados, proporcionando una respuesta integral para aplicaciones en el ámbito de la atención médica, respaldada por pruebas de concepto y una evaluación exhaustiva de seguridad.

PatientDataChain, basado en la tecnología blockchain, tiene como objetivo integrar historias clínicas personales y mejorar la trazabilidad y comunicación de datos médicos en el ámbito de la salud. Un estudio con 100 pacientes y 1144 transacciones en tres meses demostró la capacidad del sistema para unificar registros de salud personales de diversas fuentes en un sistema descentralizado de Historia Clínica Personal (PHR). Utilizando la tecnología Modex BCDB, se integraron eficientemente fuentes heterogéneas de datos médicos, validando funciones esenciales y destacando el potencial del sistema para mejorar la trazabilidad y comunicación de datos médicos en el sector de la salud, manteniendo la privacidad y seguridad del paciente (Cernian et al., 2020).

El proyecto de (Monga & Singh, 2022) se enfoca en MRBSChain, un innovador marco de gestión de registros médicos con un enfoque centrado en el paciente, permitiéndole controlar el acceso y compartición de su información médica. Utiliza un registro unificado y autenticación con algoritmos de cifrado avanzados para asegurar un control seguro de acceso. Identifica 13 factores clave de rendimiento, comparando el marco con modelos tradicionales y evaluándolo en plataformas como Ethereum y Binance Smart Chain. Los resultados indican que MRBSChain es prometedor, priorizando privacidad y seguridad en la gestión de registros médicos, abordando

desafíos de escalabilidad y eficiencia económica, respaldado por estudios que validan su enfoque centrado en el paciente y su implementación exitosa de tecnología blockchain.

5.2. Mejoras potenciales en el sistema actual de salud.

5.2.1. Áreas de la salud donde la blockchain aborda problemas existentes.

Blockchain presenta una variedad extensa de aplicaciones y utilidades en el ámbito de la salud. Al posibilitar la transferencia segura de información médica de pacientes, supervisar la cadena de suministro de medicamentos y facilitar la transmisión segura de los historiales médicos, convirtiéndose en una herramienta valiosa para los investigadores en el campo de la atención médica, permitiéndoles explorar códigos genéticos. Debido a su capacidad para respaldar análisis innovadores, las empresas del sector de la salud pueden observar cambios en sus datos en tiempo real, otorgándoles la capacidad de tomar decisiones rápidas sin intervención humana (Abbas et al., 2022).

En el área de la salud el Blockchain tiene grandes posibilidades de aplicación en la gestión de la cadena de suministro de medicamentos y a partir de ahí se destaca que esta tecnología tiene el potencial de revitalizar eficazmente sectores industriales, abarcando áreas como el transporte marítimo, la fabricación, la automoción, la aviación, las finanzas, la energía, la atención sanitaria, la agricultura y la alimentación, el comercio electrónico, entre otros (Sabbagh et al., 2021).

En la gestión de información sanitaria específicamente se encuentran importantes aplicaciones y que son de suma importancia en los procesos de gestión de información en el sector salud, estas incluyen aplicaciones en el seguimiento de recetas de opioides, información sobre el cáncer controlada por el paciente, telemedicina, atención de telesalud, identificación de pacientes, reclamaciones de seguros y registros médicos de los pacientes (Sadeghib R et al., 2022).

5.2.2. Evaluación de Beneficios Potenciales

En general, blockchain puede proporcionar un sistema de información seguro y aumentar la motivación de los pacientes para compartir registros médicos. Según Sadeghib R et al, blockchain puede mejorar significativamente la eficiencia y seguridad en el intercambio de registros médicos, lo que beneficia tanto a los pacientes como a los proveedores de atención médica. Además, destacan que blockchain permite a los médicos realizar un seguimiento de los registros sanitarios de los pacientes en segundos, lo que mejora la precisión y la disponibilidad de los registros sanitarios. También se menciona que el sector sanitario puede ahorrar alrededor de 100.000 millones de dólares empleando la tecnología blockchain en los sistemas de información sanitaria.

Las cadenas de bloques ofrecen cinco beneficios clave en comparación con los sistemas tradicionales de gestión de bases de datos de atención médica. Proporcionando una gestión descentralizada, para la colaboración entre las partes interesadas sin intermediario. En segundo lugar, proporcionan pistas de auditoría inmutables, útiles para bases de datos inalterables, como informes de reclamaciones de seguros. En tercer lugar, permiten la procedencia de los datos, como el consentimiento del paciente en ensayos clínicos aumentado la reutilización de datos verificados. En cuarto lugar, garantizan la solidez y disponibilidad de los datos, para la preservación y disponibilidad continua de registros médicos electrónicos de pacientes. Por último, mejoran la seguridad y privacidad de los datos al cifrarlos en blockchain y permitir el descifrado solo con la clave privada del paciente (Dimitrov, 2019).

5.3. Soluciones Propuestas con Blockchain.

5.3.1. Modelos de Integración blockchain en los procesos de EHR

El proyecto denominado EdgeMediChain por Akkaoui et al. se configura como un marco descentralizado de intercambio de datos de atención médica basado en la tecnología blockchain. Su propósito es establecer una plataforma segura y eficiente para compartir datos de salud entre personas involucradas en el ámbito de la salud, abarcando a pacientes, proveedores de atención médica, investigadores y aseguradoras. La innovación se basa en la combinación de tecnologías de borde (Edge) y blockchain, con el objetivo de garantizar la privacidad y seguridad de los datos de salud, al mismo tiempo que facilita un acceso ágil y sencillo para aquellos con autorización. Destacan sus características, el proyecto incorpora la implementación de contratos inteligentes para decisiones autónomas y establece políticas de control de acceso restringido, asegurando que solo las partes autorizadas puedan acceder a la información sanitaria. En el proyecto proponen el diseño de un marco de trabajo (framework) de cuatro capas, cuyo enfoque es facilitar el proceso de compartir datos de salud, es decir EHR, datos de salud personal (PHD, por sus siglas en inglés). La estructura de EdgeMediChain se organiza de manera jerárquica, compuesta por cuatro capas fundamentales. Estas capas, gestionadas de forma independiente y descentralizada en cuanto a almacenamiento y procesamiento, se entrelazan y coordinan de manera conjunta para lograr un rendimiento integral del sistema, destacando por su mayor escalabilidad, fiabilidad y capacidad de rastreo. Las cuatro capas comprenden: la Capa de generadores y consumidores de datos de salud, la Capa de minería local de borde, dirigida por autoridades de salud que implementan nodos de borde para procesar datos de salud en zonas designadas y determinan la capacidad y cantidad de nodos en cada grupo de minería local; la Capa global de blockchain, posibilitando la validación para solicitantes de datos y su acceso a información médica según los permisos y reglas definidos

en contratos inteligentes desplegados; y finalmente, la Capa de almacenamiento distribuido fuera de la cadena, encargada de mantener datos completamente cifrados. El marco de trabajo (framework) demostró su capacidad para ofrecer escalabilidad, seguridad y privacidad en el sector de la atención médica, simplificando el intercambio de datos a través de contratos inteligentes y un control de acceso fundamentado en roles. En resumen, revela como una solución eficiente y segura para la compartición de información de salud, complementando la estructura jerárquica y descentralizada del proyecto (Akkaoui et al., 2020).

La infraestructura de MediBlocks por Babu et al. opera a través de transacciones de escritura que reciben información de un método de escritura invocado por el código de cadena. Este proceso implica la generación del valor hash de los EHR, la validación mediante un mecanismo de consenso y la actualización del libro mayor. La red evalúa, ordena y compromete estas transacciones en el libro mayor distribuido, el cual actualiza el estado mundial o recupera datos de este. La característica distintiva de esta red blockchain es su capacidad para permitir que diversos usuarios, incluyendo pacientes, médicos, hospitales y otras entidades hospitalarias, se inscriban a través de un Proveedor de Servicios de Membresía (MSP) confiable. El MSP es un servicio utilizado para firmar y emitir certificados y crear claves públicas y privadas, permitiendo la autorización y verificación de usuarios a través de la Autoridad Certificadora (CA). Consta de una red blockchain Fabric autorizada, donde los participantes controlan la membresía y roles. Los datos de EHR se almacenan externamente en formato de 64 bits en MongoDB, generando un valor hash MD5. Este valor, junto al ID del paciente, se guarda en la base de datos del estado mundial. La plataforma interactiva permite a los usuarios acceder y realizar transacciones de EHR, ofreciendo también funciones de autorización y verificación. Además, el sistema Blockchain propuesto almacena dos tipos de datos, "cadena en línea" y "cadena fuera de línea", facilitando un

intercambio fluido de información sanitaria entre las partes involucradas para mejorar la atención médica. El proyecto sugiere la aplicación de Hyperledger Fabric, una blockchain autorizada, para garantizar la integridad de la información médica. Permite un intercambio seguro y anónimo de datos, preservando la privacidad y ofreciendo un control de acceso efectivo. Los resultados confirman la viabilidad de esta solución, destacando los beneficios de proteger la privacidad y autenticidad de los registros médicos (Babu et al., 2023).

Reegu et al., en 2023, presentan el desarrollo de un marco interoperable basado en blockchain, denominado BCIF-EHR, con el objetivo de mejorar la colaboración entre entidades sanitarias como hospitales y clínicas. Este marco utiliza la tecnología blockchain para asegurar la interoperabilidad entre los marcos Health Level 7 (HL7) y Fast Health Interoperability Resource (FHIR), ampliamente utilizados en el ámbito de la salud. BCIF-EHR se enfoca en salvaguardar la privacidad y seguridad de los registros médicos electrónicos, permitiendo un eficiente intercambio e integración de datos entre diversas entidades. Sigue un enfoque centrado en el paciente p2p, otorgándoles control sobre el acceso a sus registros médicos electrónicos. Además, se implementa un mecanismo basado en hash-lock para garantizar la seguridad al acceder a los registros médicos desde distintas plataformas. Entre las fases del sistema se pueden encontrar los roles y relaciones en los escenarios de registro, preacuerdo y verificación, transferencia de fondos, y el intercambio de registros médicos entre dos hospitales en el marco BCIF-EHR. Utilizan herramientas y técnicas, incluida la implementación de la tecnología blockchain, para lograr la interoperabilidad entre los marcos HL7 e HIPAA. Para lograr la interoperabilidad entre marcos, se duplican datos, una práctica crucial, aunque riesgosa. La gestión de datos, con experiencia en detectar y fusionar registros duplicados, utiliza verificaciones deterministas y algoritmos probabilísticos con identificadores estándar. Estas técnicas revelan posibles casos de registros médicos duplicados.

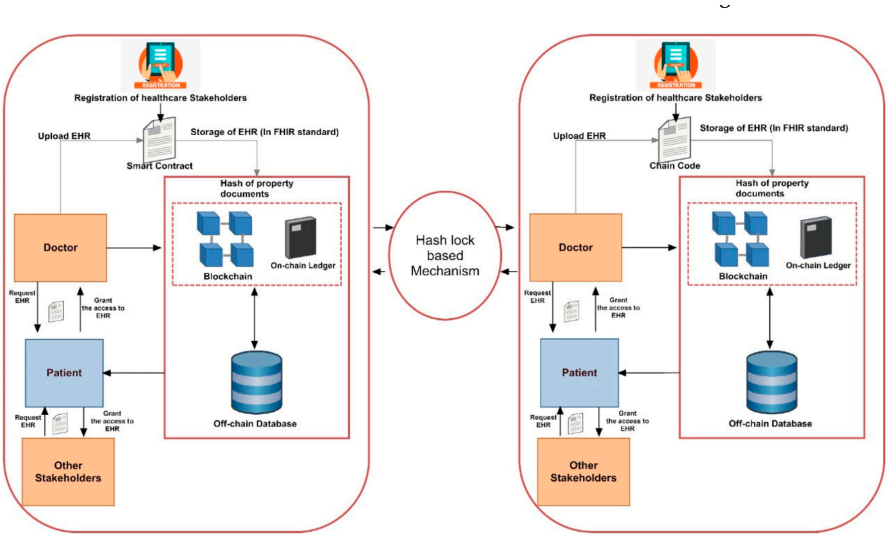

Figura 6. *Marco de intercambio de registros médicos BCIF-EHR.*

Fuente: Adaptado de Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System (Reegu et al., 2023)

En el modelo propuesto por Jennath et al., el proveedor de atención médica recopila datos del paciente, diferenciando entre personal y no personal, enviándolos a un administrador de identidad basado en Blockchain. Si hay un sistema EHR basado en una base de datos, los datos no personales se envían allí, mientras que la información personal se registra fuera de línea y su hash se guarda en Blockchain. El administrador de identidad genera un identificador único y una clave privada para el paciente. Durante la incorporación, el paciente elige preferencias de datos compartidos, actualizando la lista en Blockchain con su clave privada. En el proceso de solicitud de datos, los registros médicos se almacenan en Blockchain con una lista de verificación de permisos. Los proveedores solicitan acceso, y el paciente otorga consentimiento, verificado con la lista de verificación. Los datos consentidos se comparten, y la pista de auditoría se almacena en una Blockchain. La descentralización e inmutabilidad de Blockchain abordan desafíos de seguridad en la gestión de datos médicos. La implementación experimental, que realizaron con Hyperledger Sawtooth y comparada con una base de datos tradicional, destaca las ventajas de

Blockchain en términos de inmutabilidad y trazabilidad, fortaleciendo la integridad y seguridad de los registros médicos electrónicos.

5.4. Consideraciones Éticas y Legales

En 2019, las violaciones de datos en la salud se triplicaron, afectando a más de 41 millones de registros según un informe. Deficiencias en la seguridad de los sistemas EHR, agravadas por el trabajo remoto durante la pandemia, llevaron a consecuencias como la venta en línea de datos y chantajes a pacientes. Un solo ataque cibernético comprometió 21 millones de registros, marcando un aumento significativo desde 2018. Se registraron 572 incidentes en 2019, comparados con 450 hace cuatro años (Landi, 2020).

La compartición de información de salud está sujeta a regulaciones rigurosas y la implementación de blockchain debe ajustarse a ellas para salvaguardar la privacidad y seguridad de la información de salud. Por tanto, resulta esencial que los desarrolladores de blockchain colaboren estrechamente con los reguladores y proveedores de atención médica para asegurar que la implementación de blockchain sea conforme a las normativas existentes y proteja adecuadamente la privacidad y seguridad de la información médica (Sadeghib R et al., 2022).

Según Sabbagh et al., la incorporación del blockchain en la gestión de registros médicos plantea consideraciones éticas y legales clave. Aunque mejora la privacidad y seguridad de los datos, se deben abordar desafíos éticos, como la precisión de la información y sesgos en algoritmos de aprendizaje automático en la atención médica. Además, su implementación conlleva implicaciones legales, exigiendo atención al cumplimiento normativo y la responsabilidad legal. Abordar estos desafíos de manera efectiva es crucial para asegurar un uso responsable y beneficioso del blockchain en la gestión de registros médicos electrónicos.

El EHR en blockchain elimina intermediarios y reduce el riesgo de disparidad de datos, podría exigir cambios significativos en los sistemas existentes y una inversión considerable en infraestructura y capacitación para los profesionales de la salud (Reegu et al., 2023).

Akhter Md Hasib et al. destacan la imperatividad de abordar desafíos organizativos y éticos, especialmente en entornos de bajos ingresos, con énfasis en capacitación y respaldo técnico.

En resumidas cuentas, todos estos beneficios e implicaciones éticas y legales hacen pertinente tener en cuenta aspectos como el cumplimiento de organismos reguladores del sector salud, privacidad y confidencialidad, consentimiento informado, transparencia y responsabilidad ética de las partes involucradas, sensibilización y capacitación adecuada a todas las partes involucradas en especial a pacientes y profesionales de la salud, desarrollo ético de algoritmos y evitar sesgos en algoritmos que usen Blockchain junto aprendizaje automático (ML), auditoría e inspección para evaluar la integridad de los datos e información de manera periódica, gobierno de datos, actualización continua de tecnología y regulaciones.

6. Planteamiento de Integración y Análisis de Beneficios

6.1. Identificación de Requisitos y Casos de Uso

Akkaoui et al. (2020) propone el modelo de EdgeMediChain, el cual garantiza la gestión eficiente de los Registros Médicos Electrónicos (EMR) entre los diversos proveedores de atención médica. Este modelo incorpora la utilización de dispositivos IoT médicos para la adquisición de datos en tiempo real, permitiendo el registro y compartición de esta información para su análisis y seguimiento por parte de profesionales de la salud. A través de una autenticación robusta y un control de acceso adecuado, se reduce el riesgo de ataques cibernéticos, y se posibilita la

recopilación e intercambio de datos con propósitos investigativos, siempre preservando la privacidad de los pacientes.

En el marco de EdgeMediChain, Akkaoui et al. (2020) requiere la utilización de Go-Ethereum (Geth) versión 1.8.27, junto con el compilador de Solidity (0.4.26+), para los contratos inteligentes. El testbed, consistió en 5 máquinas virtuales ejecutando Ubuntu v14.04.6 en un laptop con un procesador Intel I5 a 2.4 GHz y 4 GB de RAM. Una de las máquinas virtuales emuló el blockchain global mediante el mecanismo de consenso Proof of Work (PoW), específicamente Ethereum (Ethash), mientras que las cuatro restantes se utilizaron para emular los pools de minería en el borde local mediante el mecanismo de consenso Proof of Authority (PoA), específicamente Clique. Para satisfacer las necesidades de latencia y seguridad se emplearon distintos mecanismos de consenso en diferentes partes del sistema. Mientras el blockchain global utilizaba PoW, los pools de minería en el borde adoptaron PoA para gestionar eficientemente los grandes volúmenes de datos generados por los dispositivos de IoT médicos (MIoT). Las interacciones entre los usuarios y la plataforma blockchain las llevaron a cabo mediante Node.js, y todas las transacciones se simularon utilizando scripts en la biblioteca web3.js a través de llamadas API JSON-RPC.

Según Akkaoui et al. (2020), esto permitió un enfoque especial en la integración de nodos en el borde (ENs) y los dispositivos de IoT. La implementación y las pruebas se centraron en cómo la adición de un conjunto de pools de minería local en el borde a la arquitectura blockchain influye en el rendimiento del sistema, así como en la escalabilidad del tamaño del libro mayor frente a la enorme cantidad de transacciones generadas por los dispositivos MIoT.

Babu et al. (2023) presentan MediBlocks que permite a los pacientes gestionar sus EHR de manera segura a través de una Interfaz de Usuario (UI). Este modelo facilita la reserva de citas en hospitales específicos, así como el tiempo y los detalles relacionados con el padecimiento.

Posteriormente, se generan los registros de salud tras el tratamiento, con la posibilidad de que laboratorios y farmacias accedan a los datos. Para proteger los registros de salud contra accesos no autorizados, implementaron una capa de transporte (TLS) y cifraron los datos del paciente mediante una clave privada generada durante el registro en la red de blockchain. Además, los pacientes tienen el control total sobre quién puede acceder a su información, utilizando una clave simétrica para cifrar los registros y gestionando las solicitudes de acceso directamente a través de intercambios seguros de claves y listas de control de acceso (ACL). En cuanto al almacenamiento, adoptaron un enfoque distribuido, donde los datos se fragmentan y distribuyen a través de la red, mejorando así la redundancia y la resistencia ante posibles fallos.

Además, Babu et al.(2023) utiliza ciertos componentes para su implementación efectiva. En términos de hardware, emplearon una CPU Intel Core i7-8550U con 16 GB de memoria RAM, ejecutando el Sistema Operativo Ubuntu 18.04 LTS. Para la blockchain, se utiliza Hyperledger Fabric versión 1.4, una plataforma permisionada que ofrece un marco modular. Como componentes clave precisaron las Autoridades de Certificación de Fabric, servicios de ordenación, nodos de respaldo, libros distribuidos y chaincode, ya que estas son las encargadas de emitir certificados para autenticar a los miembros de las organizaciones. Las aplicaciones de usuario final utilizaron un Kit de Desarrollo de Software (SDK) para interactuar con la red de blockchain, almacenando claves e identidad en una billetera. Los usuarios finales pueden interactuar con el gateway y el servidor a través del framework React para invocar las APIs REST y realizar solicitudes GET y POST al servidor. Los documentos EHR se almacenaron en una base de datos distribuida en formato base64, y su valor hash se envía al sistema de blockchain para su recuperación.

Egala et al. (2021), en Fortified-Chain garantiza la seguridad y eficiencia en el registro y transferencia de datos del paciente desde dispositivos de IoMT, asegurando la integridad de la información crítica. Luego, la computación híbrida se encarga de procesar y analizar estos datos para tomar decisiones automatizadas, mejorando la velocidad de recuperación de datos y la automatización de procesos. Permitiendo que el sistema tome el control de dispositivos consumidores para una respuesta rápida ante condiciones críticas, lo que mejora la eficiencia del sistema de atención médica e implementan medidas para garantizar el anonimato del paciente, generando identidades públicas y privadas únicas para preservar la confidencialidad y privacidad de los datos almacenados en la red.

El modelo Fortified-Chain Egala et al. (2021) establece requisitos técnicos específicos para el registro y autenticación de dispositivos IoMT, control de acceso selectivo basado en anillos (SRAC), y garantías de anonimato del paciente. Se emplea la Criptografía de Curva Elíptica (ECC) para generar claves únicas y la capa de computación híbrida para la autenticación de dispositivos. Además, se implementa el Control de Acceso Basado en Anillos Selectivos para regular los derechos de acceso a los datos esto se basa en valores de índice para proporcionar acceso seguro de solo lectura a actores remotos, y técnicas de anonimato del paciente utilizando funciones de hash y XOR para proteger la confidencialidad de los registros médicos. Estos requisitos destacan la importancia del modelo en asegurar la seguridad y privacidad en el contexto de IoMT.

Bera et al. (2023) plantean un modelo que integra tecnología Blockchain con inteligencia artificial (IA) y el internet de las cosas médicas (IoMT) con el fin de hacer un sistema de monitoreo de pacientes durante la pandemia de COVID-19 que se encuentren en casa con un entorno doméstico inteligente. Transmiten los datos a un servidor de niebla (fog server) desde dispositivos inteligentes portátiles que capturan los signos vitales y luego a un Blockchain privado para su

procesamiento y análisis en tiempo real mediante algoritmos de IA que es de gran ayuda en la toma de decisiones informadas para la atención médica, gracias al monitoreo del estado de salud de los pacientes, asegurando la privacidad y la integridad de los datos la unión de la blockchain y la IA permitió la detección temprana de síntomas.

La implementación del modelo ocurrió bajo las siguientes condiciones de dispositivos inteligentes portátiles que capturan signos vitales directamente del cuerpo del paciente y están conectados entre sí y envían esta información de forma segura a dispositivos móviles de propiedad del paciente, luego estos dispositivos transmiten los datos a un servidor de niebla, todo esto con claves de inicio de sesión utilizando criptografía de curva elíptica para el cifrado y descifrado de las transacciones, en el servidor se filtran y se procesan las informaciones útiles, convirtiéndolas en transacción que luego se cifran y se agregan a un blockchain privado en una red de servidores en la nube de igual a igual (peer-to-peer, P2P & Cloud Server Network, CSN) usando un algoritmo distribuido, precisamente el algoritmo de tolerancia a fallas bizantinas prácticas (PBFT), como mecanismo de consenso sobre las transacciones y la adición de bloques al blockchain privado. Esto permite una gestión segura y eficiente de los datos de salud del paciente en tiempo real, con la idea de mejorar la respuesta y el tratamiento a través del análisis de datos y la inteligencia artificial, ayudando a los doctores y profesionales de la salud a una mejor toma de decisiones incluso con el paciente en casa. Además de los requisitos técnicos y de hardware mencionados anteriormente como Dispositivos de internet de las cosas médicas, servidores de niebla, servidores en la nube y dispositivos móviles requiere de consideraciones éticas por ejemplo privacidad y seguridad de los datos ya que es de suma importancia garantizar altos estándares de seguridad para proteger contra accesos no autorizados, consentimiento informado, accesibilidad y equidad, transparencia y trazabilidad. A pesar de que estos requisitos éticos no se detallan explícitamente

en el documento de este caso de uso son esenciales al diseño e implementación de sistemas tecnológicos en el ámbito de la salud.

Hai et al. (2022), proponen un modelo llamado BVFLEMR (Blockchain Vertical Federated Learning E-Medical Recommendation), contiene tecnología que hace posible que los algoritmos de IA adquieran conocimiento y experiencia de diferente gama de datos localizados en distintos sitios entrenándolos por medio de una arquitectura descentralizada, es decir por medio de múltiples dispositivos pero sin requerir de compartir directamente los datos entre sí, esto es llamado aprendizaje federado el cual lo integran con blockchain para realizar un sistema de recomendación basado en la nube para registros médicos electrónicos. Este proyecto se divide en almacenamiento basado en blockchain para EHR, utilizando la plataforma blockchain diseñada para el uso a nivel empresarial Hyperledger Fabric para supervisar y rastrear continuamente las actualizaciones en los EHR en el servidor en la nube. Y también se divide en un módulo de aprendizaje colaborativo que utiliza modelos LightGBM y N-Gram en el aprendizaje colaborativo para recomendar un tratamiento personalizado para la base de datos (BD) en la nube del paciente tras analizar los EHR. El modelo BVFLEMR se orienta a proporcionar un sistema de almacenamiento y recomendación seguro, eficiente y personalizado para el tratamiento de pacientes usando EHRs de manera segura en la blockchain, y analizando los datos mediante aprendizaje federado para producir recomendaciones personalizadas. Este modelo cuenta con beneficios como mejora de la privacidad y seguridad de los datos ya que asegura que los datos de los pacientes se mantengan privados y seguros, disminuyendo preocupaciones sobre ataques cibernéticos y acceso no autorizado a información sensible, sin perder una característica importante como lo es la interoperabilidad entre diferentes instituciones de salud por medio de la blockchain.

Abordando detalles y requisitos técnicos del modelo BVFLEMR, incorporan la tecnología blockchain con Hyperledger Fabric, lo que conlleva a la configuración y gestión de la red blockchain para la supervisión continua de las actualizaciones de los EHR almacenados en la nube y para una buena eficiencia y acceso a los datos usan el sistema de archivos interplanetario (IFPS) que requiere conocimientos técnicos para su integración y uso en el marco de blockchain y aprendizaje federado. En el aprendizaje federado aplicaron técnicas para analizar datos distribuidos sin comprometer la privacidad del paciente, lo que implica manejar la comunicación entre nodos distribuidos, optimizar algoritmos para el aprendizaje con datos descentralizados y gestionar la heterogeneidad de los datos y los sistemas. Para el sistema de recomendación planteado en el modelo BVFLEMR, se usa modelos de aprendizaje automático (ML), ya mencionados anteriormente que son LightGBM (desarrollado por Microsoft que se usa para clasificación y regresión, conocido por su eficiencia en el manejo de grandes volúmenes de datos y por su capacidad para manejar el desequilibrio de datos) y N-Gram (usado para el procesamiento de lenguaje natural (PLN) que predice la probabilidad de una secuencia de palabras en función de la aparición de secuencias de N palabras en un dataset), lo que requiere competencias técnicas en el entrenamiento, validación y optimización de estos modelos para garantizar recomendaciones precisas y personalizadas para el tratamiento de pacientes. Para esta parte del sistema de recomendación se usa análisis de sentimientos y análisis emocional, lo cual implica procesamiento de lenguaje natural (NLP, abreviatura en inglés) y la interpretación de datos no estructurados para mejorar la precisión de las recomendaciones. De hecho, antes de aplicar los modelos de aprendizaje automático, los datos requieren estar preprocesados adecuadamente, lo que conlleva a procesos como ETL que exige tener en cuenta técnicas de limpieza de datos, normalización de datos, y selección de características o variables relevantes. Dado el enfoque del modelo en la protección de

datos sensibles del paciente y el requisito a cumplir normativas, el modelo debe cumplir con requisitos técnicos relacionados con la seguridad de la información y la privacidad, por lo tanto, incluye el manejo de permisos de acceso y la encriptación de datos (Hai et al. 2022).

Estos requisitos técnicos resaltan la complejidad y multidisciplinariedad del modelo BVFLEMR, ya que combina aspectos de blockchain, aprendizaje federado, ML y NLP para proponer una solución integral y segura para la gestión de EHRs. En el documento se enfocan principalmente en aspectos técnicos, pero es importante mencionar requisitos de Hardware como servidores potentes para el aprendizaje federado y de Blockchain, dispositivos de usuario final para interactuar con los sistemas y consideraciones éticas como la privacidad de los datos del paciente según las leyes de protección de datos aplicable como el GDPR en Europa o HIPAA en EE. UU y consentimiento informado explicando el uso, cómo se usarán, quién y qué medidas de seguridad se implementarán ya que estás medidas son fundamentales para su implementación exitosa y ética en un contexto real (Hai et al 2022),.

Cernian et al., 2020 presentan el modelo PatientDataChain que busca aportar solución a varias problemáticas y desafíos en el área de la salud, la falta de interoperabilidad entre diferentes proveedores de servicios de salud, y los problemas relacionados con la privacidad y seguridad de los datos, con un enfoque en tecnología blockchain para integrar registros médicos electrónicos en un sistema unificado y descentralizado. Integran EHR de diversas fuentes existentes, proveedores de atención médica como laboratorios, y datos de dispositivos vestibles y sensores de salud. El sistema también otorga propiedad y control de datos por parte del paciente siendo los mismos pacientes los que conceden acceso de sus datos de salud a proveedores de atención médica específicos. Usa un mecanismo de token basado en la clave pública del paciente para controlar el acceso a los registros médicos, asegurando la privacidad y seguridad de los datos.

PatientDataChain se integra con sistemas EHR existentes sin alterar la operación de los sistemas EHR existentes a través de interfaces de programación de aplicaciones (APIs), permitiendo la fusión de datos médicos en la infraestructura de backend de PatientDataChain. El modelo usa Modex Blockchain Database (BCDB) que permite una adopción de blockchain más sencilla en el desarrollo de software empresarial, debido a que BCDB, un sistema de almacenamiento de almacenamiento de datos híbrido que combina y conecta tecnología blockchain con motores de bases de datos existentes. Finalmente, hacen una implementación de un Concepto de Prueba (PoC), demostrando factibilidad para integrar EHR de fuentes heterogéneas en un sistema descentralizado de registros médicos electrónicos (EHR) o registros de salud personales (PHR) con intercambio de datos mejorado. Respecto aspectos técnicos registro de usuarios a través de una aplicación móvil, fusión de datos para garantizar el acceso asignando un identificador único (ID) a cada paciente, propiedad de datos con un par único de claves privadas y públicas asociadas al usuario, ya que estás claves son necesarias para la autenticación del usuario, la firma de transacciones y el cifrado/descifrado de datos. Todo esto les permite conectar no solo con sistemas EHR sino que también con dispositivos wearables como Fitbit, permitiendo la recuperación de los datos médicos y su inserción en la arquitectura de Modex BCDB. La componente blockchain almacena elementos de autenticidad (timestamp, hash y clave de cifrado), mientras que los registros médicos electrónicos cifrados se almacenan en la base de datos MongoDB en correlación con el hash de la blockchain.

PatientDataChain representa un enfoque innovador para abordar problemas de larga data o periodo antiguo, dando una solución integrada y centrada en el paciente para la gestión de EHR con el apoyo de la tecnología blockchain.

6.2. Explicación de Técnicas para la Gestión de Datos en la Integración

6.2.1. Análisis de requisitos de Datos

Es esencial saber qué requisitos y qué datos son necesarios y cómo será su uso y su protección en el sistema basado en blockchain.

Primero que todo, es esencial identificar datos confidenciales y sensibles, ya que estos requerirán una buena protección o incluso una protección adicional. Por ejemplo, la información personal de salud (PHI) debe estar sujeta a regulaciones como HIPAA. La información personal de salud, según HIPAA, se puede desglosar en registros médicos electrónicos (EHR) o registros personales de salud (PHR), información demográfica, información de facturación y pagos, datos de dispositivos médicos, notas psicológicas y psiquiátricas. Sin embargo, la PHI no se limita a los mencionados anteriormente, que están más relacionados a información creada o mantenida por proveedores de atención de salud, sino que también incluye cualquier dato que otros intermediarios del sector de la salud puedan tener, como por ejemplo, aseguradoras de salud. Debido al tipo de información manejada, que puede ser sensible o que tiene riesgo de violación de la privacidad, existen regulaciones como HIPAA en los Estados Unidos y el GDPR en Europa, que tienen estrictas pautas para evitar repercusiones sociales, emocionales y monetarias para los individuos afectados. Respecto a las técnicas que se pueden usar para proteger tanto los datos confidenciales como no confidenciales, se incluyen el cifrado de datos y técnicas de anonimización; en la blockchain, se hace uso de cifrado avanzado. Técnicas de anonimización y pseudonimización pueden ser aplicadas para mejorar la privacidad de los pacientes, en especial al momento de hacer análisis estadístico. Usando métodos como la k-anonimización, se busca proteger la identidad en un conjunto de datos. La k-anonimización es una técnica para proteger la privacidad de

información personal. Hay que considerar que la información no sea apreciable para al menos una persona menos de ese número k que sea objetivo; en otras palabras, los datos de un individuo deben ser indistinguibles para k-1 individuos. Estableciendo k como un número entero con el nivel de anonimato deseado, teniendo en cuenta que aumentar k ofrece más privacidad, pero mayor pérdida de información útil. Por ejemplo, k debe ser un número entero mayor o igual a 1, donde k=1 indica que no hay anonimización y cada registro es único. Para k=2, significa que cada registro debe ser indistinguible de al menos otro registro y, en el caso de k=5, debe ser indistinguible de al menos otros cuatro registros. Para cumplir con la k-anonimización, se usan técnicas como la supresión, que no es más que eliminar o enmascarar parte de la información, por ejemplo, eliminar la calle en direcciones o enmascarar los últimos 7 dígitos del número de teléfono por 7 letras X. Otra técnica es la generalización; por ejemplo, si la persona tiene 24 años, se podría utilizar un rango de edad para mantener la privacidad, se podría emplear entre 20 y 30 años, o en caso de usar la fecha de nacimiento, se podría reemplazar por el año o la década. El grado de probabilidad que se pueda identificar se determina mediante la proporción 1/k. Hay que tener en cuenta que existen factores como datos cuasi-identificadores que no permiten una identificación directa pero quizás, al tener, por ejemplo, código postal y ocupación y al combinar estos datos, permita la reidentificación de individuos, lo cual puede ser un riesgo para la privacidad, especialmente si se intenta reidentificar con técnicas como ataque de enlace (linkage attack), que cruza información entre diferentes bases de datos; inferencia estadística, ya que puede contener modelos estadísticos o de ML para identificar patrones o características únicas; y ataque de singularidad (unicity attack), que se centra en que al tener suficientes atributos, incluso anonimizados, permiten identificar a una persona. Todo esto resalta la importancia del uso de tecnologías y técnicas sofisticadas, de

acuerdo al contexto, junto al cumplimiento de las regulaciones de protección de datos aplicables (Wabo G et al, 2023).

Otro requisito es necesidades de acceso y control y esto requiere que esté determinado a qué datos y en qué situaciones, pero sobre todo quiénes tendrán acceso, como por ejemplo pacientes, proveedores de salud e investigadores (Jennath et al, en 2020).

Requisito fundamental es el consentimiento y propiedad de datos, ya que el usuario es el dueño de sus datos se debe establecer métodos para el consentimiento explícito del paciente para el uso y compartición de sus datos, en relación con las leyes y estándares aplicables. La blockchain puede ser utilizada para gestionar el consentimiento del paciente de manera segura y transparente por ejemplo con contratos inteligentes.

La Interoperabilidad es un factor necesario porque tiene en cuenta mecanismos estandarizados para compartir datos teniendo en cuenta una manera segura y eficiente para comunicarse e intercambiar datos entre diferentes sistemas y organizaciones e incluso regiones, usando estándares como HL7 y FHIR para facilitar la interoperabilidad (Quiel et al., 2019). Contar con técnicas de análisis de datos para la interoperabilidad puede ser de gran utilidad. Utilizar algoritmos de machine learning y análisis estadístico para mapear datos entre diferentes formatos y estándares puede facilitar la interoperabilidad entre sistemas. (IBM, s.f.) Técnicas como el procesamiento de lenguaje natural (NLP) pueden ser útiles para extraer información relevante de registros médicos no estructurados y convertirlos en formatos estandarizados como FHIR o HL7.

Cumplir con requisitos regulatorios se hace necesario casi para cualquier sistema en especial en sistemas de gestión de información de salud porque cuentan con datos sensibles e información personal que debe cumplir con las regulaciones locales e internaciones sobre la

gestión de datos de salud como HIPAA en los Estados Unidos y GDPR en Europa (Alves et al, 2022).

6.2.2. Modelado de Datos

En esta fase de modelado de datos que se incorpora soluciones con blockchain es esencial la accesibilidad, la seguridad y la integridad de los datos.

Primero analizar el tipo de base de datos ya que al tener una base de datos relacional más común, ya que se estructuran con tablas organizadas en filas y columnas, podría ser lo más intuitivo para los usuarios, pero no correcto para la diversidad de archivos que puede contener los datos de salud. Es recomendable contar con una estructura de datos flexible porque permite adaptarse a diferentes tipos de información médica y evolucionar con las necesidades del sistema. (Montemagno, et al. 2023) El uso de bases de datos NoSQL, como MongoDB o Apache Cassandra o bases de datos en la nube por ejemplo Azure Cosmos DB y Google Cloud Firestore, por su capacidad para manejar eficientemente datos no estructurados o semiestructurados, se convierte en una alternativa superior para el almacenamiento de información médica compleja. También, el empleo de sistemas de archivos distribuidos como IPFS puede mejorar la accesibilidad y persistencia de los datos a través de un sistema descentralizado (Egala et. Al, 2022).

Normalización vs Desnormalización, debido a que existen ventajas de la normalización de datos para la integridad de los datos versus la desnormalización para mejorar el rendimiento en consultas complejas. Es crucial considerar la aplicación de técnicas estadísticas para normalizar los datos a una escala común por ejemplo la normalización de rangos, lo que es relevante en el manejo de datos médicos provenientes de distintas fuentes, lo que ayudaría a estandarizar mediciones de diferentes análisis, considerando que en los procesos de seguimiento del historial

médico de un usuario es muy importante la no redundancia de los registros para que los tratamientos sean fiables y precisos. Por otro lado, la desnormalización puede ser estratégicamente implementada mediante el uso de indexación y cachés de datos para acelerar la recuperación de información en sistemas donde la rapidez de consulta es primordial, como en el acceso a historiales médicos durante emergencias, aunque deben manejarse con cuidado para evitar inconsistencias en los datos (Sql, 2023).

Hashing para proteger la confidencialidad y tener una red con menos carga, se puede considerar estrategias como almacenar solo el hash de los registros médicos en la blockchain y mantener los datos detallados de manera segura off-chain o fuera de la cadena. La utilización de algoritmos de hashing avanzados, como SHA-256 o SHA-3, asegura la creación de resúmenes de datos únicos y seguros, estos resúmenes únicos son prácticamente imposibles de revertir, lo que los hace ideales para verificar la integridad de los datos sin revelar su contenido (Gate.Io, 2023). Paralelamente, la adopción de IPFS (Metlabs, 2023) como sistema de archivos distribuido permite un almacenamiento y acceso eficiente a través de hashes únicos, fortaleciendo la integridad y confidencialidad de los datos médicos.

Pero hay un detalle que no es menor y es que algunas regulaciones normativas como el GDPR en Europa según Vollmer (2023) establece que las personas tienen derecho a exigir la eliminación de sus datos personales con exclusión de ciertos casos como interés público, esto hace necesarios aplicar otros enfoques o estrategias como guardar los datos personales en un sistema de almacenamiento externo pero que en la blockchain se registre el hash correspondiente a esos datos para tener control de acceso y permita eliminar los datos del sistema externo, otra forma es el uso de contratos inteligentes para la gestión de acceso y dado el caso de solicitud de eliminación, el contrato inteligente debe ser actualizado para revocar el acceso a los datos, otra estrategia es usar

estrategias de encriptación de datos antes de su almacenamiento en PFS o una red blockchain, por lo cual la clave de encriptación se guarda en un sistema seguro y controlado, lo cual permitiría eliminar la clave de encriptación dejando los datos inaccesibles e inteligibles, a pesar de que técnicamente sigan almacenados. Implementar estas estrategias requiere de una revisión de las regulaciones de privacidad y protección de datos y de una planificación y correcto diseño del sistema de registros médicos electrónicos basado en blockchain, mientras se sigue manteniendo ventajas de seguridad y eficiencia aportadas por la tecnología blockchain (Politou, et. Al, 2021).

Contratos inteligentes para la gestión de datos según Khatoon (2020) es comúnmente utilizado para que faciliten la creación, modificación y acceso a registros médicos, asegurando que solo las partes autorizadas puedan realizar estas operaciones. Plataformas como Ethereum, con su lenguaje Solidity, y Hyperledger Fabric ofrecen entornos robustos para el desarrollo de contratos inteligentes que pueden automatizar procesos clínicos y administrativos, garantizando la precisión y el cumplimiento de las políticas de acceso a los datos. Otras plataformas como Tezos, que soporta contratos inteligentes y ofrece la capacidad de auto-amendarse. Existen herramientas de desarrollo como Truffle Suite que ofrecen entornos de desarrollo, pruebas y despliegue integrados para Ethereum, mientras que Remix es un IDE (entorno de desarrollo integrado) basado en el navegador para escribir, probar y desplegar contratos inteligentes en Solidity.

La implementación de identificadores únicos de pacientes y proveedores de atención médica ayuda para el rastreo y acceso a los registros médicos sin comprometer la privacidad. Existen ciertas tecnologías de identificación de pacientes como UUID (Universally Unique Identifier) o DID (Decentralized Identifiers) que son técnicas comunes para generar identificadores únicos. Los UUID son identificadores estándar que garantizan la unicidad a nivel global sin necesidad de un sistema centralizado, mientras que los DIDs son una nueva forma de identificación

que permite el control autónomo sobre identidades digitales, especialmente útil en contextos descentralizados. La adopción de UUID o DIDs proporciona una metodología segura y descentralizada para la gestión de identidades dentro del ecosistema de salud, permitiendo la interoperabilidad y el acceso controlado a la información del paciente (Zwitter A. et al, 2020).

La integración de estos conceptos ayuda a crear un sistema de registros médicos electrónicos basado en blockchain seguro, eficiente y adaptable a las necesidades cambiantes de los proveedores de atención médica y los pacientes, promoviendo la escalabilidad y la adaptabilidad para necesidades clínicas y administrativas. El cumplimiento de las regulaciones de salud también ayuda a que el sistema sea funcional.

6.2.3. Criptografía para Seguridad de Datos

La criptografía desempeña un papel fundamental en la seguridad de los datos dentro de la tecnología blockchain al proporcionar un método seguro para proteger la integridad y la privacidad de la información almacenada en una cadena de bloques. Esta disciplina se puede dividir en dos categorías principales: criptografía simétrica y criptografía asimétrica. La criptografía simétrica utiliza dos claves, una privada y otra pública, donde el remitente comparte solo su clave pública para cifrar y descifrar los datos. Por otro lado, la criptografía asimétrica utiliza un protocolo HTTPS con una única clave para cifrar y descifrar, lo que la hace más económica que la primera. Ambos métodos aseguran la transparencia de los datos almacenados debido a la inmutabilidad inherente del blockchain (Montenegro, 2021).

Criptografía de curva elíptica (ECC), la encriptación de curvas elípticas implica utilizar puntos finitos con coordenadas enteras para realizar cálculos eficientes y precisos. Se emplean dos tipos de cuerpos finitos: cuerpos primos y cuerpos binarios. La adición repetida de un punto

consigo mismo genera otro punto en la curva. La seguridad de este método se basa en la dificultad de resolver el problema del logaritmo elíptico, similar al problema de logaritmo discreto en curvas elípticas. Esto garantiza que la función de encriptación no pueda ser revertida fácilmente por terceros malintencionados. La criptografía de curva elíptica ofrece varias ventajas significativas respecto al RSA. En primer lugar, permite el uso de claves más cortas, lo que mejora la eficiencia y reduce los recursos necesarios para el cifrado. Por ejemplo, un sistema ECC de 256 bits es equivalente en seguridad a un sistema RSA de 3072 bits. Además, el funcionamiento de ECC es más eficiente en términos de rendimiento en comparación con RSA, lo que lo convierte en una opción atractiva para aplicaciones donde la velocidad y la eficiencia son críticas (KeepCoding, 2023).

Encriptación Basada en Atributos (ABE), según Vishwesh 2018, se basa en la utilización de atributos, como roles, identidades o características definidas, para cifrar y descifrar datos. En lugar de utilizar una única clave como en los sistemas tradicionales de encriptación, el ABE permite el acceso a la información basado en un conjunto de criterios predefinidos. Este se divide en CP-ABE (Ciphertext-Policy Attribute-Based Encryption), en donde, la encriptación de los datos se realiza bajo una política definida que especifica qué atributos son necesarios para descifrar el contenido. Las claves de los usuarios se generan en base a sus atributos, y el descifrado sólo es posible si la clave del usuario cumple con la política del texto cifrado; y KP-ABE (Key-Policy Attribute-Based Encryption) los datos se cifran con un conjunto de atributos y las claves de los usuarios se asocian con políticas que indican qué atributos son necesarios para el descifrado. Los usuarios pueden descifrar cualquier texto cifrado que contenga atributos que coincidan con su política de clave.

La encriptación y el descifrado dependen del cumplimiento de los atributos con las políticas establecidas, lo que proporciona un mecanismo de control de acceso granular y basado en roles. ABE es particularmente útil en escenarios donde los requisitos de acceso son dinámicos y dependen de las credenciales del usuario más que de una clave compartida fija.

La criptografía basada en hash se fundamenta en el uso de funciones hash criptográficas deterministas y eficientes para generar un valor hash único de longitud fija, que actúa como un "resumen" digital del mensaje, asegurando la resistencia tanto a la pre-imagen, haciendo inviable encontrar un mensaje basado en un hash conocido, como a colisiones, evitando que dos entradas distintas produzcan el mismo hash. Teniendo algoritmos generalmente más simples y rápidos basados en números primos o en curvas elípticas, con un rendimiento relativamente rápido. Esquemas como Lamport-Diffie, Winternitz y Merkle Signature Scheme aplican estas funciones para crear firmas digitales, aunque con la limitación de que pueden requerir claves de un solo uso, lo que conlleva a tener una clave nueva para cada firma y resultar en claves y firmas de tamaño considerable, representando un desafío en términos de almacenamiento y gestión. No obstante, su potencial resistencia a la computación cuántica los perfila como candidatos ideales para sistemas de seguridad en la era post-cuántica, proporcionando un campo de investigación activo para el desarrollo de la criptografía futura (Đỗ y Khit, 2023).

RSA (Rivest–Shamir–Adleman) es un algoritmo de criptografía de clave pública desarrollado por Ron Rivest, Adi Shamir y Leonard Adleman. Es uno de los primeros y más ampliamente utilizados sistemas de este tipo y se basa en la dificultad computacional de factorizar el producto de dos números primos grandes. RSA permite tanto el cifrado de datos como la creación de firmas digitales. La seguridad de RSA se basa en la generación de una clave pública y privada y la dificultad práctica de factorizar n en sus componentes primos originales, p y q, un

problema considerado difícil de resolver con las computadoras actuales, especialmente a medida que el tamaño de los números primos aumenta. Sin embargo, la seguridad también depende de una implementación adecuada y del uso de números primos suficientemente grandes para resistir los avances tanto en algoritmos de factorización como en capacidad de cómputo (Milanov, 2009).

AES (Advanced Encryption Standard) es un algoritmo de cifrado por bloques fue desarrollado por Vincent Rijmen y Joan Daemen y seleccionado por el Instituto Nacional de Estándares y Tecnología (NIST) en 2001. AES es conocido por su seguridad y eficiencia tanto en software como en hardware. AES cifra datos en bloques de 128 bits, soporta longitudes claves de hasta 256 bits y utiliza sustitución-permutación como estructura. El algoritmo de cifrado AES (Advanced Encryption Standard) opera en varios pasos que se repiten en múltiples rondas, dependiendo de la longitud de la clave utilizada. En primer lugar, se organiza el texto plano en una matriz de 4x4 bytes, denominada estado inicial. Durante las rondas de cifrado, se realiza una serie de operaciones, incluyendo la adición de la clave de cifrado al texto plano, seguida de etapas como SubBytes, ShiftRows, MixColumns y AddRoundKey, donde se sustituyen bytes, se permutan filas, se mezclan columnas y se añade la clave de ronda. En la ronda final, se omita la etapa de MixColumns. Finalmente, después de completar todas las rondas, el estado final se convierte en el bloque de texto cifrado. AES puede ser considerado seguro contra los ataques conocidos, con la excepción de aquellos que requieren capacidades computacionales no prácticas (como ataques de fuerza bruta contra claves muy largas) o vulnerabilidades a través de ataques de canal lateral en implementaciones específicas (Ciberseg, 2022).

6.2.4. Estandarización de Datos

En la salud existen estándares que procuran mantener la interoperabilidad entre los diferentes sistemas de información en salud, posibilitando el intercambio seguro, efectivo y eficiente entre las plataformas y entidades. Los más utilizados entre las entidades de salud son:

HL7 (Health Level 7) y FHIR (Fast Healthcare Interoperability Resources). El HL7 es el más antiguo y adoptado estándar para intercambiar datos clínicos y administrativos entre software de atención médica. La versión 2.x es la más utilizada de HL7, y su enfoque es en el envío de mensajes específicos relacionados con eventos clínicos (como admisiones, transferencias, altas, y actualizaciones de ordenes médicas). Sin embargo, debido a su flexibilidad, puede resultar en implementaciones variadas que dificultan la interoperabilidad. Por otro lado, el HL7 CDA (Clinical Document Architecture) Proporciona un marco para el intercambio de documentos clínicos (como resúmenes de alta y notas de progreso) de manera estandarizada, asegurando que el contenido del documento sea comprensible tanto para humanos como para máquinas (Pais, M. J. 2019).

FHIR (Fast Healthcare Interoperability Resources) se diseñó para lograr mejorar las versiones anteriores del HL7 y otros estándares, con la utilización de las nuevas tecnologías para facilitar el intercambio de salud electrónica. FHIR estructura la información en "recursos" que representan conceptos clínicos granulares (como pacientes, admisiones, elementos de medicación, etc.) y define cómo se relacionan entre sí. Estos recursos pueden ser fácilmente compartidos o compuestos para crear registros más complejos. Emplea un conjunto de APIs basadas en RESTful, que permiten una integración más simple y directa con sistemas de información en salud modernos. Soporta formatos de datos como JSON y XML para el intercambio de datos y se beneficia de

protocolos web estandarizados para la autenticación, autorización y comunicación (Landi, H., 2019).

El HL7 y FHIR son importantes para avanzar hacia una atención médica más integrada y centrada en el paciente, facilitando el intercambio seguro y eficiente de información clínica. La elección entre estos estándares y su implementación depende de las necesidades específicas de interoperabilidad, los sistemas existentes y los objetivos de las organizaciones de salud. La estandarización de datos en el ámbito de la salud es fundamental para asegurar la interoperabilidad efectiva entre sistemas de información heterogéneos en donde el mapeo de datos obtiene un papel importante para identificar las relaciones entre los modelos de datos de los sistemas de origen y destino. Implicando la transformación de formatos, tales como, fechas, unidades de medida y la conciliación de datos para asegurar la coherencia. El proceso de mapeo de datos implicaría un análisis exhaustivo de los modelos de datos, comprendiendo su estructura y semántica, seguido por la definición de reglas claras para la transformación de datos, considerando las similitudes o las diferencias entre los sistemas, Esto puede implicar, por ejemplo, cómo se mapean los identificadores únicos de pacientes entre diferentes plataformas. Luego, se implementa la transformación de datos utilizando herramientas ETL (Extracción, Transformación y Carga) o scripts personalizados, y se aplican controles de calidad para garantizar la integridad y precisión de los datos antes de su incorporación en el blockchain debido a su naturaleza inmutable (Pais, M. J. 2019). El blockchain introduce desafíos únicos en el mapeo de datos, como la inmutabilidad de los registros, que demanda una precisión absoluta en los datos antes de su registro. Al mismo tiempo la descentralización del blockchain, lleva a la necesidad de gestionar la estandarización de datos a través de los anteriormente mencionados ya que no habría una autoridad central.

6.3. Recomendaciones para Implementaciones Futuras

6.3.1. Análisis de Tendencias Tecnológicas

Es de suma importancia explorar desarrollos recientes que cuenten con la tecnología blockchain aplicados al sector salud, en especial aquellos protocolos nuevos que promueven una gestión de registros médicos electrónicos (EHR) con mayor eficacia, seguridad y rapidez. Algunos ofrecen paradigmas de intercambio de información clínica seguros respaldados por protección y privacidad de datos. Por ejemplo, en modelos mencionados anteriormente como EdgeMediChain y MediBlocks, EdgeMediChain incorpora la implementación de contratos inteligentes y establece políticas de control de acceso restringido proporcionando una plataforma segura y eficiente para la compartición de datos de salud entre diversas partes involucradas en el ámbito de la atención médica. Otro ejemplo de modelo es MediBlocks que opera a través de transacciones de escritura que actualizan el libro mayor distribuido en la red blockchain Fabric autorizada, que les permite controlar el acceso de acuerdo con roles mejorando la seguridad y privacidad en la gestión de EHR.

La indagación en criptografías de vanguardia, incluida la de curva elíptica usada en implementaciones de contratos inteligentes, proporciona un marco más seguro para el intercambio de registros médicos, protegiendo datos en algoritmos criptográficos avanzados que garantizan una seguridad superior. La criptografía de curva elíptica (ECC) utiliza conjuntos de claves públicas y privadas para cifrar y descifrar datos, generando claves matemáticamente más desafiantes de descifrar, considerada como la próxima generación en criptografía de clave pública debido a su mayor seguridad.

La investigación sobre la integración de blockchain con tecnologías emergentes, como la inteligencia artificial (IA) y el Internet de las Cosas Médicas (IoMT), es crucial. Estas sinergias prometen revolucionar la atención médica personalizada y la administración de datos, mejorando

el acceso a la información y la eficiencia en la entrega de servicios de salud. Respecto a la integración con IoMT, Indumathi et al., 2020 proponen una arquitectura integral basada en blockchain, Internet de las cosas médicas (IoMT), y almacenamiento en la nube para gestionar datos médicos, destacando la importancia de estas tecnologías emergentes en el futuro de la atención médica.

En la integración con IA, existen varios enfoques que hacen característico el entorno propuesto por Jennath et al., 2020, para el intercambio seguro de datos médicos mediante tecnología blockchain e inteligencia artificial descentralizada. En este enfoque, se clasifica la información del paciente y se almacena de manera personal y offline, con su hash vinculado a la cadena de bloques. Esto permite que el paciente tenga control sobre los datos compartidos.

Otro aspecto a considerar en momentos de implementación y planificación son los progresos en la adopción de estándares de interoperabilidad, como HL7 y FHIR, esenciales para promover un intercambio de información de salud eficaz. La evaluación de cómo la implementación de estos estándares en plataformas blockchain puede facilitar una mejor interoperabilidad entre sistemas de EHR distintos, asegurando un flujo de datos coherente y accesible.

Se recomienda no solo centrarse en la evaluación de tecnologías y modelos existentes sino también en la anticipación de futuras innovaciones en el campo de la salud digital. Esto incluye el monitoreo continuo de avances en criptografía, como la potencial aplicación de la criptografía cuántica para fortalecer aún más la seguridad de los datos en sistemas blockchain. Asimismo, es imperativo considerar el impacto de las regulaciones actuales y futuras en el desarrollo de nuevas tecnologías y protocolos, para asegurar que las soluciones propuestas permanezcan conformes y relevantes en un entorno regulador en constante evolución.

Estos factores darán base para una adopción exitosa de avances e innovaciones tecnológicas en la gestión de EHR con blockchain en las instituciones que prestan servicios de atención médica y por ende asegurará que el proyecto se mantenga a la vanguardia de las prácticas seguras, eficientes y centradas en el paciente en el ámbito de la salud digital.

6.3.2. Benchmarking de las prácticas actuales con las planteadas

La calidad de la atención médica está intrínsicamente ligada a la efectividad de los sistemas de registros médicos electrónicos (EHR) utilizados por los proveedores de salud. Para asegurar una gestión eficaz, segura y centrada en el paciente, hay aspectos fundamentales. Entre estos se puede encontrar la interoperabilidad presente en los diferentes hospitales o plataformas, asegurando que los datos sean accesibles y útiles a través de distintos entornos médicos. El almacenamiento de datos es también en cuanto a ubicación y método, para asegurar su disponibilidad. La seguridad de los datos hace referencia a las medidas implementadas para tener acceso a la información asegurando la confidencialidad y evitando posibles vulneraciones. La gestión de acceso, en donde, solo el personal autorizado y pacientes puedan acceder a los datos pertinentes. La comunicación con los pacientes abarca las herramientas y plataformas para el acceso de información e interacción con proveedores de salud. Finalmente, el cumplimiento normativo se refiere a la adhesión con las leyes y regulaciones relacionadas con la seguridad, manejo y privacidad de los EHR. Al comparar las prácticas convencionales con las que emplean blockchain, se analizan los modelos propuestos y se destacan los beneficios y limitaciones de ambas formas de gestión de EHR.

Aspecto	Prácticas Convencionales de EHR	Prácticas con Blockchain de EHR
Almacenamiento de Datos	Centralizado en servidores, lo que puede centralizar el riesgo de ataques. También pueden ser encontrados en la nube.	Descentralizado, distribuyendo la información a través de múltiples nodos para aumentar la seguridad y la resistencia.
Interoperabilidad	Limitada por la diversidad de sistemas y estándares, complicando el intercambio de datos.	Mejorada mediante el uso de estándares abiertos como HL7 y FHIR, y facilitada por la naturaleza interoperable del blockchain.
Seguridad de Datos	Protecciones basadas en contraseñas y encriptación estándar; vulnerable a ataques centralizados.	Mejorada con encriptación avanzada, inmutabilidad de los registros y control de acceso más sofisticado mediante claves criptográficas.
Gestión de Acceso	Gestión manual de permisos basada en roles, con riesgos inherentes a la administración centralizada.	Automatizada y personalizable a través de contratos inteligentes, proporcionando un control de acceso dinámico y seguro.
Comunicación con Pacientes	Portales de pacientes con funcionalidades limitadas para el acceso y la gestión de la información de salud.	Potencial para una participación más activa del paciente en su atención médica, con acceso seguro y controlado a sus datos de salud.
Cumplimiento Normativo	Adherencia a regulaciones como HIPAA y GDPR mediante políticas y procedimientos estándar.	Facilita el cumplimiento normativo a través de la trazabilidad y la auditoría inherentemente seguras, mejorando la gestión de consentimientos.

Tabla 2. *Benchmarking*

6.4. Planteamiento de la Integración de Blockchain y Cloud Computing

Para abordar la fusión de Blockchain y la Computación en la Nube en la administración de registros médicos electrónicos (EHR), es crucial examinar el modo en que estas tecnologías pueden fortalecer la protección, facilitar la interacción entre sistemas y optimizar el procesamiento de información sanitaria.

6.4.1. Diagrama de interacción

Es importante identificar las operaciones clave en la administración de EHR que se verán favorecidas por esta integración, tales como la recolección de información de salud, la conservación segura de datos, la posibilidad de acceder y compartir expedientes médicos.

6.4.1.1. Procesos.

- Procesos Administrativos

- **Registro de Pacientes:** Ingreso de información personal y médica de nuevos pacientes en el sistema.
- **Agendamiento de Citas:** Programación de citas médicas, incluyendo consultas iniciales y de seguimiento.
- **Facturación y Procesamiento de Pagos:** Generación de facturas por servicios médicos y gestión de pagos.
- **Gestión de Consentimientos:** Obtención y gestión del consentimiento del paciente para tratamientos y para compartir información médica. Este proceso también pertenece a cumplimiento y regulación.

- Procesos Clínicos

- **Acceso a Historiales Médicos:** Consulta de historiales médicos por parte del personal médico para revisión o actualización.
- **Gestión de Prescripciones Médicas:** Emisión, actualización y revisión de prescripciones médicas.
- **Procesamiento de Órdenes Médicas:** Gestión de órdenes para pruebas diagnósticas, procedimientos, etc.

- **Monitoreo de la Salud del Paciente:** Seguimiento de indicadores de salud a través de dispositivos conectados o entradas manuales.

- Procesos de Soporte Técnico y Seguridad
- **Interoperabilidad y Compartición de Datos:** Intercambio de información médica con otros sistemas de EHR o instituciones médicas.
- **Reportes de Salud y Análisis de Datos:** Generación de reportes de salud para pacientes o análisis estadístico de datos para investigación.

6.4.1.2. Actores Potenciales. Se identifica los actores junto a sus responsabilidades y sus roles dentro del sistema de EHR para poder relacionar todo el flujo de trabajo dentro del sistema.

- **Pacientes:** Usuarios finales del sistema de EHR y propietario de los datos.
- Responsabilidades: Proporcionar información personal y de salud precisa y gestionar el consentimiento para compartir datos a través de interfaces seguras.
- Rol: Titulares de los datos y beneficiarios de los servicios de salud

- **Profesionales de la Salud:** Incluyen médicos, enfermeras, y especialistas.
- Responsabilidades: Acceder y actualizar los registros médicos para el cuidado del paciente y utilizar datos de salud de manera ética y conforme a las normativas.
- Rol: Proveedores de cuidados médicos y usuarios principales de los registros médicos para diagnóstico y tratamiento.

- **Administradores de EHR:** Responsables de la gestión y mantenimiento del sistema EHR.
  - Responsabilidades: Mantener la infraestructura del sistema EHR, incluida la integración con blockchain y cloud computing y asegurar la privacidad, seguridad y accesibilidad de los datos de salud.
  - Rol: Custodios del sistema EHR, garantizando su operación eficiente y segura.

- **Proveedores de Tecnología Blockchain:** Especialistas en blockchain que implementan y mantienen la infraestructura blockchain.
  - Responsabilidades: Implementar soluciones de blockchain que refuercen la seguridad y la trazabilidad de los datos e innovar en el uso de contratos inteligentes para la automatización de procesos.
  - Rol: Innovadores y soportes técnicos para la capa de blockchain, asegurando integridad y seguridad de datos.

- **Proveedores de Servicios de Cloud Computing:** Empresas que ofrecen soluciones de almacenamiento y computación en la nube.
  - Responsabilidades: Ofrecer soluciones escalables y seguras para el almacenamiento y procesamiento de datos, garantizar altos niveles de disponibilidad y recuperación ante desastres.
  - Rol: Socios en infraestructura, ofreciendo escalabilidad, disponibilidad y almacenamiento de datos.

- **Reguladores de Salud:** Entidades gubernamentales o independientes que regulan la privacidad y seguridad de los datos de salud.
  - Responsabilidades: Establecer y hacer cumplir regulaciones sobre privacidad, seguridad y uso de datos de salud, supervisar la implementación de tecnologías emergentes en el sector salud.
  - Rol: Vigilantes del cumplimiento de normativas, protegiendo los derechos de los pacientes y la integridad del sistema de salud.

- **Desarrolladores de Software:** Encargados de crear y mantener las aplicaciones y herramientas del sistema EHR.
  - Responsabilidades: Desarrollar y mantener aplicaciones que mejoren la experiencia de usuario y la eficiencia del sistema, integrar nuevas tecnologías, como blockchain y cloud computing, en el ecosistema del EHR.
  - Rol: Creadores de las soluciones digitales, facilitando la interacción entre usuarios, datos y tecnologías.

- **Terceros Autorizados (Aseguradoras, Otros Hospitales):** Entidades que necesitan acceder a los registros de salud de los pacientes para procesar reclamaciones, referencias o para la continuidad de la atención médica.

6.4.1.3. Mapeo de Interacciones. Se mapea cómo los actores interactúan entre sí y con el sistema EHR, considerando los roles y responsabilidades definidos. Esto incluye el intercambio de datos, la solicitud de servicios y cualquier otra forma de colaboración.

Tras identificar previamente los procesos clave, se determina cómo los actores interactúan con el sistema o entre sí. Estas interacciones pueden ser, por ejemplo, un médico accediendo a los registros de un paciente, lo que sería una interacción directa; en cuanto a interacciones indirectas, un ejemplo es cuando un paciente da consentimiento para compartir sus datos, afectando la disponibilidad de dichos datos para el personal médico. Esto permite conocer las acciones que se ejecutan en cada punto de interacción y posteriormente, establecer un flujo de datos y de trabajo.

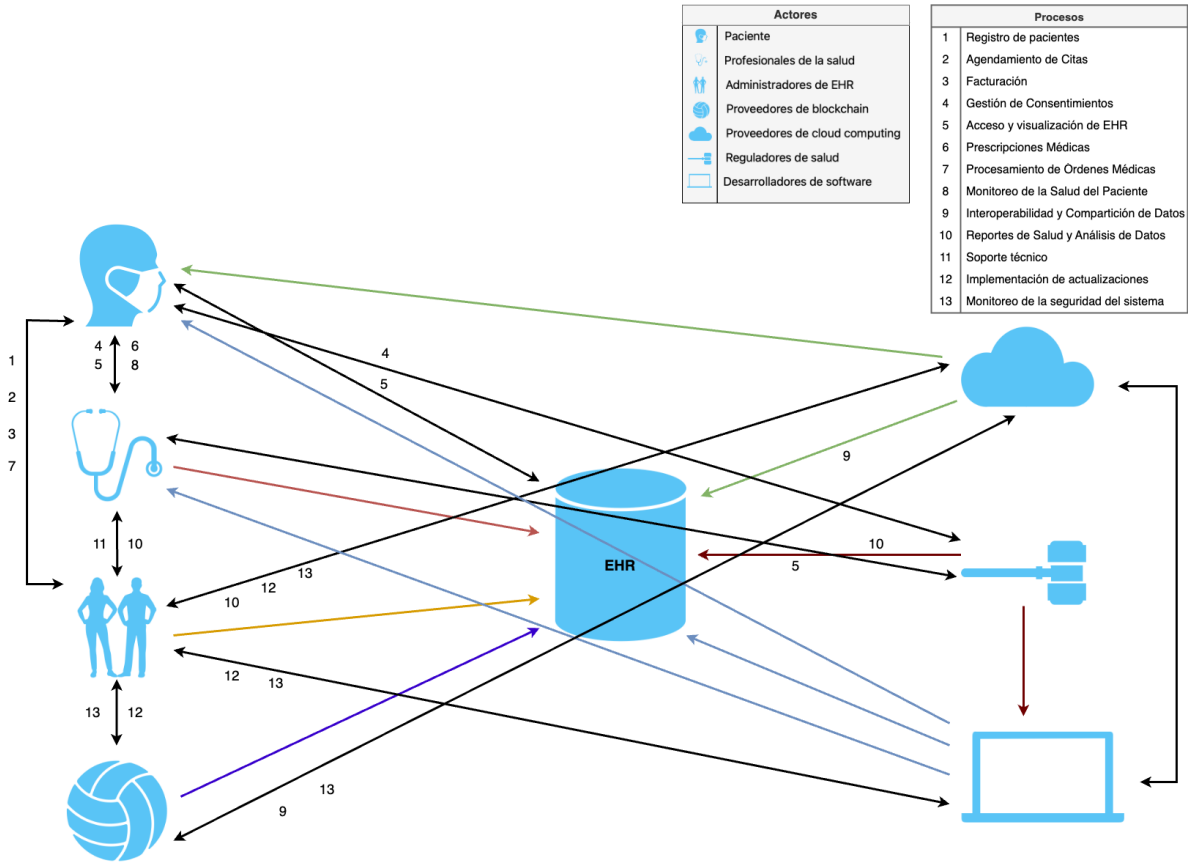

Figura 7. *Representación gráfica de interacciones.*

6.4.1.4 Seguridad y privacidad. La adopción de la criptografía de curva elíptica (ECC) en la gestión de Registros Electrónicos de Salud (EHR) mediante la integración de tecnologías de blockchain y cloud computing marca un avance significativo en la protección de datos

almacenados y en tránsito. La ECC ofrece un enfoque eficiente y seguro para el cifrado de datos, crucial para la protección de información sensible en el sector salud. Su implementación en contratos inteligentes facilita la gestión de consentimientos, la verificación de identidad, y la autorización de acceso, así como la automatización de procesos administrativos y clínicos, integrando y compartiendo datos de manera segura entre entidades. Este enfoque no solo mejora la seguridad de los datos, sino que también optimiza la eficiencia operativa, respetando las estrictas regulaciones de privacidad como HIPAA.

La gestión de identidades y accesos, crucial en el contexto de EHR, se refuerza con la implementación de Multi-Factor Authentication (MFA) y Role-Based Access Control (RBAC), asegurando que solo el personal autorizado tenga acceso a los datos. El uso de Decentralized Identifiers (DID) mejora la gestión de identidades, mientras que la k-anonimización se emplea para la visualización de la protección de la privacidad, manteniendo la utilidad de los datos sin comprometer la identidad del individuo. Estas medidas colectivas proporcionan un marco robusto para la seguridad y privacidad de EHR, abordando desafíos contemporáneos en la gestión de información de salud.

La integración de cloud computing y blockchain para la gestión de registros electrónicos de salud (EHR) se optimiza mediante el modelo de Blockchain-as-a-Service (BaaS) con Tolerancia a Fallos Bizantinos (BFT), uniendo la escalabilidad y flexibilidad de la nube con la robustez y transparencia del blockchain. Además, la arquitectura BFT puede configurarse para ser menos costosa en términos de consumo de recursos que otros mecanismos de consenso, como la Prueba de Trabajo (PoW), lo que la hace ideal para aplicaciones en cloud computing. BaaS facilita a las instituciones de salud la adopción de blockchain reduciendo costos y complejidad operativa, mientras que BFT ofrece un mecanismo de consenso seguro y eficiente, incluso frente a nodos

maliciosos, ideal para entornos con confianza limitada entre participantes. Este modelo asegura una gestión segura y eficiente de EHR, permitiendo acceso confiable y auditabilidad completa de registros médicos en cualquier momento y lugar, contribuyendo a un sistema de salud más seguro y eficiente.

Para la implementación de una solución de registros electrónicos de salud (EHR) que integre las tecnologías de blockchain y cloud computing, se recomienda una sinergia entre Amazon Web Services (AWS) y Hyperledger Fabric. AWS, líder en servicios de cloud computing, ofrece una infraestructura escalable, robusta y segura, capaz de adaptarse a las variadas demandas de los sistemas de salud. Esta plataforma no solo garantiza la elasticidad y la escalabilidad necesarias para manejar grandes volúmenes de datos de salud, sino que también proporciona herramientas avanzadas para la gestión de la seguridad y el cumplimiento de normativas críticas como la HIPAA. Mediante el uso de AWS Blockchain Templates, se facilita la implementación y configuración de redes blockchain, permitiendo a las instituciones de salud concentrarse en la innovación y mejora de los servicios sin la carga operativa de gestionar la infraestructura subyacente.

Por otro lado, Hyperledger Fabric se presenta como la plataforma de blockchain ideal para el contexto de los EHR, destacando por su enfoque en la privacidad y confidencialidad de las transacciones, un requisito indispensable para el manejo de información sensible en el sector salud. Su arquitectura permite la creación de canales privados y la ejecución de contratos inteligentes (smart contracts) para una gestión segura y eficiente de los accesos a los datos. Además, Hyperledger Fabric es conocido por su rendimiento, escalabilidad y flexibilidad en el mecanismo de consenso, incluyendo la posibilidad de implementar Tolerancia a Fallos Bizantinos (BFT) para entornos donde la seguridad es crítica. La combinación de AWS y Hyperledger Fabric ofrece una

solución integral que no solo cumple con los requisitos de seguridad y privacidad, sino que también es capaz de escalar y adaptarse a las necesidades futuras del sector de la salud, promoviendo así un sistema de EHR más seguro, eficiente y conforme a las regulaciones.

6.4.1.5 Flujo de datos. El sistema de EHR recopila datos de diversas fuentes, incluyendo registros de pacientes, historiales clínicos, resultados de laboratorio, y datos de dispositivos médicos conectados. Estos datos se generan tanto en entornos clínicos a través de dispositivos de salud. La integridad y la precisión en la generación de datos son fundamentales para el diagnóstico, tratamiento, y seguimiento de pacientes. Hyperledger Fabric facilita la recopilación y el registro de estos datos en la blockchain, asegurando su inmutabilidad y trazabilidad desde el punto de origen.

Antes de su transmisión o almacenamiento, todos los datos son cifrados utilizando tecnologías de cifrado avanzadas, como la criptografía de curva elíptica (ECC), para proteger la privacidad de los pacientes y cumplir con regulaciones como HIPAA. Este proceso de cifrado inicial se aplica tanto a los datos en reposo como en tránsito, asegurando que la información sensible esté protegida contra accesos no autorizados. La gestión de claves de cifrado se realiza mediante Hyperledger Fabric, que ofrece un sistema de permisos y accesos basado en roles, garantizando que solo los usuarios autorizados, como profesionales de salud y pacientes, puedan acceder a la información desencriptada mediante claves privadas seguras.

Una vez cifrados, los datos se transmiten de manera segura a la infraestructura de cloud computing proporcionada por AWS, utilizando protocolos de comunicación seguros como TLS/SSL, que añaden una capa adicional de seguridad durante la transmisión. En AWS, los datos cifrados se almacenan en servicios como Amazon S3, que ofrece robustas capas de seguridad

adicionales, incluyendo controles de acceso detallados, cifrado en el lado del servidor y capacidades de monitoreo para detectar y responder a amenazas de seguridad en tiempo real. La arquitectura de AWS, en combinación con Hyperledger Fabric, proporciona un entorno seguro y escalable para el almacenamiento y gestión de EHR, facilitando el acceso controlado a los datos y su integración con aplicaciones de salud, mientras se mantienen altos estándares de seguridad y privacidad.

Una vez que los datos de los registros electrónicos de salud (EHR) han sido cifrados y almacenados de manera segura en la nube utilizando Amazon S3, el siguiente paso crucial es garantizar su integridad a largo plazo y la trazabilidad de acceso mediante su registro en una blockchain, específicamente utilizando Hyperledger Fabric. Este proceso se realiza de la siguiente manera:

Integridad de Datos: Para cada conjunto de datos almacenados, se genera un resumen criptográfico (hash) único, que se registra en la blockchain de Hyperledger Fabric. Este hash actúa como una huella digital de los datos, garantizando su integridad y no repudio, ya que cualquier alteración en los datos originales resultaría en un hash diferente. Este método asegura la integridad de los datos sin necesidad de exponer la información sensible contenida en los EHR.

Acceso a Datos: El acceso o la compartición de los datos almacenados se maneja a través de contratos inteligentes en Hyperledger Fabric. Estos contratos inteligentes permiten establecer reglas detalladas sobre quién puede acceder a los datos, bajo qué condiciones y registran cada acceso o transacción en la blockchain. Esto proporciona una auditabilidad completa y trazabilidad del acceso a los datos, garantizando la seguridad y cumpliendo con las regulaciones de privacidad de datos como HIPAA.

Para el flujo de datos se tiene en cuenta los siguientes aspectos:

- Generación de Datos: Los datos se generan en diversos puntos de atención médica.
- Cifrado de Datos: Antes de la transmisión, los datos son cifrados para proteger su privacidad.
- Transmisión Segura: Los datos cifrados se transmiten de manera segura a AWS.
- Almacenamiento en la Nube: Los datos cifrados se almacenan en Amazon S3.
- Registro en Blockchain: Se genera un hash de los datos y se registra en Hyperledger Fabric.
- Acceso y Compartición de Datos: A través de contratos inteligentes, se gestiona el acceso a los datos.

Puntos de Control Clave:

- En la Generación de Datos: Verificación de la autenticidad de la fuente de datos.
- Antes y Después del Cifrado de Datos: Verificación de la eficacia del cifrado.
- Durante la Transmisión Segura: Comprobaciones de la seguridad de la transmisión.
- Al Almacenar en la Nube: Revisión de políticas de seguridad y acceso de AWS S3.
- En el Registro en Blockchain: Confirmación del registro exitoso del hash y la inmutabilidad de los datos.
- Al Acceder o Compartir Datos: Auditoría de los accesos y transacciones registrados por los contratos inteligentes.

La disponibilidad continua de los datos de los registros electrónicos de salud (EHR) es fundamental para garantizar que los profesionales de la salud tengan acceso a la información crítica del paciente cuando la necesiten, especialmente en situaciones de emergencia. Para asegurar esta

disponibilidad y resistencia ante fallos, se adoptan las siguientes estrategias en la infraestructura de cloud computing proporcionada por Amazon Web Services (AWS):

Replicación de Datos: AWS permite la replicación automática de los datos almacenados en Amazon S3 a múltiples ubicaciones geográficamente distribuidas. Esta replicación garantiza que, incluso en el caso de una falla o interrupción en una región específica, los datos permanezcan accesibles desde otras ubicaciones, minimizando así el riesgo de pérdida de datos y maximizando su disponibilidad.

Recuperación ante Desastres: AWS ofrece soluciones integradas de recuperación ante desastres que permiten restaurar rápidamente los datos y las aplicaciones en caso de incidentes. Esto incluye la capacidad de crear y gestionar copias de seguridad de los datos en S3, así como la implementación de estrategias de failover automatizadas que pueden activarse en respuesta a fallos detectados, asegurando la continuidad del acceso a la información de salud sin interrupciones significativas.

6.4.2. Modelado de la Integración de Blockchain y Cloud Computing

Se organiza el diagrama en capas para diferenciar entre la interfaz de usuario, procesamiento lógico, almacenamiento de datos, nombrando cada componente y posteriormente relacionándolos con flechas para mostrar el flujo del sistema.

6.4.2.1. Arquitectura del sistema. Lo primero para tener en cuenta es obtener el permiso para acceder al EHR. Dependiendo del usuario, este deberá solicitar el acceso a la información requerida por medio del DID para obtener la autenticación inicial. Seguidamente, durante el proceso Multi-Factor Authentication (MFA), el sistema de autenticación solicita un segundo factor

como la huella dactilar o reconocimiento facial. Tras las verificaciones anteriores y, tras confirmarse la identidad del usuario, se procede al Control de Acceso Basado en Roles (RBAC) que permite asignar permisos y accesos específicos a los usuarios según su rol dentro de la organización o el sistema. Es el API Gateway el encargado de otorgar al usuario un token de acceso. Con este token, el usuario incluye en el encabezado de las solicitudes subsecuentes al API Gateway, el cual valida el token y permite el acceso a los recursos protegidos según las políticas de acceso establecidas.

Los componentes de la arquitectura del sistema son Aplicaciones de Usuarios Finales que representa aplicaciones móviles o web a través de las cuales los pacientes y proveedores acceden al sistema; API Gateway que actúa como intermediario entre las aplicaciones de usuario y el backend; contratos inteligentes (Hyperledger Fabric) que es donde se ejecuta la verificación de credenciales de acuerdo a los roles, políticas de acceso y el consentimiento otorgado, almacenamiento en la Nube (AWS S3) que es la plataforma en la nube en la que se guardaran los EHR cifrados con ECC, y la plataforma blockchain que se va usar es Hyperledger Fabric que es donde se ejecutaran los contratos inteligentes y también donde almacena los hashes de datos y el registro de acceso.

Se tienen distintas conexiones como, por ejemplo, entre la capa de Interfaz de Usuario y el Procesamiento Lógico con conexión entre API Gateway y Aplicaciones de Usuarios Finales, esta comunicación es bidireccional ya que las aplicaciones envían solicitudes al servidor (por ejemplo, solicitud de acceso a datos de salud, actualizaciones de información del paciente) y reciben respuestas (datos solicitados, confirmaciones de acciones realizadas).

Con respecto a la conexión API Gateway y Almacenamiento en la nube (AWS S3) se considera que los datos se almacenan en la nube y se recuperan de ella según las solicitudes de los usuarios.

La interacción con la infraestructura blockchain se pueden formar conexiones por ejemplo entre API Gateway/Servicios de Autenticación y Blockchain, aunque el registro en la blockchain es principalmente unidireccional (por ejemplo, registrar hashes de datos para garantizar la integridad), la verificación de identidad y la autorización de accesos implican una consulta a la blockchain para validar permisos, lo que justifica una flecha de doble sentido en conexiones que implican verificación o consultas de estado en la blockchain.

En la arquitectura planteada hay que tener en cuenta que la conexión entre Hyperledger Fabric y Amazon S3 es indirecta y se justifica por la necesidad de vincular la información inmutable almacenada en la blockchain con los datos cifrados almacenados en la nube. La conexión es indirecta porque cuando los EHR se almacenan en AWS S3, se genera un hash criptográfico de estos datos utilizando, por ejemplo, ECC como es en este caso. El hash no contiene información de salud sensible y es único para el conjunto de datos que representa, posteriormente el hash se graba en la blockchain de Hyperledger Fabric. Por lo cual este proceso no requiere una transferencia de datos directa entre S3 y Hyperledger. Esto es beneficioso para procesos de auditoría y verificación de la integridad de los datos almacenados en S3 ya que el sistema puede recuperar el hash correspondiente de Hyperledger Fabric y compararlo con un hash recién generado de los datos actuales en S3. Si los hashes coinciden, los datos no han sido alterados desde que se almacenaron por última vez. De esta manera, se muestra como esta vinculación no constituye una conexión directa de datos, es más bien un proceso de validación teniendo en cuenta que AWS S3 maneja los datos de los EHR en su forma cifrada, que son grandes conjuntos de datos.

Hyperledger Fabric maneja representaciones criptográficas de estos datos (hashes) y lógica de control de acceso, que son mucho más pequeños en tamaño y diferentes en naturaleza. Se cumple con principios de seguridad que son relevantes en el cuidado de la salud debido a la gran cantidad de datos sensibles que se manejan en el sector salud, debido a que Hyperledger Fabric no necesita acceder directamente a los EHR para realizar sus funciones; solo requiere los hashes y los metadatos asociados con esos EHR manteniendo la trazabilidad y transparencia que exigen distintas regulaciones como el HIPAA.

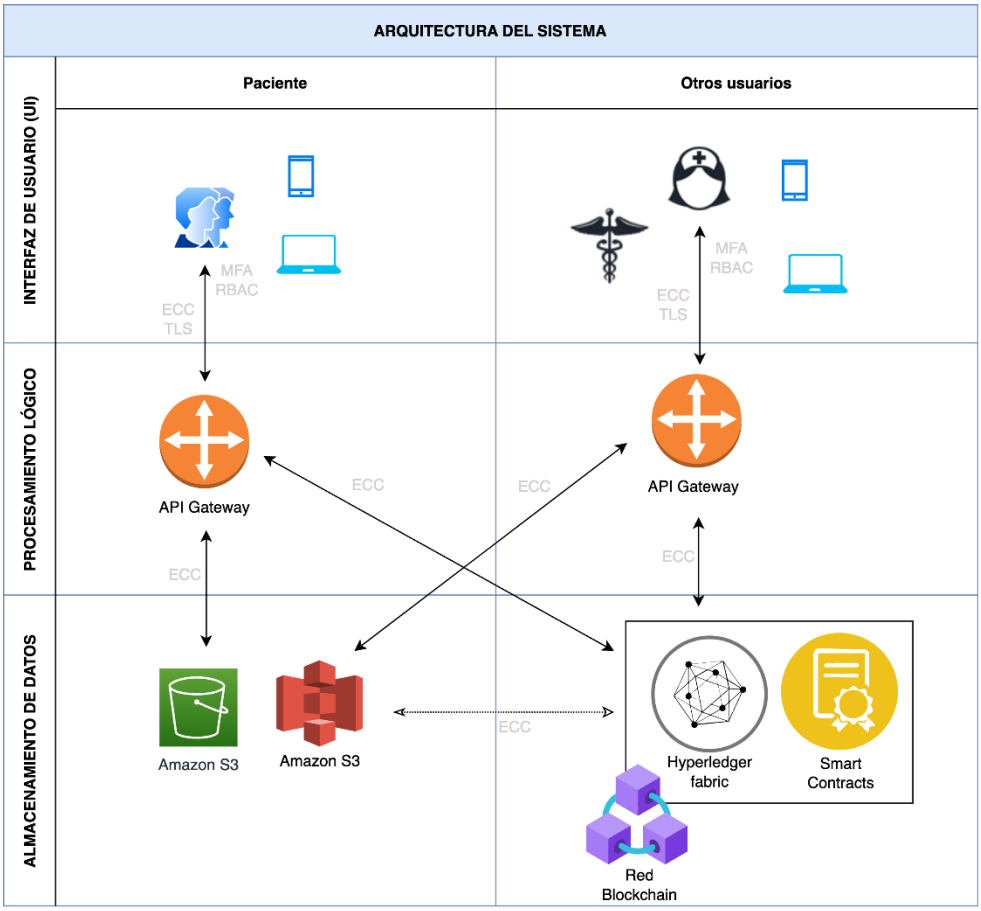

Figura 8. *Arquitectura del sistema.*

6.4.2.2. Gestión de identidades. La adopción de identificadores descentralizados (DIDs) surge como un mecanismo clave para reforzar la autenticación y la autorización de accesos dentro

de la infraestructura propuesta. Este enfoque permite a los usuarios una gestión autónoma de sus credenciales digitales, potenciando la privacidad y el control sobre sus datos personales. DIDs, implementados en la blockchain de Hyperledger Fabric, ofrecen una solución resistente a la centralización y a puntos únicos de fallo, crucial para proteger la identidad digital en el ecosistema de la salud. Se implementa soluciones de autenticación multifactor (MFA) que proporciona una capa adicional de seguridad, junto con auditorías regulares y la formación de tanto usuarios como administradores aseguran la integridad y el correcto funcionamiento del sistema. Además, se realiza la integración del control de acceso basado en roles (RBAC) para definir permisos de manera granular, garantizando que los usuarios accedan solo a la información que su rol les permite, en conformidad con regulaciones como la HIPAA.

6.4.2.3. Interoperabilidad de datos. En el modelo desarrollado, se adoptaron estándares reconocidos, como Health Level 7 (HL7) Fast Healthcare Interoperability Resources (FHIR), como fundamentos críticos, facilitando el intercambio de datos de manera eficiente y en conformidad con las mejores prácticas internacionales. Mediante la implementación de interfaces de programación de aplicaciones (APIs) detalladamente especificadas, el sistema asegura la compatibilidad y la comunicación efectiva entre la infraestructura de blockchain de Hyperledger Fabric y los servicios en la nube de Amazon S3, así como con otros sistemas de EHR existentes. Estas APIs soportarán operaciones esenciales como la consulta de registros, la actualización de datos de pacientes y la interacción segura entre sistemas, garantizando así un enfoque estructurado y sin ambigüedades para la interoperabilidad. Esta metodología no solo garantiza el acceso a información médica completa y actualizada por parte de los proveedores de atención médica, sino que también asegura la coherencia y la seguridad de los datos a través de todo el ecosistema de

salud. La interoperabilidad, implementada en este sistema, eleva significativamente la calidad de la atención al paciente, permitiendo a los profesionales de la salud tomar decisiones más informadas y gestionar los registros de salud eficazmente.

6.4.2.4. Smart Contracts para la automatización. En este proyecto, la implementación de contratos inteligentes resulta sumamente beneficiosa, proporcionando una mejora significativa en seguridad, eficiencia y gestión de consentimientos. Esta tecnología se aprovecha de diversas maneras:

Gestión de consentimientos: automatizando la gestión de consentimientos de forma segura y transparente. Esto no solo garantiza el cumplimiento de regulaciones importantes como HIPAA o GDPR, sino que también simplifica la verificación de identidad y autorización de acceso. Con ello, únicamente el personal médico autorizado tiene acceso a registros específicos, fortaleciendo así la protección de los datos del paciente.

Automatización de procesos administrativos y clínicos: Los contratos inteligentes desempeñan un papel clave en la reducción de errores y la agilización de los flujos de trabajo dentro de los entornos de atención médica. Mejorando la calidad de la atención al paciente al permitir que el personal médico se concentre más en el cuidado del paciente.

Integración y compartición segura de datos: A través de la transparencia y trazabilidad que ofrece la tecnología blockchain, facilitando la integración y compartición de datos entre diferentes entidades de manera segura.

Registro y auditoría de actividades: permite mantener un registro inmutable de todas las acciones realizadas en los registros médicos. Este registro facilita enormemente las auditorías,

ayudando en el cumplimiento normativo y mejora la seguridad del paciente, al proporcionar una evidencia irrefutable de las operaciones realizadas.

Además, este proyecto considera la seguridad de la información como una prioridad absoluta. Aunque se reconoce que ningún sistema es completamente invulnerable, la adopción de contratos inteligentes y el cifrado ECC son fundamentales para minimizar los riesgos, incluyendo aquellos derivados de errores humanos o configuraciones incorrectas. Estas medidas de seguridad están diseñadas para proteger contra el acceso no autorizado a los datos, garantizando así la integridad y confidencialidad de la información del paciente.

6.4.2.5. Monitoreo y auditoría. Para el seguimiento integral de las transacciones y accesos a los registros médicos, se emplearán Amazon CloudWatch y AWS CloudTrail. Estas plataformas se usarán en conjunto con el Explorador de Blockchain de Hyperledger Fabric, una herramienta que proporciona visualización y seguimiento de transacciones, bloques, y otros elementos relevantes dentro de la red de blockchain. Esta combinación de herramientas ofrece una visibilidad completa del sistema, generando alertas automáticas frente a actividades inusuales para propiciar una intervención temprana ante amenazas.

Respecto a las auditorías, se establecen intervalos regulares de tres meses para la revisión sistemática de los registros de transacciones y accesos, complementados por auditorías ad hoc en caso de detectarse actividades sospechosas o como respuesta a solicitudes de partes interesadas externas. La autoridad para llevar a cabo estas auditorías recae en un equipo interno de auditoría de seguridad de la información, reforzado por auditorías externas anuales para garantizar una evaluación imparcial y conforme a estándares de la industria. Las políticas de auditoría detallarán un proceso estructurado para el manejo y resolución de hallazgos, que incluye la clasificación de

los hallazgos según su gravedad, la asignación de responsabilidades para la corrección de deficiencias y la implementación de medidas correctivas. Se establece un plazo máximo de 30 días para la resolución de hallazgos críticos, con un seguimiento continuo hasta su completa mitigación.

Para mantener el sistema alineado con las prácticas de seguridad más actuales y las regulaciones vigentes, se implementará un mecanismo de revisión periódica de las políticas de auditoría y seguridad. El mecanismo contempla revisiones semestrales del comité de seguridad de la información, que evaluará las políticas actuales según las últimas tendencias en ciberseguridad y cambios en la legislación relevante, como la HIPAA, adaptando el marco de seguridad del sistema si es necesario.

La implementación de estas herramientas y políticas específicas dentro del modelo propuesto demuestra un enfoque comprometido con la integridad, seguridad y cumplimiento de la gestión de EHR, a través de la integración efectiva de tecnologías de blockchain y cloud computing.

6.5. Análisis de la Gestión del Riesgo

Los riesgos asociados con la integración de tecnologías de blockchain y cloud computing en la gestión de registros electrónicos de salud (EHR) debe ser evaluado y gestionado. Esta valoración es fundamental para identificar y mitigar posibles amenazas que puedan afectar la seguridad, privacidad e integridad de los datos sensibles de salud. Este análisis exhaustivo es esencial para garantizar la resiliencia del sistema frente a diversas vulnerabilidades y para asegurar el cumplimiento continuo con regulaciones. Mediante un enfoque estructurado que incluya la identificación de riesgos potenciales y la evaluación de su impacto, demostrando un compromiso con la protección de la información de salud. Esto subraya la importancia de una gestión de riesgos

proactiva en el desarrollo e implementación de soluciones tecnológicas avanzadas en el ámbito de la salud.

6.5.1. Identificación de riesgos potenciales y Evaluación de impacto

En la integración de blockchain y cloud computing para la gestión de EHR, es fundamental un análisis meticuloso de los riesgos y sus impactos asociados para asegurar un entorno seguro y confiable. A continuación, se presentan los riesgos potenciales identificados junto con sus respectivos impactos:

1. Errores de Configuración:
    - Riesgo: Configuraciones inadecuadas de permisos en AWS S3 o en la blockchain podrían exponer datos sensibles.
    - Impacto: La exposición de datos compromete la privacidad del paciente y puede resultar en violaciones de regulaciones como HIPAA, afectando la reputación y la confianza en el sistema.
2. Vulnerabilidades en el Software:
    - Riesgo: Software no actualizado o con defectos de diseño podría ser explotado para acceder o alterar datos de manera no autorizada.
    - Impacto: Compromete la integridad y disponibilidad de los EHR, afectando la calidad de la atención al paciente y la operatividad del sistema.
3. Gestión Inadecuada de Claves Criptográficas:
    - Riesgo: Pérdida o mal manejo de claves de cifrado ECC puede resultar en la inaccesibilidad de los datos.

- Impacto: La pérdida de acceso a datos críticos de salud puede tener consecuencias directas en la continuidad y calidad del cuidado del paciente.

4. Interoperabilidad Limitada:
    - Riesgo: Fallos en la interoperabilidad con otros sistemas de EHR pueden generar aislamiento de datos.
    - Impacto: Limita la eficacia de la atención médica al impedir el acceso completo y oportuno a los historiales de salud de los pacientes.
5. Errores de Usuarios:
    - Riesgo: Errores en la entrada de datos por parte de los usuarios o en la interpretación de la información suministrada por el sistema.
    - Impacto: Puede llevar a decisiones clínicas basadas en información incorrecta, poniendo en riesgo la salud del paciente.
6. Incumplimiento Normativo:
    - Riesgo: Falta de conformidad con regulaciones legales y estándares de la industria.
    - Impacto: Riesgo de sanciones legales, pérdida financiera y daño a la reputación de la entidad gestora.
7. Brechas de Seguridad en la Transmisión de Datos:
    - Riesgo: Intercepción de datos sensibles durante su transmisión entre la nube y los clientes debido a protocolos de seguridad inadecuados.
    - Impacto: La exposición de datos sensibles podría resultar en la explotación de la información personal y financiera del paciente.
8. Fallas de Infraestructura en la Nube:

- Riesgo: Interrupciones del servicio o pérdida de datos debido a fallos técnicos o desastres naturales que afectan a los centros de datos de la nube.
- Impacto: Interrupción del acceso a los EHR, afectando la operatividad del sistema de salud y la toma de decisiones médicas.

Para mitigar estos riesgos, se propone implementar estrategias de seguridad en varios niveles, incluyendo actualizar y mantener el software, políticas estrictas de gestión de claves criptográficas, fomentar la educación de usuarios en prácticas seguras y adoptar un marco robusto de cumplimiento normativo. Además, se enfatiza la importancia de realizar auditorías de seguridad regulares y de desarrollar un plan de respuesta ante incidentes para minimizar el impacto de cualquier brecha de seguridad.

6.6. Análisis de Mejoras y Cuantificación de Beneficios

6.6.1. Identificación de métricas claves

6.6.1.1. Rendimiento del sistema. Las métricas a considerar dentro de un modelo de registros médicos electrónicos abarca múltiples factores a tener en cuenta, como el rendimiento del sistema del modelo implementado. Entre estas, se pueden encontrar: la latencia, que registra el tiempo transcurrido entre la emisión de una solicitud hasta su confirmación (IONOS, 2023); el throughput, que cuantifica la capacidad de procesamiento del sistema mediante el análisis de la cantidad de transacciones gestionadas en un intervalo de tiempo determinado que puede ser expresado como el rendimiento en transacciones por segundo (TPS), el número máximo de transacciones que el sistema puede procesar por segundo siendo crucial para evaluar el comportamiento del sistema bajo cargas de trabajo variables (CoinMarketCap, 2023); el uso de

recursos computacionales, que evalúa la eficiencia en la utilización de los recursos disponibles; y la escalabilidad, que aborda la capacidad del sistema para adaptarse y gestionar una mayor carga de trabajo sin comprometer su funcionamiento (Academy, 2023). Estas métricas son esenciales para comprender a fondo el desempeño operativo del blockchain y son imperativas para orientar las estrategias de optimización y mejora continua del sistema.

6.6.1.2. Métricas de sostenibilidad. La sostenibilidad es un factor importante ya que se requiere mantener un equilibrio con los recursos del entorno, por lo que se hace recomendable tener en cuenta varias métricas al respecto como el consumo de gas que es una unidad de medida de la cantidad requerida de esfuerzo computacional para ejecutar operaciones en una red blockchain. El gas es relevante porque limita el uso de recursos por lo cual asegura que cada operación ejecutada en la red tenga un costo asociado dando prioridad a las tarifas de gas más alta, y el costo previene el abuso de recursos computacionales y ataques de denegación de servicios (DoS). Las tarifas de gas son un pago para mantener la red segura y funcional para los validadores o mineros que procesan y aseguran las transacciones. Cabe aclarar que no todas las blockchains tienen el término de gas, se ve en blockchains como Ethereum, que requieren cuantificar y limitar el trabajo realizado por la red, esto no se verá en blockchains que no soportan operaciones complejas como Smart contracts y si no está contemplado en su mecanismo de consenso. Ethereum que es la más usada tiene el concepto de gas para manejar y limitar los recursos de la red, también por su enfoque en complejidad computacional variable como lo son las aplicaciones descentralizadas (dApps) y Smart contracts. Algunas plataformas que soportan contratos inteligentes utilizan modelos alternativos para gestionar los recursos computacionales como tasas fijas, staking o cuotas prepagas. Otra métrica a tener en cuenta para la sostenibilidad es el consumo

de energía que tenga el sistema incluso a gran escala, las blockchains tienen diferentes requisitos y perfiles de consumo de energía, esencialmente debido a sus mecanismos de consenso y las operaciones que toleran. Es valioso tener esta métrica en cuenta debido a la sostenibilidad ambiental en especial si la energía proviene de fuentes no renovables, el consumo de energía también puede ser limitante para la escalabilidad de una red blockchain ya que al poder escalar una red permitiría tolerar más usuarios y transacciones, pero solo si se cuenta con una red eficiente energéticamente se haría esto sin incurrir en impactos ambientales o costos muy elevados. El consumo de energía varía significativamente entre blockchains esencialmente por su mecanismo de consenso, blockchains como Bitcoin tienden a tener un alto consumo de energía ya que requiere que los mineros realicen complejos cálculos computacionales para validar transacciones y crear nuevos bloques usando el mecanismo de consenso Prueba de trabajo (PoW), a diferencia de Prueba de participación (PoS) y otros mecanismos como Prueba de autoridad (PoA) o Prueba de participación delegada (DPoS) que generalmente tienen un consumo de energía mucho más bajo, ya que no solicitan la misma cantidad de cálculos computacionales intensivos (Monleón, 2022).

Para comparar y medir el consumo de energía hay que considerar que el consumo de energía se mide en kilovatios-hora (kWh) y se calcula según la eficiencia energética del hardware utilizado para la minería o la validación de transacciones, así como del total de operaciones realizadas por la red o la tasa hash de la red (cantidad de cálculos de hash por segundo) o por la eficiencia energética del hardware, que sería la cantidad de electricidad para hacer cálculos de hash. Si la blockchain no utiliza PoW, el consumo de energía se asimila más con el mantenimiento de la red y las operaciones de los nodos, teóricamente el consumo de energía en estas redes es mucho más bajo y se enfocan en hardware de servidor estándar y la infraestructura de red necesaria para operar los nodos y ejecutar las transacciones. La reducción del consumo de energía en las

blockchains son áreas activas de investigación y desarrollo para tener la sostenibilidad ambiental con seguridad y funcionalidad de la red. Otras métricas que podrían acompañar para medir la sostenibilidad de la red es el tamaño de los bloques de transacción, eficiencia y confiabilidad (Sedlmeir et Al. 2020).

6.6.1.3. Métricas de gestión de identidades. Otra categoría importante, con métricas a considerar, es la gestión de identidades, que incluye factores como el control de acceso. Esto se refiere a las políticas y pautas establecidas para regular cómo cada usuario interactúa con ciertos datos e información, lo cual contribuye a mejoras en aspectos regulatorios, seguridad, privacidad, confidencialidad, personalización y eficiencia, basados en roles o necesidades específicas. Medir el control de acceso en un entorno blockchain puede abarcar auditorías de seguridad, simulaciones de ataques, tiempos de respuesta para determinar la rapidez con que se otorga o se niega el acceso, y una tasa que permita monitorear la frecuencia de accesos no autorizados bloqueados correctamente, o incluso la frecuencia de incidentes de brechas de seguridad (Zwitter A. et al., 2020).

6.6.1.4. Métricas de interoperabilidad. La interoperabilidad en los EHR da la capacidad de que diferentes sistemas de información, dispositivos y aplicaciones para acceder, intercambiar, integrar y cooperativamente utilizar datos de manera segura y eficiente, dentro y entre instituciones, regiones y países. Para mejorar la coordinación y reducir errores médicos es importante tener en cuenta la compatibilidad con estándares internacionales como HL7, FHIR que sería crucial para facilitar esta interoperabilidad, beneficiándose de la tecnología blockchain para

asegurar la integridad y autenticidad de los datos compartidos entre sistemas heterogéneos (Montón, 2021).

6.6.1.5. Métricas acerca del usuario. El usuario es de suma importancia (Tutty et al., 2019); por lo tanto, es necesario contar con métricas relacionadas al usuario que permitan entender su experiencia con el sistema. Por ejemplo, se consideran métricas enfocadas en los usuarios finales (pacientes, médicos, enfermeras, administradores) para medir aspectos como la satisfacción del usuario, la facilidad de uso, la tasa de adopción, la cobertura e inmutabilidad. La tecnología blockchain ofrece mecanismos para la creación de registros transparentes, fundamentales para la confianza en el sistema de salud, la precisión en el diagnóstico y el tratamiento, que, a su vez, deben cumplir con regulaciones legales y de privacidad.

6.6.1.6. Métricas del impacto clínico. La implementación de la tecnología blockchain en sistemas de registros médicos electrónicos (EHR) causa un impacto clínico crucial, ya que permite conocer el estado actual de los procesos tras una implementación en comparación con el estado previo a su implementación (Añel et al. 2021). Tener métricas sobre el impacto clínico puede ser beneficioso, por ejemplo, en tiempo de toma de decisiones clínicas y mejoras en la atención al paciente. Disponer de métricas que ofrezcan la oportunidad de evaluar el impacto permite a los stakeholders tomar decisiones informadas sobre el rendimiento, la seguridad y la mejora en la atención al paciente.

6.6.1.7. Métrica de costos e inversión. Para evaluar la viabilidad financiera y la eficiencia económica de un sistema basado en blockchain, es esencial considerar una serie de métricas

relacionadas con los costos e inversión. La cobertura en una red blockchain se refiere a la cantidad de participantes o aplicaciones que utilizan la tecnología, lo que puede indicar una mayor adopción y utilidad. Los costos de implementación incluyen los gastos asociados con el desarrollo inicial y la configuración del sistema, como la contratación de expertos en blockchain y desarrolladores de software. Por otro lado, los costos de despliegue consideran los recursos necesarios para operar la infraestructura blockchain, incluido el despliegue de contratos inteligentes. Estos aspectos son cruciales para evaluar la viabilidad económica de implementar y mantener el sistema. Los costos de mantenimiento abarcan los gastos recurrentes necesarios para mantener el sistema operativo, actualizado y seguro. Además, los costos de transacción incluyen aquellos asociados con la realización de operaciones de interoperabilidad, como los costos de gas para contratos inteligentes y tarifas de transacción. Finalmente, el retorno de la inversión (ROI) evalúa el rendimiento económico del proyecto en relación con los costos y beneficios generados a lo largo del tiempo. Estas métricas ofrecen una visión integral de los aspectos financieros y económicos involucrados en la implementación y operación de un sistema basado en blockchain (Thompson et Al, 2010).

6.6.1.8. Métricas de seguridad y privacidad. Para garantizar la seguridad y privacidad en un entorno blockchain, es crucial considerar una serie de métricas y prácticas. La auditoría se convierte en una herramienta esencial para verificar la integridad y el cumplimiento de los registros, mientras que el cumplimiento regulatorio y ético asegura que todas las operaciones estén alineadas con las normativas, como el GDPR en Europa o el HIPAA en Estados Unidos, además de consideraciones éticas relacionadas con el manejo de datos médicos. La incidencia de errores médicos compara la frecuencia de errores de medicación, diagnósticos equivocados y otros errores clínicos antes y después de la implementación del EMR, mientras que la permanencia de datos

garantiza la conservación y accesibilidad de la información a lo largo del tiempo. La seguridad de los datos evalúa las medidas de protección de la privacidad y seguridad de la información de los pacientes, y la resiliencia ante fallas es la capacidad del sistema para manejar nodos o transacciones fallidas sin comprometer la integridad o disponibilidad de los datos, mientras que la detección y mitigación de brechas de seguridad se encargan de las incidencias de seguridad que resultaron en accesos no autorizados a EMR. En conjunto, estas métricas fortalecen la seguridad y la confianza en el entorno blockchain (Reegu et al 2023)

7. Conclusiones

La integración de la tecnología Blockchain en los procesos de registros médicos ha demostrado ser una solución innovadora y efectiva para las instituciones de atención y prestación de servicios en salud. Este análisis ha mostrado que la implementación de Blockchain no solo mejora la seguridad y la privacidad de los registros médicos electrónicos, sino que también facilita su interoperabilidad entre diferentes entidades de salud y sus usuarios. Además, la automatización de procesos mediante estas tecnologías ha conducido a una mayor eficiencia en la gestión de los datos de salud, permitiendo un acceso más rápido y seguro a la información médica, lo cual es crucial para la toma de decisiones en tiempo real y la mejora en la calidad de la atención al paciente. Asimismo, se identifican retos y oportunidades de mejora que podrían servir de guía para futuras implementaciones, asegurando que las soluciones tecnológicas se alineen efectivamente con las necesidades operativas y estratégicas del sector salud.

La exhaustiva revisión bibliográfica realizada confirmó que la tecnología Blockchain tiene el potencial de revolucionar la gestión de registros médicos, proporcionando soluciones innovadoras para los desafíos de seguridad, privacidad e interoperabilidad. La revisión ha destacado cómo la automatización mediante tecnologías Blockchain puede reducir significativamente los tiempos de procesamiento y mejorar la precisión de los registros médicos, facilitando así una mejor coordinación entre las diferentes entidades de atención médica. Se han explorado diversos estudios de caso y modelos de implementación que subrayan la capacidad de Blockchain para abordar desafíos críticos como la interoperabilidad y la privacidad de los datos en el registro médico electrónico, sugiriendo así caminos potenciales para futuras investigaciones y desarrollos en este campo.

Se identificaron múltiples oportunidades para la integración de la tecnología Blockchain en los sistemas de salud existentes, lo que podría llevar a mejoras significativas en la eficiencia operativa, asegurar la integridad y la confidencialidad de los datos médicos, interoperabilidad, y facilitar una mejor coordinación entre las diferentes partes interesadas del sector. Esta tecnología promueve la transparencia y la trazabilidad de las interacciones dentro de los registros médicos, elementos esenciales para aumentar la confianza de los pacientes y mejorar la calidad general del cuidado sanitario.

La propuesta de integración de la tecnología Blockchain en los procesos de registros médicos en la atención a los pacientes demuestra ser altamente beneficiosa. Este enfoque no solo refuerza la seguridad y la privacidad de los datos de salud, sino que también mejora la eficiencia de los procesos al automatizar la verificación y el intercambio de información entre distintos proveedores de servicios de salud. La implementación de Blockchain en este contexto permite garantizar un manejo más seguro y eficiente de los registros médicos, lo cual es crucial para la precisión en los diagnósticos y la rapidez en la administración de tratamientos. Además, esta integración facilita una mayor autonomía y control por parte de los pacientes sobre sus propios datos médicos, alineándose con las tendencias actuales hacia una mayor transparencia y empoderamiento del paciente. Este planteamiento evidencia que la adopción de Blockchain podría ser una solución clave para superar las barreras existentes en la gestión de información de salud y, por ende, es imperativo seguir explorando sus aplicaciones prácticas y el impacto a largo plazo en el sector salud.

La implementación de la tecnología Blockchain en el sistema de salud ha revelado resultados positivos significativos. El blockchain puede mejorar notablemente la eficiencia logística en el manejo de registros médicos, reduciendo los tiempos de acceso y procesamiento de

datos. Esto contribuye a una disminución en los tiempos de espera y atención a los pacientes, lo cual se traduce en un incremento en la satisfacción del cliente y en la calidad del servicio proporcionado. Además, la capacidad de Blockchain para proporcionar una plataforma segura y transparente mejoraría la confianza entre los pacientes y los proveedores de servicios de salud. La satisfacción de los usuarios es vital para este tipo de implementaciones, por lo cual, se realiza un análisis de métricas para la cuantificación de beneficios que ayudaría a demostrar que el blockchain no solo ayuda en los procesos internos, sino que también eleva la calidad del servicio al cliente justificando su adopción en el sector salud como una estrategia de mejora continua y adaptaciones a las necesidades modernas.

8. Recomendaciones

Para mejorar la gestión de registros electrónicos (EHR), es esencial enfocarse en fortalecer la infraestructura de cloud computing mediante la configuración adecuada de los servicios en la nube. Esto ayudará a prevenir accesos no autorizados y posibles filtraciones de datos, asegurando así la integridad y confidencialidad de la información médica almacenada y transmitida. Asimismo, se sugiere promover la interoperabilidad entre diferentes sistemas de EHR y plataformas blockchain a través de la estandarización de protocolos y formatos de datos. Esta medida facilitará una integración segura y fluida, permitiendo el intercambio eficiente y seguro de datos de salud entre diversas entidades y sistemas de atención médica. Además, se recomienda ofrecer capacitación continua para usuarios y profesionales de la salud, con programas de formación regular sobre las mejores prácticas de seguridad y el uso efectivo de los sistemas de EHR basados en blockchain. Esto garantizará una adopción adecuada y segura de estas tecnologías, así como una protección óptima de la información de salud.

Las auditorías de seguridad y pruebas de penetración regulares y con cierta frecuencia permiten identificar y mitigar vulnerabilidades en el sistema, por ejemplo, al adoptar un enfoque multicapa para la seguridad de datos incluyendo cifrado de datos, autenticación multifactor y contratos inteligentes, para proporcionar una protección robusta contra ataques cibernéticos.

La revisión y actualización de políticas de conformidad para mantener las políticas de seguridad y privacidad actualizadas con las regulaciones y normativas es crucial para asegurar el cumplimiento continuo. Conocer las regulaciones permite establecer la implementación de políticas de seguridad detalladas con una correcta gestión de claves criptográficas, lo cual ayuda a garantizar la seguridad de los datos en tránsito y almacenados. Al implementar estas recomendaciones, se espera que la integración de blockchain y cloud computing en los sistemas

de EHR no solo mejore la eficiencia y seguridad de la gestión de registros médicos, sino que también fortalezca la confianza de los pacientes en la protección de su información de salud.

Referencias Bibliográficas

Abbas, A. F., Qureshi, N. A., Khan, N., Chandio, R., & Ali, J. (2022). The Blockchain Technologies in Healthcare: Prospects, Obstacles, and Future Recommendations; Lessons Learned from Digitalization. *International Journal of Online and Biomedical Engineering*, *18*(9), 144–159. https://doi.org/10.3991/ijoe.v18i09.32253

Academy, B. (2023, 9 febrero). Escalabilidad del blockchain - sidechains y payment channels. Binance Academy. https://academy.binance.com/es/articles/blockchain-scalability-sidechains-and-payment-channels

Akhter Md Hasib, K. T., Chowdhury, I., Sakib, S., Monirujjaman Khan, M., Alsufyani, N., Alsufyani, A., & Bourouis, S. (2022). Electronic Health Record Monitoring System and Data Security Using Blockchain Technology. *Security and Communication Networks*, *2022*. https://doi.org/10.1155/2022/2366632

Akkaoui, R., Hei, X., & Cheng, W. (2020). EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange. *IEEE Access*, *8*, 113467–113486. https://doi.org/10.1109/ACCESS.2020.3003575

Alves, T., Almeida, F., Brito, F., Tourinho, F. & de Andrade, S. (2022). Regulation and Use of Health Information Systems in Brazil and Abroad. CIN: Computers, Informatics, Nursing, 40 (6), 373-381. doi: 10.1097/CIN.0000000000000828.

Andrew, J., Deva Priya Isravel, K. Martin Sagayam, Bhushan, B., Sei, Y., & Eunice, J. (2023). Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. Journal of Network and Computer Applications, 215, 103633–103633. https://doi.org/10.1016/j.jnca.2023.103633

Añel R, Garcia I, Breavo R, & Carballeira J. (2021). Historia clínica y receta electrónica: riesgos y beneficios detectados desde su implantación. diseño, despliegue y usos seguros. National Library of Medicine. 10.1016/j.aprim.2021.102220

AWS, ¿Qué es la criptografía? - Explicación sobre la criptografía - AWS, Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/cryptography/

Babu, E. S., Yadav, B. V. R. N., Nikhath, A. K., Nayak, S. R., & Alnumay, W. (2023). MediBlocks: secure exchanging of electronic health records (EHRs) using trust-based blockchain network with privacy concerns. *Cluster Computing*, *26*(4), 2217–2244. https://doi.org/10.1007/s10586-022-03652-w

Bello E., Computación en la nube o cloud computing: guía 2024, Thinking For Innovation, 26 de enero de 2024. https://www.iebschool.com/blog/que-es-cloud-computing-digital-business/

Bera, B., Mitra, A., Das, A. K., Puthal, D., & Park, Y. H. (2023). Private Blockchain-Based AI-Envisioned Home Monitoring Framework in IoMT-Enabled COVID-19 Environment. *IEEE Consumer Electronics Magazine*, *12*(3), 62–71. https://doi.org/10.1109/MCE.2021.3137104

Cerchione, R., Centobelli, P., Riccio, E., Abbate, S., & Oropallo, E. (2022). *Blockchain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem*.

Cernian, A., Tiganoaia, B., Sacala, I. S., Pavel, A., & Iftemi, A. (2020). Patientdatachain: A blockchain-based approach to integrate personal health records. *Sensors (Switzerland)*, *20*(22), 1–24. https://doi.org/10.3390/s20226538

Chelladurai, U., & Pandian, S. (2022). A novel blockchain based electronic health record automation system for healthcare. *Journal of Ambient Intelligence and Humanized Computing*, *13*(1), 693–703. https://doi.org/10.1007/s12652-021-03163-3

Ciberseg. (2022, 9 marzo). ¿Qué es el cifrado AES y cómo funciona? Ciberseguridad. https://ciberseguridad.com/guias/prevencion-proteccion/criptografia/cifrado-aes/

Cloudflare, ¿Cómo funciona la criptografía de clave pública? Encriptación de clave pública y SSL, (s.f.), https://www.cloudflare.com/es-es/learning/ssl/how-does-public-key-encryption-work/

CoinMarketCap. (2023, 24 enero). Throughput Definition. CoinMarketCap Academy. https://coinmarketcap.com/academy/glossary/throughput

Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society, 39, 283–297. https://doi.org/10.1016/j.scs.2018.02.014

Daraghmi, E. Y., Daraghmi, Y. A., & Yuan, S. M. (2019). MedChain: A design of blockchain-based system for medical records access and permissions management. IEEE Access, 7, 164595–164613. https://doi.org/10.1109/ACCESS.2019.2952942

Dimitrov, D. V. (2019). Blockchain applications for healthcare data management. *Healthcare Informatics Research*, *25*(1), 51–56. https://doi.org/10.4258/hir.2019.25.1.51

Egala, B. S., Pradhan, A. K., Badarla, V., & Mohanty, S. P. (2021). Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things with Effective Access Control. *IEEE Internet of Things Journal*, *8*(14), 11717–11731. https://doi.org/10.1109/JIOT.2021.3058946

Egala, B. S., Pradhan, A. K., Gupta, S., Sahoo, K. S., Bilal, M., & Kwak, K. S. (2022). CoviBlock: A Secure Blockchain-Based Smart Healthcare Assisting System. *Sustainability (Switzerland)*, *14*(24). https://doi.org/10.3390/su142416844

Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. *Journal of Medical Systems*, *42*(8). https://doi.org/10.1007/s10916-018-0993-7

Fuentes Blanco, E. Andrés. (2022). *Contratos Inteligentes : Un análisis Teórico Desde la Autonomía Privada en el Ordenamiento Jurídico Colombiano.* Editorial UniMagdalena. pp 13-17, http://www.jstor.org/stable/j.ctv2fwfzm8

Gate.Io. (2023, 23 noviembre). ¿Qué es el hash en Blockchain? Los conceptos básicos cubiertos. Gate Learn. https://www.gate.io/es/learn/articles/what-is-hashing-in-blockchain/864

Gutiérrez, O., Romero, G., Pérez, L., Salazar, A., Wightman, P., & Charris, M. (2020). Healthyblock: Blockchain-based it architecture for electronic medical records resilient to connectivity failures. *International Journal of Environmental Research and Public Health*, *17*(19), 1–38. https://doi.org/10.3390/ijerph17197132

Hai, T., Zhou, J., Srividhya, S. R., Jain, S. K., Young, P., & Agrawal, S. (2022). BVFLEMR: an integrated federated learning and blockchain technology for cloud-based medical records recommendation system. *Journal of Cloud Computing*, *11*(1). https://doi.org/10.1186/s13677-022-00294-6

Honavar, S. (2020). Electronic medical records - The good, the bad and the ugly. In *Indian Journal of Ophthalmology* (Vol. 68, Issue 3, pp. 417–418). Wolters Kluwer Medknow Publications. https://doi.org/10.4103/ijo.IJO_278_20

IBM, Blockchain ¿Qué es la tecnología blockchain? (s.f.), https://www.ibm.com/es-es/topics/blockchain

Ibor, A. E., Edim, E. B., & Ojugo, A. A. (2023). Secure Health Information System with Blockchain Technology. *Journal of the Nigerian Society of Physical Sciences*, *5*(2). https://doi.org/10.46481/jnsps.2023.992

Indumathi, J., Shankar, A., Ghalib, M. R., Gitanjali, J., Hua, Q., Wen, Z., & Qi, X. (2020). Block Chain Based Internet of Medical Things for Uninterrupted, Ubiquitous, User-Friendly, Unflappable, Unblemished, Unlimited Health Care Services (BC IoMT U6HCS). *IEEE Access*, *8*, 216856–216872. https://doi.org/10.1109/ACCESS.2020.3040240

IONOS. (2023, septiembre 13). ¿Qué es la latencia? IONOS Digital Guide. https://www.ionos.es/digitalguide/servidores/know-how/latencia/

Jamil, F., Ahmad, S., Iqbal, N., & Kim, D. H. (2020). Towards a remote monitoring of patient vital signs based on iot-based blockchain integrity management platforms in smart hospitals. *Sensors (Switzerland)*, *20*(8). https://doi.org/10.3390/s20082195

Jang, S., Rahmadika, S., Shin, S. U., & Rhee, K. H. (2021). PDPM: A patient-defined data privacy management with nudge theory in decentralized e-health environments. *IEICE Transactions on Information and Systems*, *E104D*(11), 1839–1849. https://doi.org/10.1587/TRANSINF.2021NGP0015

Jennath, H. S., Anoop, V. S., & Asharaf, S. (2020). Blockchain for Healthcare: Securing Patient Data and Enabling Trusted Artificial Intelligence. *International Journal of Interactive Multimedia and Artificial Intelligence*, *6*(3), 15. https://doi.org/10.9781/ijimai.2020.07.002

KeepCoding, R. (2023, 31 enero). ¿Qué es la criptografía de curva elíptica? KeepCoding Bootcamps.https://keepcoding.io/blog/que-es-la-criptografia-de-curvaeliptica/#:~:text=Esta%20criptograf%C3%ADa%20de%20curva%20el%C3%ADptica%20se%20caracterizan%20por,de%20forma%20eficiente%20y%20sin%20errores%20de%20redondeo.

Khatoon, A. (2020). A Blockchain-Based Smart Contract System for Healthcare Management. Electronics, 9(1), 94. https://doi.org/10.3390/electronics9010094

Köse, İ., Cece, S., Yener, S., Seyhan, S., Özge Elmas, B., Rayner, J., Birinci, Ş., Mahir Ülgü, M., Zehir, E., & Gündoğdu, B. (2023). Basic electronic health record (EHR) adoption in **Türkiye is nearly complete but challenges persist. *BMC Health Services Research*, *23*(1). https://doi.org/10.1186/s12913-023-09859-w

Landi, H. (2019). Amazon, Google, Microsoft, and IBM renew pledge to support interoperability and advance open standards. Fierce Healthcare (Online), https://www.proquest.com/trade-journals/amazon-google-microsoft-ibm-renew-pledge-support/docview/2266661042/se-2

Landi, H. (2020, January 20). *Number of patient records breached nearly triples in 2019*. https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats

Lee, J. S., Chew, C. J., Liu, J. Y., Chen, Y. C., & Tsai, K. Y. (2022). Medical blockchain: Data sharing and privacy preserving of EHR based on smart contract. *Journal of Information Security and Applications*, *65*. https://doi.org/10.1016/j.jisa.2022.103117

Lee, Y. L., Lee, H. A., Hsu, C. Y., Kung, H. H., & Chiu, H. W. (2022). SEMRES - A Triple Security Protected Blockchain Based Medical Record Exchange Structure. *Computer Methods and Programs in Biomedicine*, *215*. https://doi.org/10.1016/j.cmpb.2021.106595

Madine, M., Salah, K., Jayaraman, R., Al-Hammadi, Y., Arshad, J., & Yaqoob, I. (2021). AppxChain: Application-level interoperability for blockchain networks. *IEEE Access*, *9*, 87777–87791. https://doi.org/10.1109/ACCESS.2021.3089603

Mayer, A. H., Rodrigues, V. F., Da Costa, C. A., Da Rosa Righi, R., Roehrs, A., & Antunes, R. S. (2021). FogChain: A Fog Computing Architecture Integrating Blockchain and Internet of Things for Personal Health Records. *IEEE Access*, *9*, 122723–122737. https://doi.org/10.1109/ACCESS.2021.3109822

Metlabs. (2023, 30 diciembre). ¿Qué es IPFS?: La Revolución Descentralizada del Almacenamiento en la Web. https://metlabs.io/que-es-ipfs-almacenamiento-descentralizado/

Milanov, E. (2009). The RSA Algorithm. https://sites.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf

Monga, S., & Singh, D. (2022). MRBSChain a novel scalable medical records binance smart chain framework enabling a paradigm shift in medical records management. *Scientific Reports*, *12*(1). https://doi.org/10.1038/s41598-022-22569-3

Monleón, F. G. (s. f.). El blockchain al servicio de la sostenibilidad. ESIC. https://www.esic.edu/rethink/tecnologia/el-blockchain-al-servicio-de-la-sostenibilidad

Montemagno J & equipo de microsoft. (2023). Uso de bases de datos NoSQL como una infraestructura de persistencia - .NET. Microsoft Learn. https://learn.microsoft.com/es-es/dotnet/architecture/microservices/microservice-ddd-cqrs-patterns/nosql-database-persistence-infrastructure

Montenegro, I. (2021, 27 julio). Encriptación Simétrica y Asimétrica: Conoce sus diferencias. GB Advisors. https://www.gb-advisors.com/es/encriptacion-simetrica-y-asimetrica-conoce-sus-diferencias/

Montón, J. M. G. (2021, 25 mayo). Interoperabilidad de los sistemas de salud. ehCOS. https://www.ehcos.com/interoperabilidad-los-sistemas-salud/

OPS/OMS, Organización Panamericana de la Salud. Sistemas de información para la salud, s.f., https://www.paho.org/es/temas/sistemas-informacion-para-salud#:~:text=Los%20Sistemas%20de%20Informaci%C3%B3n%20para,beneficio%20de%20la%20salud%20p%C3%BAblica

OPS Organización Panamericana de Salud, Registros Médicos Electrónicos, s.f., https://www3.paho.org/relacsis/index.php/es/areas-de-trabajo/gt10-registros-medicos-electronicos/

Pais, M. J. L. (2019). Mapeamentos De HL7-v2.x Para FHIR. ProQuest Dissertations Publishing, https://www.proquest.com/dissertations-theses/mapeamentos-de-hl7-v2-x-para-fhir/docview/2917303306/se-2?accountid=29068

Park, Y. R., Lee, E., Na, W., Park, S., Lee, Y., & Lee, J. H. (2019). Is blockchain technology suitable for managing personal health records? Mixed-methods study to test feasibility. *Journal of Medical Internet Research*, *21*(2). https://doi.org/10.2196/12533

Peterson, K., Deeduvanu, R., Kanjamala, P., & Boles, K. (n.d.). *A Blockchain-Based Approach to Health Information Exchange Networks*, https://www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf

Poongodi, T., Sujatha, R., Kiruthika, M., & Suresh, P. (2022). Chapter 9 - IoT-based health care data analytical paradigm using blockchain technology. In S. Bhattacharyya, N. K. Mondal, K. Mondal, J. P. Singh, & K. B. Prakash (Eds.), *Cognitive Data Models for Sustainable Environment* (pp. 203–230). Academic Press. https://doi.org/https://doi.org/10.1016/B978-0-12-824038-0.00001-8

Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2021). Blockchain Mutability: Challenges and Proposed Solutions. IEEE Transactions on Emerging Topics in Computing, 9(4), 1972–1986. https://doi.org/10.1109/TETC.2019.2949510

Qu, J. (2022). Blockchain in medical informatics. Journal of Industrial Information Integration, 25, 100258–100258. https://doi.org/10.1016/j.jii.2021.100258

Quiel, Y. C., Saavedra, A., & Villarreal, V. (2019). Estándares de codificación e interoperabilidad en Salud: evaluación del proyecto AmIHEALTH. https://www.redalyc.org/journal/3776/377665579007/html/

Reegu, F. A., Abas, H., Gulzar, Y., Xin, Q., Alwan, A. A., Jabbari, A., Sonkamble, R. G., & Dziyauddin, R. A. (2023). Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System. *Sustainability (Switzerland)*, *15*(8). https://doi.org/10.3390/su15086337

Sabbagh, P., Pourmohamad, R., Elveny, M., Beheshti, M., Davarpanah, A., Metwally, A. S. M., Ali, S., & Mohammed, A. S. (2021). Evaluation and classification risks of implementing blockchain in the drug supply chain with a new hybrid sorting method. *Sustainability (Switzerland)*, *13*(20). https://doi.org/10.3390/su132011466

Sadeghib R, J. K., Prybutok, V. R., & Sauser, B. (2022). Theoretical and practical applications of blockchain in healthcare information management. *Information and Management*, *59*(6). https://doi.org/10.1016/j.im.2022.103649

Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The Energy Consumption of Blockchain Technology: Beyond Myth. Business & Information Systems Engineering, 62(6), 599–608. https://doi.org/10.1007/s12599-020-00656-x

Sql. (2023, 4 agosto). Normalización y desnormalización en Bases de Datos SQL, SQL. Programar en SQL. https://www.programarsql.com/normalizacion-y-desnormalizacion-en-bases-de-datos-sql/

Sumathi, M., Vijayaraj, N., Peter, S., Raja, R., Rajkamal, M., Sumathi, M., Vijayaraj, N., Raja, S. P. R., & Rajkamal, M. (2022). INTERNET OF THING BASED CONFIDENTIAL HEALTHCARE DATA STORAGE, ACCESS CONTROL AND MONITORING USING BLOCKCHAIN TECHNIQUE. *Computing and Informatics*, *41*, 1207–1239. https://doi.org/10.31577/cai

Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, *50*. https://doi.org/10.1016/j.jisa.2019.102407

Tecnologías Información, Gestión de registros médicos: Políticas y Procedimientos (s.f.). https://www.tecnologias-informacion.com/registrosmedicos.html

Thi Bac, D., & Khit, B. (2023). An overview of quantum resistance digital signatures based on hash functions. Tạp Chí Khoa Học, 52(3A), 40–54. https://doi.org/10.56824/vujs.2023a046

Thompson, D., Velasco, F., Classen, D., & Raddemann, R. J. (2010). Reducing clinical costs with an EHR: investments in performance management are essential to realizing the full benefits of an EHR system--including reduced costs and improved quality of care. Healthcare Financial Management, 64(10), 106-. https://www.proquest.com/trade-journals/reducing-clinical-costs-with-ehr/docview/811379490/se-2

Tuler De Oliveira, M., Henrik, L., Reis, A., Verginadis, Y., Menezes, D., Mattos, F., & Delgado Olabarriaga, S. (2022). *SmartAccess: Attribute-Based Access Control System for Medical Records based on Smart Contracts*. *4*, 1–20. https://doi.org/10.1109/ACCESS.2017.DOI

Tutty, M. A., Carlasare, L. E., Lloyd, S., & Sinsky, C. A. (2019). The complex case of EHRs: examining the factors impacting the EHR user experience. Journal of the American Medical Informatics Association, 26(7), 673–677. https://doi.org/10.1093/jamia/ocz021

Vishwesh J & Meenakshi S (2018). CP-ABE Protocol for Iot with Cloud. IJERT.https://doi.org/10.17577/IJERTCONV5IS22035

Vollmer, N. (2023, 4 abril). Artículo 17 UE Reglamento general de protección de datos. Privacy/Privazy according to plan. Nicholas Vollmer. https://www.privacy-regulation.eu/es/17.htm

Wabo, G. K., Prasser, F., Gierend, K., Siegel, F., & Ganslandt, T. (2023). Data Quality– and Utility-Compliant Anonymization of Common Data Model–Harmonized Electronic Health Record Data: Protocol for a Scoping Review. JMIR Research Protocols, 12https://doi.org/10.2196/46471

Wei, P., Wang, D., Zhao, Y., Kumar, S., & Kumar, N. (2020). Blockchain data-based cloud data integrity protection mechanism. Future Generation Computer Systems, 102, 902–911. https://doi.org/10.1016/j.future.2019.09.028

Windari, A., Susanto, E., & Fadhilah, I. Q. (2023). Hospital administrative services with electronic medical records: A meta-analysis. In *Journal of Public Health and Development* (Vol. 21, Issue 3, pp. 333–348). Mahidol University - ASEAN Institute for Health Development. https://doi.org/10.55131/jphd/2023/210325

Xiang, X., & Zhao, X. (2022). Blockchain-assisted searchable attribute-based encryption for e-health systems. *Journal of Systems Architecture*, *124*. https://doi.org/10.1016/j.sysarc.2022.102417

Xu, X., Guo, Y., & Guo, Y. (2023). Fog-enabled private blockchain-based identity authentication scheme for smart home. *Computer Communications*, *205*, 58–68. https://doi.org/10.1016/j.comcom.2023.04.005

Yadav, S. G. S., Gunisetti, L., Koduri, S. B., Scaria, T., Dixit, A., & Lokesh, S. (2023). Securing electronic health records using blockchain technology for IoT in healthcare domain. *Soft Computing*. https://doi.org/10.1007/s00500-023-08489-y

Zhang, J., Li, Z., Tan, R., & Liu, C. (2021). Design and Application of Electronic Rehabilitation Medical Record (ERMR) Sharing Scheme Based on Blockchain Technology. *BioMed Research International*, *2021*. https://doi.org/10.1155/2021/3540830

Zhang, N., Li, J., Lou, W., & Hou, Y. T. (2018). PrivacyGuard: Enforcing Private Data Usage with Blockchain and Attested Execution. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11025 LNCS*, 345–353. https://doi.org/10.1007/978-3-030-00305-0_24

Zwitter A., Gstrein O, & Yap, E. (2020). Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual. Frontiers in Blockchain, 3. https://doi.org/10.3389/fbloc.2020.00026