UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE INGENIERÍA

**PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS DE
INFORMACIÓN**

**Modelo de seguridad de los datos clínicos para los dispositivos mHealth
basado en Blockchain**

TESIS

Para optar el título profesional de Ingeniero de Sistemas de Información

AUTOR(ES)

Natividad Peña, Cristhian Alexis (0000-0002-0956-4289)

Gutierrez Díaz, Angel Elí (0000-0002-1831-7781)

ASESOR

Pérez Pichis, Roy (0000-0003-2113-0405)

Lima, 06 de Enero de 2020

DEDICATORIA

Esta tesis está dedicada a nuestros padres por su sacrificio, motivación y apoyo incondicional durante nuestra etapa universitaria y crecimiento profesional.

AGREDECIMIENTOS

Agradecer a Dios por iluminarnos día a día y por permitirnos concluir con nuestro objetivo.

RESUMEN EJECUTIVO

La salud móvil (mHealth) ofrece servicios que facilita al personal médico y al paciente el acceso a su información médica desde cualquier lugar conectado a internet. Asimismo, es necesario garantizar la seguridad de dichos datos ya que genera un impacto en la atención del paciente. La incapacidad de acceder a la información podría conllevar al retraso del tratamiento y a un mal manejo para la toma de decisiones.

Por ello, proponemos un modelo de seguridad para proteger los datos de pacientes en sistemas mHealth utilizando Blockchain. Este modelo se implementa bajo una plataforma de Blockchain que permite recopilar, compartir e integrar los datos de manera segura a través de una aplicación móvil mediante dispositivos mHealth para la atención médica en las clínicas de Perú. Se definió un escenario de pruebas para validar el modelo propuesto, se realizó el estudio con un grupo de usuarios a través de una aplicación móvil de salud, los datos médicos utilizados fueron brindados por una clínica peruana en calidad de investigación. Durante el estudio, se validó el control de accesos a la red, el acceso a la información médica a usuarios autorizados, la integridad de datos en cada transacción y la evaluación del rendimiento del sistema con una alta carga de transacciones. Como resultado final se obtuvo que, la implementación del modelo propuesto garantizó la autenticación, confidencialidad, integridad y disponibilidad de los datos generando mayor seguridad en los sistemas mHealth, así como también demostró ser un sistema escalable soportando una alta carga de transacciones.

Palabras clave: mHealth; Blockchain; dispositivos wearables; seguridad

Data security model for mHealth devices based on Blockchain

ABSTRACT

Mobile health (mHealth), offers services that help to medical staff and patients to get access to their data from any place through an internet connection. Likewise, it is necessary to guarantee the security of the data that generates an impact on the patient's care. The inability of accessing the data could lead to delays in treatment and decision making.

Therefore, we propose a security model to protect patient data in mHealth systems using Blockchain. This model is implemented under a Blockchain platform that allows collecting, sharing and integrating data in a safe way through a mobile app for mHealth devices, for medical care in Peruvian clinics. A test scenario was defined to validate the proposed model. Also, the study was conducted with a group of users through a health mobile app and the used medical data was provided by a hospital in Peru as anonymized research data. During the study, we validated the following topics: access control to the network, access to medical information of authorized users, data integrity on each transaction and performance evaluation of the system under a high user transaction load. As a final result, we conclude that the implementation of the proposed model guaranteed authentication, confidentiality, integrity and availability of the data, generating enhanced security in mHealth systems, as well as proved to be a scalable system supporting a high transaction load.

Keywords: mHealth; Blockchain; wearable devices; security

TABLA DE CONTENIDOS

INTRODUCCIÓN.....	1
CAPÍTULO 1: DEFINICIÓN DEL PROYECTO	3
1.1 Objeto de estudio	4
1.2 Dominio del problema	4
1.3 Planteamiento de la solución	6
1.4 Objetivos del proyecto	6
1.4.1 Objetivo General	6
1.4.2 Objetivos Específicos	7
1.5 Indicadores de éxito	7
CAPÍTULO 2: LOGROS DE LOS STUDENT OUTCOMES.....	9
2.1 STUDENTS OUTCOMES (ABET)	10
2.1.1 Student Outcome A.....	10
2.1.2 Student Outcome B	12
2.1.3 Student Outcome C	13
2.1.4 Student Outcome D.....	13
2.1.5 Student outcome E	14
2.1.6 Student outcome F	15
2.1.7 Student outcome G.....	16
2.1.8 Student outcome H.....	16
2.1.9 Student outcome I	17
2.1.10 Student outcome J	18
2.1.11 Student outcome K.....	18
CAPÍTULO 3: ESTADO DEL ARTE.....	20
3.1 Análisis	27
3.1.1 ¿Qué modelos y arquitecturas de seguridad existen para la protección de los datos clínicos de los pacientes durante su almacenamiento en una red interna?	27
3.1.2 ¿Qué modelos y arquitecturas de seguridad existen para la protección de los datos clínicos de los pacientes durante su transmisión?	42
3.1.3 ¿Qué aplicaciones de salud existen para la protección de datos clínicos de los pacientes?	48
3.2 Conclusiones	54

CAPÍTULO 4: MARCO TEÓRICO	56
4.1 Antecedentes	57
4.2 mHealth.....	58
4.3 Blockchain	60
4.5 Internet de las cosas	62
4.6 Compartición de datos P2P	64
4.7 Blockchain en el sector Salud	65
4.8 Normativas internacionales reguladoras de Blockchain en el sector Salud.....	66
4.9 Reglamento general de protección de datos	69
CAPÍTULO 5: DESARROLLO DEL PROYECTO.....	71
5.1 Benchmarking	72
5.1.1 Diseñando una arquitectura segura para aplicaciones m-Health	72
5.1.2 Compartir datos de mHealth a través de redes de datos nombrados	73
5.1.3 Sistema liviano de salud móvil seguro y rastreable.....	74
5.1.4 MedRec: Uso de Blockchain para acceso a datos médicos y gestión de permisos	75
5.1.5 Un enfoque Blockchain aplicado a una plataforma de tele dermatología en la región de Cerdeña.....	75
5.1.6 Compartir historias clínicas electrónicas seguras y fiables usando Blockchain.....	76
5.2 Modelo Propuesto	79
5.2.1 Recopilación de datos.....	79
5.2.2 Procesamiento de datos	79
5.2.3 Monitoreo del sistema	80
5.3 Implementación	81
5.3.1 Autenticación	81
5.3.2 Confidencialidad	82
5.3.3 Integridad	84
CAPÍTULO 6: RESULTADOS DEL PROYECTO.....	85
6.1 Autenticación	86
6.2 Integridad de los datos	87
6.3 Rendimiento del sistema	89
6.4 Plan de Costos.....	91
6.5 Plan de Continuidad.....	92
6.5.1 Post Implementación	92
6.5.2 Adaptabilidad del modelo	92

CAPÍTULO 7: GESTIÓN DEL PROYECTO	94
7.1 Plan de Gestión de Alcance	94
7.2 Plan de Gestión de la Calidad	95
7.3 Plan de Gestión de Comunicaciones	97
7.4 Plan de Gestión de Riesgos	100
7.5 Plan de Gestión de Recursos Humanos	102
7.6 Plan de Gestión de Cronograma	103
LECCIONES APRENDIDAS	105
CONCLUSIONES	106
RECOMENDACIONES	107
GLOSARIO	108
BIBLIOGRAFÍA	110
ANEXO A - WASC	112
ANEXO C – Costos y Presupuestos	114

ÍNDICE DE TABLAS

Tabla 1. Problema y causas del Proyecto	6
Tabla 2. Indicadores de éxito del proyecto.....	8
Tabla 3. Student Outcome A	12
Tabla 4. Student Outcome B	13
Tabla 5. Student Outcome C	13
Tabla 6. Student Outcome D	14
Tabla 7. Student Outcome E.....	15
Tabla 8. Student Outcome F.....	16
Tabla 9. Student Outcome G	16
Tabla 10. Student Outcome H	17
Tabla 11. Student Outcome I.....	18
Tabla 12. Student Outcome K	19
Tabla 13. Criterios de inclusión y exclusión	22
Tabla 14. Lista de Papers analizados.....	26
Tabla 15. Artículos de modelos y arquitecturas	42
Tabla 16. Tabla de evaluación para arquitectura de evaluación para mHealth	73
Tabla 17. Tabla de evaluación para arquitectura de red de datos nombrados	74
Tabla 18. Tabla de evaluación para arquitectura basada en LIST	74
Tabla 19. Arquitectura de evaluación para mHealth	75
Tabla 20. Arquitectura de evaluación para mHealth	76
Tabla 21. Arquitectura de evaluación para mHealth	77
Tabla 22. Plan de Gestión de Comunicaciones	99
Tabla 23. Lista de riesgos del proyecto	101
Tabla 24. Plan de Gestión de Recursos Humanos	103
Tabla 25. Plan de Gestión del Cronograma	104

ÍNDICE DE FIGURAS

Figura 1. Porcentaje de factores de riesgo en aplicaciones mHealth usando el modelo OWASP	5
Figura 2. Sistema Propuesto para el control de acceso	27
Figura 3. Arquitectura propuesta para un sistema e-Health.....	28
Figura 4. Block-Chain Avanzado.....	29
Figura 5. Modelo de Seguridad de Registros Médicos basados en Blockchain	30
Figura 6. Marco seguro para compartir datos clínicos en Blockchain	32
Figura 7. Sistema de Arquitectura LIST	33
Figura 8. Interacciones de alto Nivel en la construcción concreta.....	34
Figura 9. Un sistema de m-Salud jerárquico de tres niveles bajo escuchas	35
Figura 10. Estructura del entorno virtual de la propuesta	36
Figura 11. Recolección de data de Salud Personal.....	39
Figura 12. Protección de la Integridad de Datos de Salud Personal.....	39
Figura 13. Diagrama del bloque del procedimiento de incorporación de datos.....	43
Figura 14. Diagrama de bloques del procedimiento de extracción de datos	44
Figura 15. Modelo propuesto a alto nivel.....	44
Figura 16. Modelo conceptual Cloud basado en EMR/ERH/PHR	46
Figura 17. Diagrama de componentes del sistema de MedRec.....	48
Figura 18. NDNFit espacio de nombres y objeto de datos	50
Figura 19. mHealth como tecnología emergente	57
Figura 20. Infraestructura mHealth	58
Figura 21. Escenario de mHealth.....	59
Figura 22. Enfoque Cloud para Electronic Medical Records.....	59
Figura 23. Figura del flujo de trabajo de Blockchain	60
Figura 24. Lista de tipo información consumido por wearables	63
Figura 25. Comunicación peer – to peer	64
Figura 26. Flujo de trabajo de blockchain enfocado en EHR	66
Figura 27. Retos y oportunidades en la seguridad en el sector salud Blockchain	68
Figura 28. Distribución de prioridad según arquitectura de seguridad para los datos clínicos.....	78
Figura 29. Distribución de prioridad según arquitectura de seguridad para los datos clínicos.....	78
Figura 30. Modelo de Seguridad de los datos clínicos para los dispositivos mHealth basado en Blockchain	80
Figura 31. Arquitectura de mHealth en Blockchain.....	81

Figura 32. Doble autenticación al sistema	82
Figura 33. Solicitud del segundo factor de autenticación	87
Figura 34. Generación de bloques en la red Blockchain.....	88
Figura 35. Detalle de un bloque de la red de Blockchain.....	89
Figura 36. Tiempo promedio de respuesta de red de Blockchain.....	90
Figura 37. Tiempo promedio de respuesta basado en las funciones principales	91
Figura 38. Costos del proyecto	92
Figura 39. Propuesta del plan de continuidad del proyecto.....	93

INTRODUCCIÓN

En este documento, se constituye la memoria del proyecto “Modelo de Seguridad de Datos Clínicos para los dispositivos mHealth basado en Blockchain”. Para efectos de validación del modelo se construye un sistema mHealth basado en un marco de desarrollo propuesto por Hyperledger Composer que permite el fácil desarrollo de aplicaciones empresariales bajo la tecnología Blockchain, proporcionando fiabilidad en la información que fluye en el entorno. Hyperledger es una plataforma de código abierto, fundado en diciembre del 2015 por Linux Foundation.

El presente documento está conformado por siete capítulos, la cual se detalla a continuación:

Primer capítulo, consiste en definir el problema y causas en función a estudios que evidencien la situación actual del entorno. También, se define la solución a implementar, así como también los objetivos generales y específicos. Estos objetivos están respaldados por indicadores de éxito.

Segundo capítulo, se definen los Student Outcomes propuestos por ABET, así como también las competencias que exige la carrera de Ingeniería de Sistemas de Información. El cumplimiento de cada exigencia de ABET, se ve relacionado con la competencia de los autores del proyecto, así como la naturaleza de este.

Tercer capítulo, se describen los principales aportes con relación al presente proyecto. También, se clasifica y se realiza un análisis de las propuestas realizadas, su alcance, costo y esfuerzo. Para el proyecto, las propuestas están relacionadas a modelos y arquitecturas que brinden seguridad a sistemas mHealth. Por último, se describen las conclusiones de la clasificación de las soluciones planteadas por diversos autores.

Capítulo cuatro, consiste en definir los principales conceptos que ayuden a entender el contexto del proyecto. Estas definiciones permitirán la comprensión de la problemática, propuesta y resultados de la implementación.

Capítulo cinco, relacionado al desarrollo del proyecto, su propuesta y como se ha llevado a cabo la mejora de la situación actual en la seguridad de un sistema mHealth. Se describen métricas, indicadores, metodología, medio de validación.

Capítulo seis, consiste en evidenciar los principales resultados de la ejecución de la solución planteada. Estos resultados están directamente relacionados con el desarrollo del proyecto.

Capítulo siete, se muestran los procesos aplicados al presente proyecto que permitieron la correcta gestión de inicio a fin. Se consideraron en casi su totalidad las áreas de conocimiento establecidos por el PMBOK.

CAPÍTULO 1: DEFINICIÓN DEL PROYECTO

El primer capítulo tiene como fin describir el proyecto, poner en contexto la problemática identificada y el planteamiento de la solución. Además, se da a conocer el objetivo general y los objetivos específicos de este proyecto; así como también los indicadores de éxito para cumplir dichos objetivos.

1.1 Objeto de estudio

El presente proyecto tiene como objeto de estudio los beneficios de implementar la tecnología Blockchain en un sistema mHealth basado en la seguridad de datos de los pacientes con el objetivo de cumplir atributos de seguridad que exige un sistema sanitario. El desarrollo se basó en Hyperledger Composer, un framework para el desarrollo de aplicaciones empresariales para compartir, transferir datos de manera segura entre los participantes de la red de Blockchain.

El desarrollo del proyecto está relacionado con uno de los campos de la Ingeniería de Sistemas de Información, seguridad de información.

1.2 Dominio del problema

Se han realizado diversos estudios entorno al nivel de seguridad en que se encuentran los datos clínicos en un sistema mHealth. Se analizaron 53 aplicaciones móviles de salud y el 6% enviaron credenciales inseguras de inicio de sesión, el 36% de las aplicaciones estudiadas fueron comprometidas la comunicación entre el cliente y servidor, así como el 40% no protegieron la integridad de la información de los pacientes (Cifuentes, Beltrán, & Ramírez, 2015). Por otro lado, según un estudio de Kaspersky, se detectaron alrededor de 9 millones de paquetes de ransomware móvil.

Figura 1. Porcentaje de factores de riesgo en aplicaciones mHealth usando el modelo OWASP

(Cifuentes, Beltrán, & Ramírez, 2015)

Estos estudios, evidencian la preocupación por la que los proveedores de estos servicios mHealth deben tener y optar por soluciones de seguridad para evitar incidentes y la información se vea comprometida. Además, esto repercute directamente en la salud del paciente, ya que, al ser alterada los datos clínicos, se pueden diagnosticar en base a información errónea.

Según lo mencionado, se identificó el problema principal y sus causas relacionadas:

PROBLEMA	DESCRIPCIÓN
Los dispositivos utilizados en mHealth en las clínicas presentan vulnerabilidades poniendo en riesgo los datos clínicos del paciente.	Mala gestión de los riesgos asociados a la seguridad de los datos involucrados en los dispositivos m-Health. Falta de conocimiento del entorno al que se encuentran expuestos los activos de la clínica. Deficientes sistemas de autenticación en los dispositivos m-Health. Deficientes conexiones seguras en el flujo de datos.

Tabla 1. Problema y causas del Proyecto

1.3 Planteamiento de la solución

Ante la problemática presentada anteriormente, se propone un modelo de seguridad de datos en los dispositivos mHealth para la recolección y transferencia segura de información. El marco de trabajo usado será Hyperledger Composer, el cual brinda herramientas de desarrollo para crear soluciones empresariales basadas en un sistema descentralizado. Asimismo, se plantea monitorear el rendimiento del sistema para la evaluación de su escalabilidad para una futura interoperabilidad con otras entidades sanitarias.

1.4 Objetivos del proyecto

1.4.1 Objetivo General

Implementar un modelo de seguridad de los datos clínicos del paciente para los dispositivos mHealth basado en Blockchain.

1.4.2 Objetivos Específicos

Para el cumplimiento del objetivo general, se plantearon 4 objetivos específicos:

- ✓ **OE1:** Analizar los modelos de seguridad existentes y la tecnología de Blockchain.
- ✓ **OE2:** Diseñar un modelo de seguridad de los datos clínicos del paciente para los dispositivos mHealth basado en Blockchain.
- ✓ **OE3:** Validar el modelo de seguridad de los datos clínicos del paciente para los dispositivos mHealth basado en Blockchain.
- ✓ **OE4:** Elaborar un plan de continuidad que garantice, a lo largo del tiempo, la sostenibilidad y escalabilidad del modelo propuesto.

1.5 Indicadores de éxito

A continuación, se describe los indicadores de éxito que miden el cumplimiento de los objetivos específicos planteados.

INDICADOR DE ÉXITO	DESCRIPCIÓN	OBJETIVOS ESPECÍFICOS
IE1	Conformidad del profesor cliente sobre el análisis de diversos modelos de seguridad de datos para mHealth y la tecnología Blockchain.	OE1
IE2	Conformidad del profesor cliente del modelo de seguridad de los datos clínicos del paciente para los dispositivos mHealth basado en Blockchain.	OE2

IE3	Conformidad por expertos sobre la implementación del modelo de seguridad propuesto.	OE3
IE4	Conformidad por parte del profesor cliente sobre el plan de plan de continuidad elaborado.	OE4

Tabla 2. Indicadores de éxito del proyecto

CAPÍTULO 2: LOGROS DE LOS STUDENT OUTCOMES

En el presente capítulo se definirán los Student Outcomes de ABET y las competencias que certifican a la carrera de Ingeniería de Sistemas de Información. Por otro lado, se detalla cómo el proyecto “Modelo de Seguridad de los datos clínicos para los dispositivos mHealth basado en Blockchain” cumple y se alinea con las competencias.

2.1 STUDENTS OUTCOMES (ABET)

ABET es una organización no gubernamental sin fines de lucro reconocida por el Consejo de Acreditación para la Educación Superior. Acredita programas universitarios en diferentes campos de las tecnologías de información, ciencias aplicadas y naturales, computación a nivel de licenciatura y maestría. (ABET, s.f.)

La acreditadora afirma que los alumnos durante la etapa universitaria deben ser monitoreados y controlados para que éstos cumplan con las competencias de ABET. Asimismo, los alumnos deben recibir toda clase de información sobre la carrera como la malla curricular y asuntos de la carrera. ABET exige una serie de objetivos y resultados que el alumno graduado debe cumplir (ABET, 2017).

2.1.1 Student Outcome A: Aplicar conocimientos de matemáticas, ciencias, computación e ingeniería.

El presente proyecto cumple con este Outcome debido a que nuestro resultado final se involucra directamente con las ciencias informáticas y computación con los algoritmos de cifrado y factores de autenticación que buscan asegurar la información de los pacientes médicos.

Durante la realización del presente proyecto, se han realizado diversos análisis para llevar a cabo el éxito de este: Análisis técnico, análisis de tiempo, análisis económico.

Tipo Análisis	Descripción	Aplicación
Análisis Técnico	- Se estudiaron diversas tecnologías que permiten ayudar a la problemática de seguridad de datos clínicos, se concluyó que la tecnología Blockchain abarca gran parte de los	Aplicación de computación e ingeniería.

	principales atributos de seguridad en un sistema mHealth. - Respecto al proyecto, se realizó un análisis de factibilidad y adaptabilidad de la tecnología Blockchain en el sector salud, específicamente en un sistema mHealth.	
Análisis de tiempo	- Dado que la tecnología Blockchain está en una etapa temprana en la adopción en soluciones de seguridad en el Perú, se realizó un análisis detallado sobre la viabilidad del proyecto respecto al uso de esta tecnología como medio de validación del proyecto. El tiempo de realización es de 10 meses por lo que se distribuyó de manera detallada las actividades a realizar para el éxito de este.	Aplicación de matemáticas e ingeniería.
Análisis económico	- En la realización del proyecto, se realizó un análisis respecto al costo y presupuesto a tomar en cuenta en caso el proyecto	Aplicación de matemáticas, ciencias e ingeniería.

	se despliegue en un ambiente de producción. Se tomó en consideración los roles de las personas a cargo del proyecto, tecnologías a usar. Para el desarrollo del sistema en Blockchain se usó un Framework de código abierto para su rápido despliegue y sin costo alguno.	

Tabla 3. Student Outcome A

2.1.2 Student Outcome B: Diseñar y conducir experimentos en base al análisis e interpretar los datos

El presente proyecto cumple con el presente Outcome ya que durante el proyecto se realizaron análisis de diferentes modelos, arquitecturas y tecnologías que tenían como objetivo el cumplimiento de cuatro principales atributos de seguridad en la cual se basa el modelo propuesto, sustentada mediante estadísticas.

Evidencia	Descripción
Análisis Benchmarking	- Se realizaron dos análisis de Benchmarking. Primero, enfocada a la mejor tecnología aplicada para la solución propuesta. Segundo, en base a la tecnología concluida, qué framework es adaptable para el escenario del problema, esto

	influye un análisis de viabilidad y costos.

Tabla 4. Student Outcome B

2.1.3 Student Outcome C: Diseñar sistemas, componentes o procesos para encontrar soluciones en la atención de necesidades teniendo en cuenta restricciones económicas, sociales, políticas, éticas de salud y seguridad y otras propias del entorno empresarial

El cumplimiento de este outcome se debe al resultado de este proyecto que queda respaldado con parámetros de políticas y éticas de salud debido al factor del valor del activo que debe ser confidencial e íntegro. Asimismo, el resultado mitiga los riesgos de seguridad de los datos, pérdida de dinero y el daño reputacional de las organizaciones.

Entregable	Aplicación
Modelo de Seguridad de los datos clínicos para los dispositivos mHealth basado en Blockchain	Diseñar sistemas y sistemas para la propuesta de solución al problema identificado
Flujo de Información de datos en red Blockchain	

Tabla 5. Student Outcome C

2.1.4 Student Outcome D: Participar en equipos multidisciplinarios, liderando o desarrollando eficientemente sus tareas con profesionales de diferentes campos o campos de aplicación.

El presente proyecto, cumple con este outcome ya que, durante la realización del proyecto, se interactuaron con diferentes perfiles profesionales como: expertos en TI, para la aprobación del modelo propuesto; médicos, para entender cómo es el tratamiento

de la información de los pacientes; profesor cliente, quien es el especialista en seguridad de los datos; profesor gerente, quien brinda orientación sobre el flujo de trabajo que se necesita para la realización del proyecto.

Evidencia
Reuniones semanales con el asesor experto en el tema de seguridad
Reuniones con los expertos de seguridad para la retroalimentación con respecto a la propuesta y validación
Reuniones con médicos para identificar los diversos análisis con dispositivos wearables, así como la conformidad de la validación del sistema.

Tabla 6. Student Outcome D

2.1.5 Student outcome E: Identificar, formular y resolver problemas de ingeniería.

El presente proyecto, cumple con este outcome ya que durante el transcurso de la realización de este se identificaron tres aspectos importantes: problema, diseño de la solución y la validación de este mediante la aprobación del experto o del interesado.

Evidencia	Descripción
Identificación del problema a tratar	Se recopiló datos y gráficos estadísticos evidenciando el problema en el sector

	salud en mHealth respecto a la seguridad de datos clínicos.
Diseño del modelo propuesto	Basado en un análisis de viabilidad y efectividad de la tecnología a usar se diseñó un modelo para brindar solución a la problemática identificada.
Validación del sistema propuesto	Basado en un escenario de pruebas, se implementó la solución.
Analizar resultados y conocimientos relacionado a la validación implementada	Una vez implementado, se analizaron los resultados y se generó conocimiento para futuros trabajos sobre la tecnología usada para el sector tratado.

Tabla 7. Student Outcome E

2.1.6 Student outcome F: Proponer soluciones de ingeniería con responsabilidad profesional y ética

El presente proyecto cumple con este outcome ya que durante la realización del proyecto se realizaron actas de reunión evidenciando lo tratado y los comentarios del avance del proyecto; también se realizaron acuerdos de confidencialidad con el especialista encargado de TI y el representante de la entidad sanitaria.

Evidencia	Descripción
Información usada para la validación del proyecto	El objeto de nuestro proyecto son los datos clínicos de pacientes, por lo que es de carácter confidencial. Por ello, para la realización de la validación se usó datos de investigación proporcionado por la clínica y no datos reales ya que son propios de los pacientes.

Tabla 8. Student Outcome F

2.1.7 Student outcome G: Comunicar oralmente o por escrito ideas o resultados de manera clara y efectiva.

El presente proyecto cumple con este outcome, ya que semanalmente se realizaron reuniones con el cliente y se transmitieron los avances, nuevas ideas, resultados del proyecto, etc. Asimismo, se realizaron presentaciones al comité donde se les explicó de manera clara y concisa los puntos clave del proyecto.

Por otro lado, las reuniones realizadas con los expertos en seguridad para el refinamiento del modelo propuesto, así como su validación respectiva.

Evidencia
Reuniones semanales con el asesor experto en el tema de seguridad
Reuniones con los expertos de seguridad para la retroalimentación con respecto a la propuesta y validación
Exposiciones con el comité de tesis a fin de evidenciar el cumplimiento de los objetivos propuestos.
Elaboración del paper de tesis explicando los antecedentes, propuesta, caso de estudio, resultados y conclusiones.

Tabla 9. Student Outcome G

2.1.8 Student outcome H: Identificar el impacto de las soluciones de ingeniería en el contexto global, económico y del entorno de la sociedad.

El presente proyecto cumple este outcome, ya que el resultado final mitiga el riesgo que los datos sean vulnerados y expuestos. También, transmite seguridad a los pacientes ya que sus datos no serán manipulados por personas ajenas a los procesos de la clínica. El impacto se basa en los resultados obtenidos en la validación del proyecto.

Evidencia
Propuesta de modelo de seguridad de datos en el sector salud, específicamente en un sistema mHealth.
Esta propuesta sirve como referencia para proponer soluciones mHealth seguras en el Perú.

Tabla 10. Student Outcome H

2.1.9 Student outcome I: Reconocer la necesidad de mantener sus conocimientos actualizados.

A lo largo del proyecto se realizaron diversas actividades que aportaron al conocimiento del alumno, como por ejemplo el análisis de las diferentes soluciones que existen en la actualidad, así como también, las normas establecidas para la seguridad y protección de los datos confidenciales de los pacientes. El sistema actual exige a las compañías en general asegurar la información tanto de sus clientes como de las personas que laboran en el centro. Asimismo, muchas empresas apuestan por la transformación digital lo cual, es necesario que se conozcan los diferentes riesgos y vulnerabilidades de seguridad al cual se encuentran expuestos. Este proyecto afectará positivamente a la empresa y al paciente, ya que garantizará la seguridad de los datos que se encuentran alojados en el sistema.

Por otro lado, durante el proyecto se usó la tecnología Blockchain, la cual se encuentra en una etapa temprana en la adopción por diversos rubros en el Perú. Por ello, al ser una

tecnología disruptiva proporciona nuevos conocimientos y aprendizajes en el uso de estos sistemas de información en nuevos escenarios.

Evidencia
Búsqueda de papers de investigación para determinar la tecnología adecuada para proponer una solución al problema identificado
Desarrollo de la plataforma de salud en un framework de Blockchain

Tabla 11. Student Outcome I

2.1.10 Student outcome J: Analizar hechos del mundo contemporáneo identificando el impacto en el desempeño profesional de ingeniería

A lo largo del proyecto se analizaron diversas fuentes sobre ataques informáticos a hospitales, sobre todo en la autenticación para acceder a la información y en ataques a cifrado de datos. Asimismo, para justificar la problemática, se recopilaron y analizaron diversas estadísticas y tendencias en ataques informáticos al sector salud tanto a nivel nacional como a nivel mundial. Además, también se realizaron los análisis de la tecnología propuesta en otros partes del mundo teniendo resultados positivos.

2.1.11 Student outcome K: Utilizar las técnicas, herramientas y metodologías necesarias para la práctica de la ingeniería

En el transcurso del proyecto se realizaron diferentes actividades para la obtención de resultados a corto plazo. Las fases del PMBOK para la dirección de proyectos; así como toda propuesta, es necesario, el respaldo mediante expertos o pruebas realizadas por los usuarios. También, el uso de metodologías ágiles para la entrega de valor en un tiempo determinado denominado sprint.

Evidencia	Descripción
Metodología PMBOK	Se usó la metodología PMBOK para segmentar por partes el desarrollo del proyecto con los entregables requeridos.
Metodologías ágiles	Se usó para entregar valor en un periodo corto durante sprints.

Tabla 12. Student Outcome K

CAPÍTULO 3: ESTADO DEL ARTE

En el presente capítulo “Estado del arte” se presenta la recopilación y el análisis de investigaciones sobre modelos, arquitecturas y aplicaciones relacionadas a la protección de datos clínicos. Esto se basa en criterios de búsqueda a través de bancos de datos reconocidos a nivel mundial. Estos artículos se clasificarán según su aporte y enfoque para la protección de datos clínicos.

Se realizó una evaluación sistemática de literatura de papers teniendo en cuenta las pautas usadas por Kitchenham en su paper “Guidelines for performing systematic literature reviews in software engineering” (Kitchenham, 2007), se han seguido una serie de pasos para proporcionar una metodología efectiva y sistemática:

- Planificación de la revisión: Se elaboran preguntas de investigación y se define el protocolo de búsqueda de fuentes de información.
- Desarrollo de la revisión: En este paso se aplica el protocolo definido en el paso anterior y se obtienen las fuentes principales de información de acuerdo con los criterios definidos.
- Resultados de la revisión: En este paso se presentan los resultados del análisis de las fuentes de información seleccionados anteriormente.

Para la realización de búsqueda de artículos científicos, se plantearon tres preguntas esenciales que abarcan el enfoque de nuestra propuesta.

Pregunta 1 ¿Qué modelos y arquitecturas de seguridad existen para la protección de los datos clínicos de los pacientes durante su almacenamiento en una red interna?

Pregunta 2: ¿Qué modelos y arquitecturas de seguridad existen para la protección de los datos clínicos de los pacientes durante su transmisión?

Pregunta 3: ¿Qué aplicaciones de salud existen para la protección de datos clínicos de los pacientes?

Para el presente proyecto, se utilizaron las siguientes bases de datos: Spring Link, IEEE Xplore Digital Library, AMIA y ACM Digital Library. La investigación abarca el período comprendido entre enero de 2015 y diciembre de 2018. Adicionalmente, se utilizaron las siguientes consultas para la búsqueda de los artículos: (security and mhealth or data), (blockchain AND data Access), (architecture and block-chain or m- health), (security and protocols and mobile healthcare), estos fueron aplicados tanto para las palabras clave de los artículos como para el título y contenido. Luego de ello, se aplicaron los criterios de selección y exclusión mostrados a continuación:

Criterios de inclusión	Criterios de exclusión
Soluciones de seguridad mHealth basados en modelos, arquitecturas, blockchain.	Soluciones de seguridad relacionados a eHealth
La solución propuesta se haya implementado en alguna institución sanitaria.	El artículo sea de un idioma distinto al inglés
Análisis de los problemas de seguridad encontrados en mHealth	El periodo de publicación de los artículos inferior al año 2015
Revistas registradas en Scimagojr	

Tabla 13. Criterios de inclusión y exclusión

A continuación, se presenta una lista de artículos en la siguiente tabla, producto de los criterios de investigación utilizados que han sido extraídos de las bases de datos mencionadas anteriormente.

N°	Título	País	Año	Autores
1	A standard-based model for the sharing of patient-generated health information with electronic health records	Inglaterra	2015	Walter Sujansky Douglas Kunz
2	Tamper-Resistant Mobile Health Using Blockchain Technology	Japón	2017	Daisuke Ichikawa, Makiko Kashiyama, Taro Ueno
3	Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice	España	2017	Achilleas Papageorgiou, Michael Strigkos, Eugenia Politou, Efthimios Alepis, Agusti Solanas, Constantinos Patsakis
4	Analysis of Security Vulnerabilities for Mobile Health Applications	Colombia	2015	Y. Cifuentes, L. Beltrán, L. Ramírez
5	mHealth - Investigating an Information Security Framework for	Inglaterra	2016	Nattaruedee Vithanwattana, Glenford Mapp, Carlisle

	mHealth Data: Challenges and Possible Solutions			George
6	Wearable devices and healthcare: Data sharing and privacy	Australia	2018	Banerjee, S., Hemphill, T., y Longstreet, P
7	Advanced Techniques for Deploying Reliable and Efficient Access Control_Application to E-healthcare	Túnez	2016	Faouzi Jaïdi, Faten Labbene-Ayachi, Adel Bouhoula
8	Designing a Secure Architecture for m-Health Applications	EEUU	2017	Muhammad J. Alibasa, Marlon R. Santos, Nick Glozier, Samuel B. Harvey,
9	Lightweight Sharable and Traceable Secure Mobile Health System.	China	2017	Yang Yang, Ximeng Liu, Robert H. Deng y Yingjiu Li
10	A Physical Layer Security Scheme for Mobile Health Cyber-Physical Systems	EEUU	2016	Rachad Atat, Lingjia Liu, Jonathan Ashdown, Michael Medley, John Matyjas, and Yang Yi
11	Sharing mHealth Data via Named Data Networking	Japón	2016	Haitao Zhang, Zhehao Wang, Christopher Scherb

12	Efficient joint encryption and data hiding algorithm for medical images security	Jordania	2017	Hiba Abdel-Nabi, Ali Al-Haj
13	MedRec:Using Blockchain for Medical Data Access and Permission Management	EEUU	2016	Asaph Azaria, Ariel Ekblaw, Thiago Vieira and Andrew Lippman
14	Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research	EEUU	2016	Laure A. Linn, Martha B. Koo
15	Secure and Trustable Electronic Medical Records Sharing using Blockchain	EEUU	2017	Alevtina Dubovitskaya, Zhigang Xu, Samuel Ryu,Michael Schumacher, Fusheng Wang
16	Advanced blockchain architecture for e-health systems	China	2017	W. Liu , S.S. Zhu, T. Mundie ,U. Krieger
17	Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management	Hungría	2017	Gábor Magyar
	Blockchain: A Panacea for Healthcare Cloud-Based Data Security and	China	2018	Christian Esposito, Alfredo De Santis, Genny

18	Privacy?			Tortora, Henry Chang, Kim-Kwang Raymond Choo.
19	Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications	China	2017	Xueping Liang, Juan Zhao, Sachin Shetty, Jihong Liu y Danyi Li
20	Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems	China	2018	Rui Guoi, Huixian Shi, Qinglan Zhao y Dong Zheng

Tabla 14. Lista de Papers analizados

3.1 Análisis

3.1.1 ¿Qué modelos y arquitecturas de seguridad existen para la protección de los datos clínicos de los pacientes durante su almacenamiento en una red interna?

Artículo 1: “Advanced Techniques for Deploying Reliable and Efficient Access Control Application to E-healthcare”

Hoy en día la atención médica está usando recursos electrónicos, lo cual es un avance importante tanto para la industria sanitaria como para la tecnológica. Asimismo, éstos manejan activos sumamente valiosos como los registros médicos electrónicos de pacientes, por lo cual es un gran desafío para la industria y necesita de mecanismos de seguridad para garantizar la privacidad, integridad y disponibilidad de la información. Los sistemas de e-Healthcare enfrentan varios problemas al definir soluciones de control de acceso rigurosas y flexibles (Jaidi, Labbene-Ayachi, & Bouhoula, 2016). Asimismo, uno de los factores clave requeridos para garantizar la seguridad de los sistemas e-Healthcare, es control de acceso. Los autores estudiarán el problema de la conformidad de las políticas de bajo nivel dentro de las bases de datos relacionales. Asimismo, propondrán una solución avanzada para implementar políticas de control de acceso confiables y eficientes. Esta solución amplía el ciclo de vida convencional de una política de control de acceso y permite principalmente administrar el cumplimiento de la política. Los autores pretenden integrar los controles de acceso de alto nivel con los de bajo nivel, ya que normalmente se trabajan de forma separada.

Descripción del sistema propuesto:

Figura 2. Sistema Propuesto para el control de acceso

El objetivo principal es mantener la coherencia y el cumplimiento entre la definición de alto nivel de una política de control de acceso (definición de la política) y su definición de bajo nivel (la política concreta).

Artículo 2: “Designing a Secure Architecture for m-Health Applications”

Durante un estudio Verizon Data Breach Investigation Review demostró que las infracciones de datos en el sector sanitario han aumentado casi diez veces entre 2014 y 2015. Por otro lado, en (Alibasa, Santos, Glozier, Harvey, & Calvo, 2017) los autores afirman que los registros médicos, para los piratas informáticos, tienen más valor que la información de las tarjetas de crédito. En el presente artículo, los autores proponen una arquitectura de software, la cual está diseñada para separar los datos identificables de los datos no identificables para mantenerse en el anonimato. La anonimización se considera uno de los requisitos de privacidad para la seguridad de los sistemas m-Health. Asimismo, la propuesta está diseñada para aplicaciones web y móviles.

Arquitectura propuesta:

Figura 3. Arquitectura propuesta para un sistema e-Health

Los datos identificables y no identificables tienen distintos grados de sensibilidad. Cada servidor tiene su propia base de datos y aplicación de servicio web. Si los delincuentes informáticos acceden a los datos no identificables, no pueden obtener nada sobre una persona en particular, pero si obtienen acceso a datos identificables, solo pueden observar los nombres y correos electrónicos. Las credenciales de los usuarios se almacenan en la aplicación móvil del cliente, por lo que al desinstalar la aplicación se perderán las credenciales del usuario.

Artículo 3: “Advanced blockchain architecture for e-health systems”

El intercambio universal de datos personales de pacientes provenientes de varias fuentes, requieren métodos clave de procesamiento por el control y el mantenimiento de la integridad de datos, procedencia, privacidad, etc. Además, proporcionar identificación confiable del paciente con protocolos de autenticación y control de acceso. También, mantener la sensibilidad a los problemas culturales, legales y éticos asociados con los datos de salud universalmente accesibles. En este artículo los autores demuestran una arquitectura de Blockchain como un nuevo sistema que permite el intercambio de registros médicos de forma segura y eficiente. El enfoque de la cadena de bloques avanzada fue diseñado para satisfacer las demandas en el crecimiento de atención médica a través de dispositivos electrónicos.

Figura 4. Block-Chain Avanzado

Como se observa en la Figura, hay dos subprocesos de procesamiento dimensional para la cadena de bloques para e-Health. El paciente inicia el bloque generando su información de salud. En los subprocesos verticales de procesamiento, se encuentran los bloques de e-Health procesados por los proveedores de servicios para sus servicios de tratamiento prestados. Cada bloque generado debe estar firmado por todas las partes involucradas antes de su publicación. Antes de que cualquier nodo quiera participar en la red de blockchain, debe estar certificado y emitir un certificado autenticado.

Artículo 4: “Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research”

Este artículo se basa en gran medida en las investigaciones publicadas del Massachusetts Institute of Technology sobre el uso de un blockchain público para gestionar y controlar el acceso a los datos personales. La propuesta implica el uso de blockchain público con un gestor de control de acceso para los registros de salud. Cuando un proveedor de atención médica crea un registro médico (prescripción, prueba de laboratorio, resultado de patología, resonancia magnética) se crearía una firma digital para verificar la autenticidad del documento o imagen. Los datos de salud serían encriptados y enviados al lago de datos para su almacenamiento.

Figura 5. Modelo de Seguridad de Registros Médicos basados en Blockchain

El usuario configuraría transacciones específicas y detalladas sobre quién tiene acceso, el marco de tiempo asignado para el acceso y los tipos particulares de datos a los que se puede acceder. En cualquier momento, el usuario puede modificar el conjunto de permisos. Las políticas de control de acceso también se almacenarían de forma segura en una cadena de bloques y solo el usuario podría cambiarlas. Esto proporciona un entorno de transparencia y permite al usuario tomar todas las decisiones sobre qué datos se recopilan y cómo se pueden compartir los datos. Después de que se le concede acceso a un proveedor de atención médica a la información de salud de un usuario, él consulta el blockchain para los datos del usuario y utiliza la firma digital para autenticar los datos. El proveedor de servicios de salud podría utilizar una aplicación personalizada de primer nivel para analizar los datos de salud.

Artículo 5: “Secure and Trustable Electronic Medical Records Sharing using Blockchain”

Los registros médicos electrónicos son información privada y confidencial en el sector salud y deben establecerse métodos seguros para evitar que esta información caiga en manos de terceras personas. Por otro lado, almacenar y compartir datos entre múltiples identidades, mantener el control de acceso a través de numerosos contratos y el consentimiento puede hacer que el tratamiento no sea el efectivo. También, tener un historial completo sobre el tratamiento de un paciente, por ejemplo, las radiaciones suministradas en un paciente, así como los diagnósticos obtenidos. Asimismo, también confiar en una entidad centralizada que gestione los datos de los pacientes, políticas de control de acceso, significa tener un punto único de falla. En este artículo los autores presentan las perspectivas del uso de Blockchain en los registros médicos de salud, en particular, para compartir los datos entre proveedores de servicios de salud y para estudios de investigación.

Figura 6. Marco seguro para compartir datos clínicos en Blockchain

Artículo 6: “Lightweight Sharable and Traceable Secure Mobile Health System”

Un propietario de datos podría hacer cumplir la política de acceso en el índice de los documentos para realizar la autorización de búsqueda. Sin embargo, se requiere que el sistema vuelva a encriptar los archivos encriptados y actualice las claves secretas de los usuarios para revocar a un usuario. Esto no es adecuado para un sistema mHealth, que tiene una gran cantidad de EHR y una gran cantidad de usuarios. Además, los costos de cálculo de estos esquemas aumentan con la complejidad de las estructuras de acceso. Sin embargo, estos esquemas no proporcionan la función de control de acceso. En este artículo, los autores proponen un sistema de arquitectura, modelo que combate amenazas y requerimientos de seguridad de LiST.

1. Sistema de Arquitectura. Consiste principalmente en cuatro tipos de partes:

- a. Red inalámbrica de sensores corporales (WBSN) que actúa como la función del propietario de los datos,
- b. Personal sanitario que se considera usuario de datos

- c. La nube pública
- d. Centro de generación de claves (KGC).

Figura 7. Sistema de Arquitectura LIST

2. Modelo contra amenazas

Se asume que el KGC es una entidad de plena confianza. En el sistema propuesto, el servidor público en la nube se considera semi- honesto y curioso. Sigue las operaciones predefinidas para realizar búsquedas en EHR en nombre de los usuarios de datos, pero es curioso en el sentido de que intenta derivar información sensible de los EHR almacenados o las palabras clave de texto sin formato de las trampas de palabra clave enviadas por los usuarios.

3. Requerimientos de seguridad de LiST Proceso para Resolver el problema

1. Visión general
2. Construcción concreta
  - a. Configuración del sistema
  - b. Generación de la clave

- c. EHR y encriptamiento de la clave
- d. Generación de la clave de señuelo
- e. Recuperación de datos
- f. Desencriptación de datos y verificación
- g. Rastreo de usuario corrupto
- h. Revocamiento de cuenta de usuario

Figura 8. Interacciones de alto Nivel en la construcción concreta.

Artículo 7: “A Physical Layer Security Scheme for Mobile Health Cyber-Physical Systems”

La salud móvil (m-Health) es una aplicación potencial de los sistemas ciberfísicos (CPS), donde los sensores biomédicos y los dispositivos móviles interactúan estrechamente para transmitir datos médicos a un servidor de m-Health. En este documento, los autores consideran un sistema m-Health jerárquico de tres niveles: i) el nivel de red del sensor que captura las señales vitales; ii) la capa de la red de informática móvil procesa y enruta los datos detectados a una ubicación remota fija; iii) el nivel de red de back-end que procesa y analiza los datos médicos detectados junto con el historial médico del

paciente. Para ello, se ha propuesto un esquema de seguridad de capa física para el nivel de informática móvil en m-Health CPS utilizando herramientas de geometría estocástica. Se tuvieron expresiones derivadas analíticamente para la región de transmisión alrededor de un usuario móvil típico que satisface una probabilidad de confidencialidad, una probabilidad de interrupción de objetivo y una restricción de umbral de retardo. Además, se ha proporcionado un análisis sobre el promedio de la demora de extremo a extremo en un enlace típico. Se compararon las medidas de rendimiento en dos escenarios diferentes: cuando la información sobre los comportamientos de los usuarios está disponible y cuando no está disponible. Además, se consideraron dos casos: i) cuando el usuario móvil transmite al vecino más cercano, y ii) cuando transmite al vecino más lejano. Los resultados numéricos han demostrado que estar equipado con información sobre espías puede beneficiar el rendimiento del sistema en términos de secreto y latencia. Por otro lado, cuando no se puede obtener esa información, siempre es mejor transmitirla al vecino más cercano.

Figura 9. Un sistema de m-Salud jerárquico de tres niveles bajo escuchas

Artículo 8: “Tamper-Resistant Mobile Health Using Blockchain Technology”

Claramente se ha demostrado que los servicios médicos mediante los dispositivos móviles brindan efectos beneficiosos, tanto en la reducción de costos como en la forma de conectar a las personas con

sus proveedores de atención médica. Las aplicaciones móviles ayudan a médicos y pacientes a ser más interactivos en la forma de prestar servicios médicos a través de un monitoreo remoto y un tratamiento en tiempo real de forma independiente a la ubicación del paciente. Estos datos necesitan ser protegidos debido a su alto valor. Los autores desarrollan y evalúan un sistema mHealth a prueba de manipulaciones utilizando la tecnología Blockchain ya que permite la computación confiable y auditable usando una red descentralizada.

Figura 10. Estructura del entorno virtual de la propuesta

Se ha comprobado el correcto envío a la red Blockchain de Hyperledger Fabric privada. Asimismo, se ha verificado que todos los nodos participantes se ejecuten normalmente. Por otro lado, los datos se actualizaron correctamente ante fallas en la red siendo resistente a manipulaciones. También los datos fueron auditables en la red.

Artículo 9: “Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management”

El autor nos da a conocer que, en la actualidad, hay una gran cantidad de sistemas de información de salud separados, que mantienen los datos de los pacientes individuales en enormes silos de información de salud. Para integrar estos silos de datos aislados, se crean y mantienen continuamente una serie de

interfaces. Para resolver el problema de interconectar los diferentes sistemas de registro de datos de salud, ha surgido una amplia gama de protocolos; entre estos no existe uno ampliamente aceptado, por lo que el problema del intercambio de datos sigue siendo un problema cotidiano grave. En el artículo, el autor presenta su modelo de aplicación, explicando cómo solucionará los tres problemas que se encuentran en el contexto. Primero, nos explica acerca de la red de almacenamiento de EMR Healthcare, en él se indica que los productores de información en el caso de una infraestructura basada en cadenas de bloques están proporcionando información hacia la cadena de bloques donde una red incentivada de igual a igual la está emitiendo; durante dicha emisión, cada peer realiza el mismo procedimiento ciñéndose a un sistema de reglas de consenso, lo que da como resultado la validación y seguridad de la información. La validación se produce aplicando las reglas de validez a la información publicada por los actores mientras que la seguridad se realiza mediante un procedimiento de seguridad especial llamado mining, la cual se señala como una actividad demandante de recursos que entierra la información entrante en la cadena de bloques. Segundo, nos explica qué se hará con la disponibilidad de data autorizada y no autorizada. Los servidores con disponibilidad autorizada son aplicados en niveles institucionales y de organización de atención médica. En estos niveles, los permisos se organizan en clases de permisos donde el registro es necesario para los actores individuales que están utilizando los permisos emitidos. El acceso directo a los datos del paciente supone siempre el acceso autorizado donde se identifica al propietario del permiso. Finalmente, el autor nos explica acerca de los incentivos y los costos operacionales, Para ello nos indica que el sistema basado en permisos no necesita incentivos directos, ya que los propietarios del sistema definen los incentivos de manera implícita. Además, son a menudo sistemas patentados donde las reglas de consenso están incorporadas en las reglas de operación. Por otro lado, los sistemas abiertos, sin permiso, deberían tener un incentivo, cuyo valor crea una conexión entre las partes que financian y las que operan. El autor señala que los tokens de salud introducidos pueden ser canjeados por las compañías de seguros y utilizados por los operadores de las máquinas de servicio de almacenamiento y seguridad, de esta manera la sólida red de computadoras de servicio asegura el funcionamiento sin problemas del sistema donde los costos de mantenimiento, respaldo y operación son asumidos por ellos.

Artículo 10: “Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications”

Los hospitales y las instituciones médicas pueden usar datos para vincularlos con otros datos de registros electrónicos de salud, como notas clínicas, para facilitar el monitoreo de la salud, el diagnóstico de enfermedades y el tratamiento. Las compañías de seguros de salud pueden hacer políticas detalladas y estratégicas de acuerdo con las características individuales, lo que beneficia a los clientes a elegir planes de seguro flexibles de acuerdo con sus necesidades. Para manejar el intercambio de datos de salud entre las instituciones, es necesario contar con una infraestructura segura de intercambio de datos. Sin embargo, existen varios desafíos relacionados con la privacidad, la seguridad y la interoperabilidad. En primer lugar, los datos de salud son muy sensibles a la privacidad, especialmente a medida que se almacenan más datos en una nube pública, lo que aumenta los riesgos de exposición de datos. En segundo lugar, los sistemas actuales usan una arquitectura centralizada, que requiere una confianza. Además, la integración efectiva de los datos de salud y la interoperabilidad entre los sistemas de salud sigue siendo una tarea desafiante. Otro desafío es que los usuarios tienen poco control sobre sus datos personales de salud. Por estas razones, en este documento, se presenta un diseño de un sistema de salud móvil para la recopilación, el intercambio y la colaboración de datos de salud personales entre personas y proveedores de servicios de salud, así como compañías de seguros. El sistema también se puede ampliar para acomodar el uso de datos de salud con fines de investigación. Al adoptar la tecnología blockchain, el sistema se implementa de forma distribuida y sin confianza. El algoritmo para manejar los registros de datos puede preservar la integridad y la privacidad al mismo tiempo. Mientras tanto, adoptamos el concepto de canal soportado por Hyperledger Fabric para tratar con la comunicación aislada requerida por escenarios específicos.

Es así como los autores proponen el siguiente diseño:

Los datos de salud personales provienen de dispositivos portátiles como rastreadores de actividad o relojes inteligentes y dispositivos médicos, como marcapasos o desfibrilación, así como la entrada manual del usuario para el seguimiento del tratamiento, como el uso de medicamentos y la capacitación. Para sincronizar los datos personales a la nube para un acceso conveniente y un proceso posterior, el usuario primero puede registrarse en el proveedor de servicios en la nube para obtener una cuenta en línea con suficiente capacidad de almacenamiento.

Figura 11. Recolección de data de Salud Personal.

Por otro lado, los datos de salud provienen de una variedad de dispositivos todo el día, lo que resulta en una gran cantidad de registros de datos, para facilitar el procesamiento de datos se desarrolló un método basado en árbol para la gestión de la integridad del registro de datos de salud.

Figura 12. Protección de la Integridad de Datos de Salud Personal

Finalmente, para el intercambio de datos y colaboración en salud, el usuario puede compartir datos con proveedores de servicios de salud para buscar servicios de atención médica y con compañías de seguros para obtener un presupuesto de la póliza de seguro y para estar asegurado. Cuando se detecta el uso compartido de datos en el sistema, se generará un evento para registrar la solicitud de acceso a datos.

Modelos y Arquitecturas	Descripción
<i>Advanced Techniques for Deploying Reliable and Efficient Access Control_Application to E-healthcare</i>	Modelo para el cumplimiento de las validaciones, verificaciones y el monitoreo del cumplimiento de las políticas de control de acceso de las bases de datos de healthcare. Proponen una solución avanzada para implementar políticas de control de acceso confiable y eficiente.
<i>Designing a Secure Architecture for m-Health Applications</i>	Los autores discuten una arquitectura de software para almacenar y administrar los datos recopilados en aplicaciones de salud móviles. Los datos identificables y no identificables se almacenan en servidores separados y se cifran.
<i>Advanced blockchain architecture for e-health systems</i>	Los autores describen una arquitectura de blockchain como una nueva solución para proporcionar un mecanismo de seguridad en el intercambio de registros médicos. El enfoque del Advance Blockchain fue diseñado para satisfacer las demandas en el crecimiento de la atención médica.
<i>Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research</i>	En este documento se describe un gestor de control de acceso basado en blockchain para los registros de salud, lo cual involucra a los desafíos de interoperabilidad de la industria sanitaria. La infraestructura de TI basada en blockchain tiene un gran potencial para promover el desarrollo de la medicina en precisión, promover el avance en la investigación médica e invitar a los pacientes a ser más responsables de su salud.
<i>Secure and Trustable Electronic Medical Records Sharing using Blockchain</i>	En este documento se presentan perspectivas sobre el manejo de datos de cuidado de salud basado en blockchain, específicamente para compartir datos EMR entre proveedores de servicio de salud y para estudios de

	investigación. Se propone un marco para administrar y compartir datos de EMR para la atención del paciente con cáncer. Se implementa en el hospital Stony Brook University Hospital. El trabajo reduce el tiempo de respuesta para el intercambio de EMR, mejorar en la atención médica y reducir costos.
<i>Lightweight Sharable and Traceable Secure Mobile Health System</i>	Los autores proponen un sistema de arquitectura, modelo que combate amenazas y requerimientos de seguridad de LiST que mejoren el rendimiento en los dispositivos móviles, la seguridad de los datos y las preocupaciones sobre la privacidad.
<i>A Physical Layer Security Scheme for Mobile Health Cyber-Physical Systems</i>	El objetivo de este estudio fue desarrollar y evaluar un sistema mHealth a prueba de manipulaciones utilizando la tecnología blockchain, que permite la computación confiable y auditable utilizando una red descentralizada.
<i>Tamper-Resistant Mobile Health Using Blockchain Technology</i>	El objetivo de este estudio fue desarrollar y evaluar un sistema mHealth a prueba de manipulaciones utilizando la tecnología blockchain, que permite la computación confiable y auditable utilizando una red descentralizada.
<i>Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management</i>	El autor propone la arquitectura de blockchain para ayudar a resolver el problema del almacenamiento seguro de datos y garantizar la disponibilidad de datos ERH al mismo tiempo.

<i>Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications</i>	Los autores presentan el diseño de un sistema de salud móvil para la recopilación, el intercambio y la colaboración de datos de salud personales entre personas y proveedores de servicios de salud mediante el uso de la tecnología blockchain.

Tabla 15. Artículos de modelos y arquitecturas

3.1.2 ¿Qué modelos y arquitecturas de seguridad existen para la protección de los datos clínicos de los pacientes durante su transmisión?

Artículo 11: “Efficient joint encryption and data hiding algorithm for medical images security”

El autor mediante su artículo (Al-Haj & Abdel-Nabi, 2017) indica que las imágenes médicas de los pacientes son de carácter confidencial y requieren de mecanismos de seguridad para evitar que esta información caiga en terceras personas y realicen acciones ilícitas con estos activos. Asimismo, no solo implica que esta información pueda ser vista y divulgada por personas no autorizadas, sino que éstas puedan ser alteradas poniendo en riesgo la vida del paciente cuando un especialista médico toma una decisión en base a un diagnóstico médico modificado. El autor propone dar solución a la seguridad de las imágenes médicas mediante tecnologías de criptografía y marca de agua digital. Donde la primera garantiza la confidencialidad de la información para que pueda ser visto por personas autorizadas, y la segunda donde asegura la integridad de las imágenes. El aporte está conformado de dos procedimientos: Incrustación de datos y extracción de datos.

Figura 13. Diagrama del bloque del procedimiento de incorporación de datos.

Involucra tres etapas principales: en la primera etapa, píxeles de la imagen de portada se barajan aleatoriamente y luego se dividen de manera desigual en dos partes siendo una de mayor tamaño que la otra; en la segunda etapa, se le incorporan dos marcas de agua a la imagen; en la tercera etapa, la parte grande se cifra con AES y se combina con la parte pequeña.

Figura 14. Diagrama de bloques del procedimiento de extracción de datos

Es el inverso directo del procedimiento de incrustación de datos. Primero, la misma clave con que se usó en la incrustación se usa para dividir la imagen en dos partes. Luego la marca de agua de la parte encriptada se extrae para descifrarla.

Artículo 12: “A standard-based model for the sharing of patient- generated health information with electronic health records”

Este documento propone un modelo estándar para la recopilación automatizada de datos de pacientes utilizando dispositivos de salud personales y el intercambio seguro de estos datos con los registros electrónicos de salud de los proveedores autorizados (EHR). El modelo aborda una serie de requisitos importantes para la recopilación práctica y el intercambio de dichos datos entre pacientes y proveedores. Los elementos técnicos del modelo se basan en las características de los dispositivos de salud personales, los repositorios de datos de salud y los estándares de interoperabilidad que ya existen.

Figura 15. Modelo propuesto a alto nivel

El modelo estándar propuesto aquí constituye un "hombre de paja" destinado a fomentar el pensamiento, las discusiones y el refinamiento a través de implementaciones piloto y mejoras. Aunque el modelo se basa en tecnologías y estándares existentes, la combinación específica propuesta aquí aún no se ha utilizado (a nuestro entender) en un entorno de producción para solicitar y recuperar PGHI para proveedores y EHR. Es bastante posible (y probable) que las variaciones de este modelo sean necesarias antes de que sea adecuado para su designación como un componente requerido de la certificación EHR en el programa de uso significativo.

Artículo 13: “Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?”

Los autores a través de su investigación muestran que actualmente la transformación digital está invadiendo varios sectores, entre ellos el sector de salud; la omnipresencia de los dispositivos inteligentes (por ejemplo, dispositivos Android e iOS y dispositivos portátiles) ha dado lugar a un cambio de paradigma en la industria de la atención médica. Estos desarrollos han allanado el camino para los registros personales de salud (PHR), donde los pacientes participan más en su recopilación de datos, el control de sus condiciones de salud, etc, utilizando sus teléfonos inteligentes o dispositivos portátiles. Por ello, el autor presenta como la tecnología Blockchain abarca varios puntos importantes como la seguridad e integridad de los datos en los registros electrónicos de salud. Primero, nos explica la necesidad actual y los beneficios del EMR (Electronic Medical Record), EHR (Electronic Health Record) y PHR (Personal Health Record). Ayudando con la eficiencia en los procesos del centro de salud, analizando mejor la evolución del paciente, ahorrando costos tanto para el paciente, como para el consultorio, ayudando en la toma de decisiones médicas, etc.

Figura 16. Modelo conceptual Cloud basado en EMR/ERH/PHR

Segundo, en el caso del blockchain, el autor explica que esta es una tecnología capaz de construir una base de datos en línea, abierta y distribuida, que consiste en una estructura de datos (también conocida como bloque) que se encuentran vinculados entre sí. Estos bloques se distribuyen entre múltiples nodos de una infraestructura, y no están centralmente almacenados. Cada bloque contiene una marca de tiempo de su producción, del bloque anterior y de los datos de la transacción, y en el contexto de salud, la asistencia sanitaria del paciente, sus datos y la información del proveedor de salud.

La secuencia de una arquitectura blockchain sería la siguiente:

1. Se crean nuevos datos de atención médica para un paciente en particular (por ejemplo, a partir de una consulta u operación como una cirugía).
2. Se crea una instancia de un nuevo bloque y se distribuye a todos los peers presentes en la red del paciente.
3. Después de que la mayoría de los peers hayan aprobado el nuevo bloque, el sistema lo insertará en la cadena. Esto nos permite lograr una visión global del historial médico del paciente de forma eficiente, verificable y de manera permanente. Si no se alcanza el acuerdo, entonces el bloque no

pertenecería a la cadena principal.

4. Una vez el bloque ha sido insertado en la cadena, los datos en cualquier bloque no podrán ser modificados sin modificar todos los bloques subsiguientes. En otras palabras, la modificación se puede detectar fácilmente.

Artículo 14: “Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems”

Los autores reconocen la importancia de los Electronic Health Records, ya que permite a los pacientes poseer el control para generar, administrar y compartir sus análisis médicos con usuarios terceros que ellos consideren relevantes. Sin embargo, en la situación actual, los pacientes comparten sus EHR en las distintas áreas durante los eventos de la vida, lo que hace que los EHR se muevan de una base de datos de proveedor de servicios a otra. Por lo tanto, el paciente puede perder el control de los datos de salud existentes, mientras que el proveedor de servicios generalmente mantiene la administración principal. Por estas razones, los autores proponen construir un esquema de firma basada en atributos (MA-ABS) con múltiples autoridades, para cumplir con el requisito de blockchain en sistemas EHR distribuidos. Aprovechando el ABS con la tecnología blockchain, esta propuesta podría preservar la privacidad de los pacientes y mantener la inmutabilidad de los EHR. A continuación, se detalla la propuesta de los autores. Con respecto a la combinación de propuestas, esto se refiere a crear una nueva propuesta partiendo de la tecnología blockchain y la propuesta de un esquema ABS con múltiples autoridades en un sistema EHRs para predicados monótonos, y el número del emparejamiento bilineal involucrado en Signing aumentado con el número de autoridades, esto se presentó en el artículo “Attribute-based signatures: Achieving attribute-privacy and collusion-resistance”. Con respecto al siguiente aporte, el principal desafío para múltiples autoridades es el ataque de colusión. Para contrarrestar tal riesgo, una semilla de función pseudoaleatoria se comparte en cada dos autoridades y se preserva en secreto. Además, en KeyGen, la clave privada de cada autoridad está integrada en la clave privada del paciente. Según esta estructura, el protocolo resiste los ataques de colusión de las autoridades corruptas. Finalmente, bajo el cálculo de la suposición Diffie-Hellman bilineal, se demuestra que el modelo de oráculo aleatorio, la propuesta tiene una baja probabilidad de sufrir un ataque predicado selectivo y disfruta de la privacidad perfecta para el firmante, lo que asegura la privacidad de la fuga de datos del

paciente. Además, se realiza una comparación entre el método propuesto y otras obras típicas sobre costo y propiedad. Demuestra que esta propuesta generalmente ofrece un mejor rendimiento.

3.1.3 ¿Qué aplicaciones de salud existen para la protección de datos clínicos de los pacientes?

Artículo 15: “MedRec: Using Blockchain for Medical Data Access and Permission Management”

Diferentes tipos de regulación han puesto barreras en el desarrollo tecnológico de la gestión de datos médicos, así como también una serie de sistemas internos incompatibles y direcciones de datos médicos desfragmentados limitan la capacidad de los pacientes para interactuar y hacerlos partícipe de la administración de su historial médico. Los pacientes enfrentan obstáculos para autorizar el intercambio de datos (con otros médicos consultores o incluso miembros de la familia) debido a la falta de una interfaz común o un sistema estándar que orquesta el acceso al registro en las bases de datos. Los autores proponen MedRec, la cual es una solución que permite a los pacientes administrar sus datos, así como también involucrar a los investigadores u entidades externas a involucrarse como mineros de la red Blockchain.

Figura 17. Diagrama de componentes del sistema de MedRec

Como principales beneficios que ofrece esta aplicación son las siguientes:

Registro completo e inmutable de los permisos de autenticación para facilitar el acceso a los datos y auditoría. Autorización de uso compartido de datos, con sincronización de contenido sin cadena de bloques. Interoperabilidad con la infraestructura de almacenamiento de datos existente de los proveedores. Incentivos de minería de Blockchain para investigadores médicos a través de recompensas de metadatos anonimizadas. Interfaz de usuario de diseño intuitivo para el uso del paciente y del proveedor. Se presenta la arquitectura de MedRec, donde el médico agrega un nuevo registro a través de la aplicación. La información se almacena en la base de datos local y se guarda el hash del registro con los permisos correspondientes gracias a Ethereum y una biblioteca API de fondo. El paciente puede descargar su información, previamente haber validado en el blockchain los permisos correspondientes a través del controlador de acceso a la base de datos.

Artículo 16: “Sharing mHealth Data via Named Data Networking”

La principal motivación de los autores es la tendencia del uso de los sistemas mHealth, así como también muestra interés en brindar una mayor seguridad a los datos de los pacientes usando nuevas redes. Una manera de asegurar la integridad y confidencialidad de los datos clínicos durante su transmisión es el desarrollo de aplicaciones mHealth basado en primitivas de red de datos nombrados (NDN), lo cual permitirá brindar una mayor protección a los datos clínicos de los pacientes. NDNFit se experimenta como una aplicación móvil basada en la web donde recopila información de las actividades físicas de los usuarios y muestra estadísticas en base al rendimiento obtenido. Por otro lado, NDNFit pretende ser un ecosistema de servicios siendo los usuarios quienes componen sus propias redes de procesamiento de datos de salud. Asimismo, brinda una autenticación y control de acceso a los datos a nivel de paquetes, en lugar de inferir la autenticidad de los datos de las conexiones TLS. También, propone una comparación entre NDN y TCP / IP para mHealth. El objetivo es mostrar que las primitivas de NDN simplifican la forma en que se pueden llevar a cabo un ecosistema de aplicaciones distribuidas con menos barreras de entrada.

Figure 2: NDNFit namespace and data objects.

Figura 18. NDNFit espacio de nombres y objeto de datos

Artículo 17: “Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice”

El autor a través de su investigación intenta recopilar estudios previos que involucren la seguridad de la información de diversos tipos de pacientes, de esta forma evidenciar la vulnerabilidad a la que se encuentran expuestos los usuarios. La investigación realizada por el autor evidencia un problema que se incrementa, ya que como se mencionó la demanda por el uso de tecnología y aplicaciones en general ha aumentado. Por tal motivo la data que los usuarios almacenan en sus dispositivos, en decir la información privada debería mantenerse como tal, confidencial. Para esto, se proporciona un análisis de las inquietudes de seguridad y privacidad en las aplicaciones m-health a través de la evaluación, monitoreo y registro, a largo plazo, del ciclo de vida completo de las aplicaciones, entre enero del 2016 y agosto del 2017.

- Evaluación la calidad de todos los canales de comunicación.
- Realización de una investigación en la cual pone en evidencia la forma en que los desarrolladores de aplicaciones respondieron a los informes de seguridad.
- Desarrollo de un procedimiento de auditoría de cumplimiento GDPR para determinar si las aplicaciones revisadas cumplen con los nuevos requisitos legales de la Unión Europea.

Asimismo, el autor propuso lo siguiente para resolver el problema

1. Criterios de recopilación de aplicaciones
  - a. Criterio 1: La aplicación debe ser libre
  - b. Criterio 2: El contenido de la aplicación debe estar en inglés
  - c. Criterio 3: La aplicación requiere conocer datos personales y de salud para ser funcional y, de acuerdo con su descripción, se espera que transmita los datos de los usuarios a un host remoto
  - d. Criterio 4: La aplicación debe tener al menos 100.000 descargas y una calificación mínima de 3.5 / 5 estrellas en Google Play.
2. Metodología de evaluación para investigar las características de seguridad y privacidad que ofrece cada aplicación: La metodología adoptada para evaluar las 20 aplicaciones recolectadas de m-health tiene como objetivo responder a las siguientes tres

preguntas principales de investigación:

- o ¿Qué partes tienen acceso a los datos personales de la aplicación?
- o ¿A qué datos exactos puede acceder cada parte?
- o ¿Qué tan seguro es cada canal de comunicación?

Artículo 18: “Analysis of Security Vulnerabilities for Mobile Health Applications”

En este documento, los autores presentan un análisis de las vulnerabilidades de seguridad para las aplicaciones mHealth, de acuerdo con las siguientes categorías: información médica, educación y concientización, monitoreo de control remoto, soporte diagnóstico, soporte de tratamiento y comunicación y entrenamiento para trabajadores de la salud. Esta investigación se realiza con la finalidad de analizar las aplicaciones mHealth para poder adquirirlas de manera personal o a nivel de organización. Es por ello, que los autores proponen un análisis de las vulnerabilidades de seguridad utilizando los criterios de OWASP para determinar el riesgo de ataque en las aplicaciones mHealth para dispositivos móviles basados en Android. La evaluación de seguridad solo considera el análisis del código APK. Un archivo APK es un archivo ZIP con el ejecutable. Si este código tiene una falla de seguridad, puede afectar negativamente la confidencialidad, integridad y disponibilidad de la información registrada en las aplicaciones de mHealth. Además, el mercado tiene disponibles diferentes tipos de escáneres que realizan pruebas de vulnerabilidad con ataques conocidos, y tiene una alta efectividad en la detección de ataques; esto se puede usar para este tipo de análisis. Es importante que los desarrolladores y usuarios de aplicaciones mHealth móviles intenten crear conciencia sobre los estándares de seguridad que se deben implementar al momento de desarrollar o actualizar este tipo de aplicaciones. Con la evaluación de riesgos analizada con OWASP, es posible concluir que las vulnerabilidades son principalmente desencadenadas por la aceptación de datos de diferentes fuentes. Es importante establecer mecanismos con limitaciones en fuentes de información empleadas por las aplicaciones, lo que mejoraría la confianza en el lado del usuario final.

Artículo 19: “mHealth – Investigating an Information Security Framework for mHealth Data: Challenges and Possible Solutions”

Se ha demostrado claramente que las soluciones de mHealth brindan más atención médica centrada en el paciente y mejoran la eficiencia general de los sistemas de atención médica. Además, estas soluciones pueden reducir potencialmente el costo de proporcionar atención médica en el contexto de las crecientes demandas del envejecimiento de la población en las economías avanzadas. Además, el uso de Cloud Computing se está convirtiendo en una opción para que el sector de la salud almacene datos de atención médica; pero el almacenamiento de datos en la nube plantea serias preocupaciones. Es por esto, que los autores realizan un análisis de lo que sería la integración del mHealth y la nube y también mencionan las consideraciones que se deben tener sobre las aplicaciones que intervienen en este proceso. Se tiene que garantizar que solo las aplicaciones o dispositivos que hayan sido aprobados puedan acceder a los datos de atención médica. Por lo tanto, es necesario que existan requisitos legales que controlen la extracción de datos sanitarios en términos de protección de datos personales y directrices éticas. Adicionalmente se debe incluir restricciones con respecto a qué aplicaciones se pueden instalar en el dispositivo o verificar las firmas digitales en las aplicaciones para garantizar que solo las aplicaciones de entidades de confianza estén instaladas en el dispositivo y ese código no se haya modificado. Cloud brinda a los clientes la oportunidad de almacenar su información en la nube de forma remota y utilizar aplicaciones de alto rendimiento bajo demanda. el modelo de implementación en la nube será dictado por el tipo de aplicación que se mueva a la nube. Inicialmente, las implementaciones en la nube para aplicaciones clínicas echarán raíces en nubes privadas o híbridas dado que estas aplicaciones requieren el más alto nivel de seguridad, privacidad y disponibilidad. Finalmente, el objetivo de esta investigación es que si bien es cierto que Cloud aporta en la inclusión de los dispositivos mHealth, hay que tomar otras consideraciones al momento de incorporar aplicaciones con permisos y accesos a la información que será alojada en este entorno.

Artículo 20: “mHealth – Investigating an Information Security Framework for mHealth Data: Challenges and Possible Solutions”

Estos problemas mencionados son actualmente desafíos clave en la salud móvil. Se debe hacer frente a los que tienen derecho a acceder a los registros de salud, los pacientes o profesionales de la salud, y garantizar que sólo las aplicaciones o dispositivos que han sido aprobados serán capaces de acceder a los datos de salud. Es por ello que es necesario que debe haber requisitos legales que controlan la

extracción de datos de los datos de salud en cuanto a la protección de datos personales, así como las normas éticas. Por ejemplo, un tercero (fuera de la relación médico-paciente) debe recibir permiso de un paciente con el fin de utilizar su / sus datos personales antes de realizar la investigación futura en la asistencia sanitaria.

El autor nos da a conocer que la gestión de datos de la salud móvil en Cloud tiene un cierto conjunto de desafíos como: Los datos pueden estar en cualquier lugar en la nube, no son estáticos, el proveedor de la nube podría replicar datos por razones legítimas, la administración del proveedor de la nube necesita acceder al bloque físico con el fin de optimizar el entorno de la nube; además, debido a la virtualización de la nube de usuario, si los datos ha sido manipulado, es muy difícil descubrir cómo y cuándo se produjo dicha manipulación; los servicios móviles significan que los servicios son ahora móvil, por lo que es difícil realizar un seguimiento de lo que hacen los servicios de datos; por lo tanto, es difícil descubrir las violaciones de datos utilizando la nube. Es por ello, que el autor realiza un análisis de lo que sería la integración del mHealth y la nube y también menciona las consideraciones que se deben tener sobre las aplicaciones que intervienen en este proceso. Se tiene que garantizar que solo las aplicaciones o dispositivos que hayan sido aprobados puedan acceder a los datos de atención médica. Por lo tanto, es necesario que existan requisitos legales que controlen la extracción de datos sanitarios en términos de protección de datos personales y directrices éticas. Adicionalmente se debe incluir restricciones con respecto a qué aplicaciones se pueden instalar en el dispositivo o verificar las firmas digitales en las aplicaciones para garantizar que solo las aplicaciones de entidades de confianza estén instaladas en el dispositivo y ese código no se haya modificado.

3.2 Conclusiones

En conclusión, se ha podido observar en diversas investigaciones científicas sobre los desafíos de seguridad que está siendo frente el mHealth. Asimismo, existen soluciones de seguridad a los datos clínicos en representación de arquitecturas, modelos o algoritmos que brinden seguridad garantizando la disponibilidad, integridad, confidencialidad y autenticidad llegando a la conclusión que cada uno de ellos puede abordar uno o dos de los mismos. Por otro lado, se ha concluido que la tecnología blockchain puede garantizar tanto la integridad de sus datos mediante la cadena de bloques, la disponibilidad mediante la distribución del libro mayor y la sincronización de la información cuando éste se restaure, confidencialidad mediante sus algoritmos complejos y los recursos computacionales que se necesita para generar bloques y agregarlos a la cadena.

También, se ha observado diversas arquitecturas como software, redes que aportan a la seguridad de los datos clínicos durante su etapa de transición. Este es un factor clave ya que se puede lograr un alto nivel de seguridad a nivel de perímetro, pero mientras si lo que se encuentra alrededor no se protege, la información clínica que ingrese pudo haber sufrido alguna modificación por algún malintencionado durante su etapa de transición. Por ello, otro problema y enfoque a abordar es la seguridad de los datos cuando éstos están en tránsito.

Por último, se pretende realizar un modelo de seguridad de los datos clínicos para dispositivos mHealth basado en la tecnología Blockchain. Para llegar a la tecnología a basar se ha tenido que analizar diversas soluciones bajo esta tecnología, revisando el impacto que éste genera, las brechas de seguridad que estas soluciones cubren y donde se ha implementado.

CAPÍTULO 4: MARCO TEÓRICO

En el presente capítulo se definen los principales conceptos relacionados al proyecto, conceptos enfocados en la protección de los datos clínicos de los pacientes por medio de los dispositivos que se utilizan para la captación e interpretación de los datos. Entre las principales definiciones se encuentra el ecosistema mHealth, la cual es el enfoque en el sistema sanitario en la que se basará el proyecto. Asimismo, se indicarán las principales amenazas a las que este sistema está expuesto. También, la tecnología Blockchain como tal, de manera que será el soporte que permitirá brindar una solución de seguridad a los datos clínicos de los pacientes. Además, se definirá a grandes rasgos cómo la tecnología Blockchain interviene en la prestación de servicios de salud a distancia mediante los dispositivos mHealth.

4.1 Antecedentes

Los datos de salud personales de cada paciente proporcionan información importante a las empresas interesadas (proveedores) involucradas en el área de salud y a las investigaciones médicas; sin embargo, los datos, en general, no están protegidos para un adecuado manejo de información. Por ejemplo, las Historias Clínicas del paciente, según la normativa decretada por el Minsa - Ley N 30024 indica que se deben salvaguardar de manera electrónica estos datos a través de formularios digitales, por lo que los datos sensibles del paciente están expuestos: Anamnesis, diagnóstico, plan de trabajo (exámenes o interconsultas) y las recetas. En este sentido, los sistemas que almacenan los datos del paciente son vulnerables a posibles extracciones de datos, por lo que surgieron algunas investigaciones para gestionar el intercambio de datos de salud centrada en el usuario basado en Blockchain. Blockchain se inicia a partir del nacimiento de la criptomoneda denominada Bitcoin.

Figura 19. mHealth como tecnología emergente

En azul vemos como el término mhealth acaba ganando popularidad en nuevas tecnologías emergentes.

En líneas generales, esta tecnología estructurada de forma consistente por bloques almacenados y mantenidos dentro de una red a la que denominaron red Blockchain; se basa en el pseudo anonimato (reemplazando nombres con identificadores) y la infraestructura de clave pública para mantener la privacidad de los usuarios. La estructura protege los datos personales de los ataques

cibernéticos y al mismo tiempo mantiene un registro visible de dónde se originaron los datos en la cadena de bloques.

4.2 mHealth

Según la Organización Mundial de Salud (OMS), mHealth se define como: “... la práctica de la medicina y la salud pública soportada por dispositivos móviles como teléfonos móviles, dispositivos de monitorización de pacientes, asistentes personales digitales y otros dispositivos inalámbricos”. Se ha visto la gran evolución de los dispositivos inalámbricos como smartphones, wereables, PDA's, etc la cual permite la facilidad en este tipo de servicios. Asimismo, IBSG de Cisco (Evans, 2011) calculó que en el 2020 habrá 50,000 millones de dispositivos conectados a internet lo que se estima que en promedio una persona tendrá 6.58 aparatos. El mHealth permite al médico monitorear constantemente nuestro estado de salud mediante dispositivos como los sensores o wearables y móviles como se observa en la siguiente figura:

Figura 20. Infraestructura mHealth

A continuación, una estructura básica sobre mHealth:

Figura 21. Escenario de mHealth

Figura 22. Enfoque Cloud para Electronic Medical Records

4.3 Blockchain

La tecnología Blockchain permite a los usuarios compartir su contabilidad de transacciones. El registro de eventos que ocurren en la red de blockchain se distribuye a todos los participantes de la red, quienes a su vez usan sus computadoras para validar las transacciones; eliminando así la necesidad de tener un intermediario externo como un banco o un centro de compensación central. Los registros de Blockchain solo pueden actualizarse por consenso de la mayoría de los participantes en el sistema y, una vez ingresados, la información nunca puede borrarse, proporcionando un seguimiento de auditoría detallado de todos los eventos asociados.

Figura 23. Figura del flujo de trabajo de Blockchain
(Cusack, 2017)

El sector de la salud no es ajeno a esta moda, ya que blockchain también se puede extender a la cadena de suministro de medicamentos y sobre todo al almacenamiento e intercambio de información, principalmente en cinco aspectos:

- La historia clínica de los pacientes.
- La información generada en ensayos clínicos.
- Los datos genómicos.
- La información generada por los propios pacientes a través de dispositivos conectados (IoT – Internet of Healthcare Things).
- Los procesos de reclamación y pago de servicios sanitarios asegurados.

Una de las características resaltantes en la tecnología es que si se cambia cualquier Bit/dato en el desarrollo del transporte o recepción de los datos, éste y todos los siguientes a partir de él son invalidados. Si a esta característica se añade que el modelo de almacenamiento distribuido puede contener una gran cantidad de nodos en los que se replica la información tenemos un sistema donde “un montón de gente se puede poner de acuerdo sobre lo que sucedió en el pasado”; es decir, Blockchain almacena un historial durante cada recorrido por sus nodos, por lo que se puede recrear diferentes pasos o historial de acuerdo con los estudios nodos. Sobre esta base se vislumbra que el valor de esta tecnología radica en su capacidad de:

Transparencia:

- Compartir de forma fácil y ser visible para todos los participantes son características importantes y que pueden ser aprovechadas en aquellos entornos que carecen o que necesiten de transparencia.

Confianza:

- La inmutabilidad de la cadena de bloques hace casi imposible que se realicen cambios una vez creados, lo que aumenta la confianza en la integridad de los datos y reduce las oportunidades de fraude.

Desintermediación:

- Con Blockchain el protocolo de consenso acordado por todos los miembros de la red garantiza que se almacenarán y verificarán sólo aquellas transacciones permitidas por los participantes, haciendo innecesaria la existencia de un tercero, eliminando costes, retrasos y reduciendo la complejidad.

Colaboración:

- Blockchain puede programarse para ejecutar transacciones de forma consecutiva lo que facilitará a los participantes colaborar en la creación de procesos conjuntos.

Seguridad:

- El hecho de que el protocolo de Blockchain utilice clave pública y privada consigue que la seguridad en las transacciones y la confidencialidad sean máximas. También se pueden establecer cadenas públicas abiertas, compartidas o privadas en las que la participación se limita a entidades previamente aceptadas.

Blockchain ofrece el potencial para hacer frente a la falta de comunicación de red y una vista dispersa de las transacciones en la arena proveedor. También puede proporcionar una defensa contra el fraude y el abuso. Con la colaboración fluida no sólo dentro, sino a través de redes, y la visibilidad de las transacciones de los pacientes y los resultados mensurables, blockchain puede ser un elemento clave en la implementación de la atención basada en valores.

4.5 Internet de las cosas

A inicios del 2000, el concepto de interconectar los objetos cotidianos con la red y personalizar los resultados en base a nuestros intereses se denominó IoT. En el ambiente de salud, los emprendimientos de tecnología están tomando, formando desde la aparición de los wearables para poder medir nuestras condiciones de salud y analizar nuestra información para brindarnos detalles de nuestro estado físico. La tendencia de innovar e interconectar cualquier dispositivo cotidiano con internet y sus beneficios continuará por lo próximos años, por lo que será necesarios parametrizar, en el sector salud, los datos que serán enviados y analizados dentro un entorno controlado.

Figura 24. Lista de tipo información consumido por wearables

(Huang , 2015)

Como se sabe los dispositivos IoT presentan una gran variedad de vulnerabilidades de seguridad, se estima que el 70% de los dispositivos son vulnerables a los ataques más simples (Pagnotta, 2014), esto involucra el robo de contraseñas hasta el control total del dispositivo afectando la integridad de los datos poniendo en riesgo la vida del paciente. Asimismo, la empresa tecnológica HP realizó un estudio de investigación relacionado a la seguridad de IoT llegando a las siguientes conclusiones:

- El 80% de dispositivos IoT no requirió contraseñas complejas y de varios caracteres.
- El 70% de dispositivos IoT no cifra las comunicaciones a Internet y a la red local.
- El 60% de dispositivos IoT planteó problemas de seguridad con sus interfaces de usuario.
- El 60% de dispositivos IoT no utiliza cifrado al descargar actualizaciones de software (HP, 2014)

Múltiples dispositivos electrónicos que se encuentran conectados entre sí pueden proporcionar volúmenes de datos significativos en cuanto a cantidad. Estos datos pueden estar ligados a historias clínicas del paciente que permiten visualizar la información detallada de cada consulta a lo largo

de su vida. Estos datos ayudan a los doctores o enfermeras a supervisar el estado actual de los pacientes en base a sus afecciones pasado o presente, ya que el profesional tendrá la información en un solo sistema. Por esta parte, IoT se utiliza para la supervisión de los pacientes a través de los wearables o gadgets que indicar el estado del paciente en tiempo real. Si se habla de IoT para el sector salud, las tecnologías más avanzadas son los sensores implementados en los equipos: celular, relojes, gadgets. El sin fin de herramientas que permite controlar el ritmo cardíaco, la presión arterial y puede predecir hasta la diabetes y a seguir una rutina diaria de ejercicios para pacientes que requieran desarrollo físico.

4.6 Compartición de datos P2P

Peer to peer es una red informática que permite que los usuarios y sus bloques (nodos) sean pseudónimos de manera predeterminedada; es decir, este tipo de transmisión y compartición de datos se realizarán de manera anónima. Por ejemplo, para descargar un archivo a través de redes P2P, los ficheros de la descarga se separan en pequeñas partes para su traslado, luego los usuarios solicitan diferentes partes al distribuidor (servidor). En este sentido, esos mismos usuarios se convierten en servidores adhoc para los bloques que están solicitando.

Figura 25. Comunicación peer – to peer

La diferencia entre este tipo de red y las habituales radica en el método y tipo encaminamiento de las distintas arquitecturas de redes (permiten el flujo libre de información). Dentro del tipo de redes que pertenecen a esta estructura se definen: La centralizada mantiene un directorio en un servidor central. La descentralizada y estructurada que también es conocida como una red híbrida y la descentralizada y no estructurada que establece que no existen computadoras o nodos que funcionan como controladores centrales de peticiones. Todos los nodos funcionan como clientes y como servidores.

Finalmente, si bien es cierto que Blockchain funciona como un libro de bloques compartidos confiables y públicos de transacciones que todos pueden inspeccionar pero que ningún usuario final controla, el funcionamiento utiliza un encriptamiento del protocolo blockchain dentro de una red BC. Este comportamiento utiliza el concepto de usuario-servidor donde el cliente se vuelve un usuario y un servidor para el nuevo solicitando que requiera el bloque obtenido por el host.

4.7 Blockchain en el sector Salud

En los últimos tiempos se ha visto el avance innovador en la prestación de servicios de salud usando las tecnologías de información y comunicaciones. Asimismo, se puede observar que se involucra más al paciente como parte de los procesos de atención médica, así como también garantizar la seguridad de los registros clínicos del paciente, es ahí donde entra blockchain que garantiza la integridad y confidencialidad de los datos del paciente brindándole la potestad a los dueños de los datos el control de la gestión de accesos a la información.

Cuando se crean nuevos datos de atención médica para un paciente en particular (por ejemplo, a partir de una consulta y una operación médica, como una cirugía), se crea una instancia de un nuevo bloque y se distribuye a todos los pares en la red del paciente. Después de que la mayoría de los pares hayan aprobado el nuevo bloque, el sistema lo insertará en la cadena. Esto nos permite lograr una visión global del historial médico del paciente de una manera eficiente, verificable y permanente. Si no se alcanza el acuerdo, se crea una bifurcación en la cadena y el bloque se define como huérfano y no pertenece a la cadena principal. Una vez que el bloque se ha insertado en la cadena, los datos en cualquier bloque dado no se pueden modificar sin modificar todos los bloques

posteriores garantizando la integridad de la información (Esposito, De Santis, G., Chang, & Choo, 2018).

Figura 26. Flujo de trabajo de blockchain enfocado en EHR

4.8 Normativas internacionales reguladoras de Blockchain en el sector Salud

El almacenamiento de los datos de los pacientes plantea numerosos factores a tomar en cuenta. Con el fin de cumplir con las leyes definidas para la privacidad, seguridad para el acceso a los datos clínicos de las personas, las instituciones han invertido en mejorar los sistemas que almacenan estos datos. Sin embargo, el impacto de estos esfuerzos ha disminuido debido a las cambiantes y crecientes necesidades de la industria y las nuevas incorporaciones de tecnologías asociadas al sector salud y del gobierno.

En abril el año 2016 Standards Australia presentó un nuevo campo de actividad técnica propuesta (NFTA) por la Organización Internacional de Normalización (ISO) para considerar el desarrollo

de normas para apoyar la tecnología blockchain. La propuesta de un NFTA a la ISO estaba destinado a establecer un nuevo comité técnico ISO para blockchain. El nuevo comité sería responsable de apoyar la innovación y la competencia cubriendo temas de estándares de interoperabilidad, la terminología, privacidad, seguridad y auditoría. En septiembre de 2016, ISO Australia anunció que gestionará la Secretaría de ISO / TC 307 después de que la Organización Internacional de Normalización (ISO) aprobó la propuesta para las nuevas Normas Internacionales de blockchain. En este momento hay 33 países miembros de ISO / TC 307, incluyendo: Alemania, Reino Unido, Japón, Rusia, Francia, Singapur, China, EE.UU. y muchos otros.

Uno de los aspectos más importantes de un sistema de salud es la forma en que sus datos se comparten a través de los procesos en la cadena de valor. Blockchain admite el uso compartido de información sin que pueda eliminar las duplicaciones, errores e inconsistencias que pueden surgir con el almacenamiento de datos tradicional; es decir, esta tecnología elimina el intermediario que existe entre la petición de un servicio o transacción con el que recibe dicha petición como una solicitud.

El uso de Blockchain en salud y la atención al paciente exige la participación de múltiples partes interesadas, incluidos los proveedores, planes de salud y los gobiernos individuales. La unificación de este grupo para formar las normas será un reto. Debido a la naturaleza de la información del cuidado de la salud, tener seguro de datos es de gran importancia. Existen múltiples soluciones para abordar los problemas de privacidad, como se centra en la cadena valor de Blockchain para proporcionar evidencia de hechos inalterables al escribir el hash de las transacciones durante el envío o recepción de información, mientras que las propias transacciones se almacenan fuera del Blockchain. Esto mantiene la integridad de las transacciones, al tiempo que permite la capacidad de borrar las transacciones. Mientras Blockchain ofrece una solución potencial a un aspecto de la seguridad, se requerirá medidas adicionales para asegurar que los datos son seguros.

Healthcare Industry Challenge	Blockchain Opportunities
Fragmented Data	• Decentralized storage using computer networks for patient data • Shared data across the network and nodes • Decentralized source of Internet of Things (IoT) data
Timely Access to Patient Data	• Distributed, secure access to patient health data across the distributed ledger • Shared data enables real-time updates across the networks
System Interoperability	• Decentralized Internet and computer networks across geographies • Enables authenticity (system authentication)
Data Security	• Digitizing data security of transactions – digital identity protects patient privacy
Patient Generated Data	• Data from wearable devices (IoT) aggregated to provide holistic patient care
Access and Data Inconsistency	• Smart Contracts create a consistent and rule-based method for accessing and analyzing patient data that can be permissioned to selected health organizations
Cost Effectiveness	• Reduced transaction costs and real-time processing to make the system more efficient • Elimination of third-party applications removes time lag in data access

Figura 27. Retos y oportunidades en la seguridad en el sector salud Blockchain

En la actualidad, las nuevas tecnologías emergentes no están reguladas en particular para su uso o aplicación detallada. Sin embargo, como a nivel general, estas tecnologías se rigen a normas generales establecidas por el sector al que están destinados. En este caso, Blockchain se encuentra reguladas a nivel de salud por las leyes detalladas a continuación.

4.9 Reglamento general de protección de datos

El reglamento general de protección de datos (RGPD) es el reglamento opcional a la protección de las personas físicas respecto al manejo o gestión de los datos físicos de las personas o usuarios que son almacenados o gestionado en un entorno controlado. El RGPD describe al principio de la responsabilidad proactiva como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento. En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben determinar de forma explícita la forma en que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión. A nivel de salud, uno de los puntos esenciales es el consentimiento. El RGPD señala que el paciente “debe dar su consentimiento explícito al tratamiento de sus datos”. Muchos centros tendrán que incluir una hoja de autorización en los historiales y ficheros para su posterior archivo; dentro de estas normas se puede establecer una relación con los siguientes artículos:

Artículo 15. Concede a los ciudadanos el derecho de acceso que requiere empresas para detallar qué datos personales se está procesado.

Artículo 17. Concede a los ciudadanos el derecho a ser olvidados y a la supresión de datos que requiere que las empresas detengan procesamiento y eliminación de datos personales bajo petición.

Artículos 20. Concede a los ciudadanos el derecho a la portabilidad de los datos para permitir a los ciudadanos transferir datos personales entre empresas a petición.

Artículos 25, 32. Requieren que las empresas implementen datos razonables medidas de protección para proteger a los ciudadanos personales datos y privacidad por diseño.

Artículos 33, 34. Requieren que las empresas denuncien violaciones de datos a las autoridades de supervisión y a las personas afectadas por una violación dentro de 72 horas.

Artículo 35. Requiere que las empresas realicen un impacto en la protección de datos evaluaciones para identificar los riesgos para los datos de los ciudadanos de la UE y esbozar medidas para garantizar que se aborden esos riesgos.

Artículo 37. Requiere que ciertas empresas designen protección de datos funcionarios para supervisar la seguridad de los datos de la estrategia y GDPR.

En el sector de salud en Perú existen normas que protegen los datos del paciente y que son almacenados en sistemas que se basan en una arquitectura tecnológica (sea una tecnología nueva o no). En este caso, las tecnologías emergentes como Blockchain deben adaptarse en el proceso traslado e interpretación de los datos del usuario deben seguir ciertas normativas tal como indica la norma:

“El paciente o usuario de salud debe brindar un consentimiento a través de su firma en virtud del tratamiento de sus datos sensibles contenidos en la historia clínica electrónica (ver Anexo N° 11), conforme a lo señalado en la Ley N° 29733, Ley de Protección de Datos Personales. Dicho consentimiento se exceptúa en caso de que el tratamiento de sus datos sensibles se realice en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del paciente o usuario de salud, observando el secreto profesional, en caso de que medien razones de interés público previsto por la Ley, o cuando se realicen estudios epidemiológicos siempre que se apliquen procedimientos de disociación adecuados.”

CAPÍTULO 5: DESARROLLO DEL PROYECTO

En este capítulo, se describe el desarrollo del proyecto que se basa en el benchmarking realizado donde se analizan algunas soluciones al problema identificado; en base a los resultados obtenidos, se presenta el modelo propuesto con el diseño de la solución y la implementación realizada.

5.1 Benchmarking

Como parte del desarrollo del proyecto se realizó un análisis sobre los diversos modelos y arquitecturas de seguridad para los datos clínicos, asimismo se realizó una investigación sobre la tecnología de Blockchain.

Para llevar a cabo este análisis, se utilizó la metodología del Benchmarking tomando como referencia atributos de seguridad para el entorno mHealth los cuales están priorizados en función a su importancia en dicho ambiente:

1. Disponibilidad
2. Integridad
3. Autenticación
4. Confidencialidad

Se analizaron 6 artículos científicos compartiendo diversas tecnologías enfocados en la seguridad de los datos clínicos:

5.1.1 Diseñando una arquitectura segura para aplicaciones m-Health

En esta propuesta, se discute una arquitectura para almacenar y administrar los datos recopilados en aplicaciones móviles de salud. Los datos identificables y los datos no identificables se almacenan en servidores separados bajo un sistema de cifrado seguro.

Se aplica un listado sobre el cumplimiento de los atributos de seguridad:

	Arquitectura de Software para mHealth	Aplica
Autenticación	Ambos servidores en el diseño solicitan claves secretas o tokens RSA de aplicación antes de que el cliente pueda comunicarse con ellos.	x
Confidencialidad	Cifrado AES	x
Integridad	NO APLICA	-
Disponibilidad	Equilibradores de Carga , limita los puertos abiertos solo para los usos de los servicios necesarios.	x

Tabla 16. Tabla de evaluación para arquitectura de evaluación para mHealth

Fuente: Elaboración Propia

5.1.2 Compartir datos de mHealth a través de redes de datos nombrados

Se propone una aplicación distribuida de salud móvil (mHealth) en base a la arquitectura de red de datos nombrados (NDN). Asimismo, se analiza el diseño y la implementación inicial de un prototipo de NDNFit. También, se identifican importantes diferencias entre la red de datos nombrados y TCP/IP para mHealth.

Se aplica un listado sobre el cumplimiento de los atributos de seguridad:

	Arquitectura de red de datos nombrados (NDN)	Aplica
Autenticación	Control de acceso basado en nombre (NAC). Control de acceso centrado en los datos con las relaciones básicas entre las claves	x

Confidencialidad	Clave de cifrado KEK y clave de descifrado KDK	x
Integridad	NO APLICA	-
Disponibilidad	NO APLICA	-

Tabla 17. Tabla de evaluación para arquitectura de red de datos nombrados

Fuente: Elaboración propia

5.1.3 Sistema liviano de salud móvil seguro y rastreable

Se propone un sistema que combate amenazas y requerimientos de seguridad con la finalidad de mejorar el rendimiento de los dispositivos móviles, la seguridad de los datos y las principales preocupaciones sobre la privacidad de los datos clínicos.

Se aplica un listado sobre el cumplimiento de los atributos de seguridad:

	Arquitectura basada en LIST	Aplica
Autenticación	Centro de generación de claves (KGC)	x
Confidencialidad	Encriptación ligera mediante un algoritmo de cifrado	x
Integridad	NO APLICA	-
Disponibilidad	Nube Pública	x

Tabla 18. Tabla de evaluación para arquitectura basada en LIST

Fuente: Elaboración Propia

5.1.4 MedRec: Uso de Blockchain para acceso a datos médicos y gestión de permisos

MedRec es una aplicación que gestiona los registros de manera descentralizada utilizando la tecnología Blockchain. Asimismo, gestiona la autenticación, confidencialidad, responsabilidad y el intercambio de datos. Por otro lado, incentiva a interesados médicos como investigadores y autoridades de salud pública para que participen en la red como "mineros" en la red de Blockchain.

Se aplica un listado sobre el cumplimiento de los atributos de seguridad:

	Blockchain (Ethereum)	Aplica
Autenticación	Database Gatekeeper para la gestión de los permisos de usuarios basado en roles (RBAC).	x
Confidencialidad	Clave Pública y Clave Privada	x
Integridad	Hash criptográfico Keccak-256 , la cual genera un texto de 256 bits usado por Ethereum.	x
Disponibilidad	Descentralización de la información en una cadena de bloques	x

Tabla 19. Arquitectura de evaluación para mHealth

Fuente: Elaboración Propia

5.1.5 Un enfoque Blockchain aplicado a una plataforma de tele dermatología en la región de Cerdeña

Se presenta un enfoque basado en la tecnología Blockchain con la finalidad de brindar nuevas funcionalidades seguras a una plataforma existente para tele dermatología la cual se implementó en una ciudad italiana. Dentro de estas nuevas funcionalidades incluyen el dar acceso completo al paciente a sus registros médicos manteniéndola segura a nuevas amenazas.

Se aplica un listado sobre el cumplimiento de los atributos de seguridad:

	Blockchain (Ethereum)	Aplica
Autenticación	Administrado a través de un contrato inteligente en la capa de aplicación descentralizada	x
Confidencialidad	La información para cada solicitud de paciente se codifica utilizando cifrado simétrico y, por lo tanto, se utiliza la misma clave de cifrado para cifrar y descifrar datos	x
Integridad	Decentralized Ledger Technology (DLT) genera confianza y garantiza la integridad de los datos sin la necesidad de una tercera parte de confianza.	x
Disponibilidad	Smart Contracts a través de una plataforma descentralizada	x

Tabla 20. Arquitectura de evaluación para mHealth

Fuente: Elaboración propia

5.1.6 Compartir historias clínicas electrónicas seguras y fiables usando Blockchain

En este documento, se presenta las perspectivas de los autores sobre el manejo de datos de cuidado de la salud basado en blockchain, en particular, para compartir datos EMR entre proveedores de servicios de salud y para estudios de investigación. Se propone un marco para administrar y compartir datos de EMR para la atención del paciente con cáncer.

Se aplica un listado sobre el cumplimiento de los atributos de seguridad

	Blockchain (Hyperledger)		Aplica
Autenticación	Los permisos son aplicados por la lógica del Chaincode		x
Confidencialidad	Los datos clínicos almacenados en el repositorio de la nube se cifran con una clave secreta del paciente, SKAES P		x
Integridad	Las transacciones están firmadas digitalmente		x
Disponibilidad	La disponibilidad de los datos compartidos está garantizada al proporcionar una plataforma en la nube para almacenar los datos		x

Tabla 21. Arquitectura de evaluación para mHealth

Fuente: Elaboración Propia

Como resultado de este análisis, se obtuvo lo siguiente:

Figura 28. Distribución de prioridad según arquitectura de seguridad para los datos clínicos

Fuente: Elaboración Propia

Figura 29. Distribución de prioridad según arquitectura de seguridad para los datos clínicos

Fuente: Elaboración propia

Los pesos adjuntos a los atributos de seguridad se encuentran en relación a la prioridad que debería tener un modelo o arquitectura de seguridad sobre los datos clínicos del paciente; siendo 1 el de menor prioridad y 4 el de mayor prioridad.

En conclusión, sobre este análisis de benchmarking, se obtuvo que la tecnología de Blockchain en cualquier escenario de los mostrados anteriormente, cumplen con los 4 principales atributos de seguridad que se requieren para los datos clínicos del paciente; lo que garantizará una mayor seguridad y confiabilidad para los mismos.

5.2 Modelo Propuesto

Se ha propuesto un modelo de seguridad para los datos clínicos en los dispositivos mHealth basado en la tecnología Blockchain, ver Figura 30. El objetivo de este modelo es mantener la seguridad en el proceso de recopilación y transferencia de datos. Se diseñaron tres fases que componen el modelo propuesto: En primer lugar, la recopilación de datos de los pacientes a través de los dispositivos mHealth. En segundo lugar, el procesamiento de los datos para su privacidad y seguridad en la Red de Blockchain en la nube y, en tercer lugar, el monitoreo del sistema y evaluación del rendimiento.

5.2.1 Recopilación de datos

Los datos del paciente son recopilados a través de los dispositivos mHealth mediante el uso de wearables, ingreso de datos en un teléfono móvil, PDA, etc. El paciente comparte su información otorgando accesos al personal médico y a sus familiares

5.2.2 Procesamiento de datos

La información fluye a través de conexiones seguras a la red de Blockchain en la nube replicándose la información entre todos los nodos participantes previamente habiéndose ejecutado algoritmos de consenso.

5.2.3 Monitoreo del sistema

En esta fase, se evalúa el rendimiento del sistema y la generación de nuevos bloques en la red. Esto permitirá evaluar la escalabilidad del sistema.

Figura 30. Modelo de Seguridad de los datos clínicos para los dispositivos mHealth basado en Blockchain

Fuente: Elaboración Propia

El modelo propuesto, toma en consideración los principales requisitos de seguridad de datos en los dispositivos mHealth como la Disponibilidad, que significa la accesibilidad a la información por parte de una parte autorizada en cualquier momento y lugar; la Integridad, para garantizar que los datos almacenados no hayan sido modificados por terceros no autorizados y verificar que la información haya sido enviada por una entidad confiable; Autenticidad, para verificar la identidad de los actores de la red, y Confidencialidad donde cada participante solo puede tener acceso a la información según su rol en la organización y acceso autorizado

Por otro lado, para brindar mayor soporte al diseño de nuestro modelo, en la Figura 31 se propuso una arquitectura que conecta diversos componentes del sistema de salud con la tecnología Blockchain.

Figura 31. Arquitectura de mHealth en Blockchain

Fuente: Elaboración propia

5.3 Implementación

Para darle un mayor soporte al modelo propuesto, se ha realizado una prueba de concepto mediante la implementación de una red de Blockchain utilizando el Hyperledger Composer brindada por Linux; en el cual se realizaron las configuraciones para levantar la red propuesta; además, se realizaron dos aplicaciones simulando el sistema de una entidad sanitaria; 1) Para el administrador, 2) Para los usuarios frecuentes (Doctor, Familiar y Paciente). Esta prueba de concepto se basó en dos escenarios que pudieron demostrar 3 atributos de seguridad principales de los 4 que se plantearon en nuestro modelo propuesto. A continuación, se presenta las validaciones realizadas a nivel de Autenticación, Confidencialidad e Integridad y los resultados obtenidos.

5.3.1 Autenticación

Se establecieron dos factores de autenticación para poder acceder a la red: algo que se sabe y algo que se tiene. Para esto, cada usuario (paciente, doctor y familiar) nuevo fue registrado por el

administrador de la red; durante este proceso, se crearon las credenciales (usuario y contraseña) y automáticamente se generó un identificador único denominado certificado digital por cada registro. Este identificador fue compartido con cada usuario y para cada primera interacción con el sistema, la aplicación solicita el identificador, que debe estar alojado en el dispositivo móvil (celular, Tablet o laptop).

Figura 32. Doble autenticación al sistema

5.3.2 Confidencialidad

Para este atributo, se plantearon los mismos escenarios comentados anteriormente, pero su validación consistía en otras actividades.

Escenario I: Para este escenario, se estableció la conexión de 4 dispositivos (2 Laptops, 2 Celulares). Asimismo, se definieron 2 doctores (laptops), un paciente y un familiar.

- Primero, el paciente realizó un total de 15 registros de sus datos (frecuencia cardíaca, presión arterial y glucosa) y cada uno de estos se envió al Doctor 1; para este primer caso, se intentó acceder a la información desde el familiar registrado en la red y el Doctor 2 dando como resultado la restricción el acceso a la red, para este mismo caso, se ingresó con el Doctor 1 pudiendo visualizar toda la información compartida por el Paciente.

- Segundo, el mismo paciente le otorga permisos al Familiar, este ingresa a la red y ahora si puede visualizar toda la información.
- Tercero, el paciente realiza un total de 10 registros y esta vez las envía al Doctor 2 pero le quita los permisos al Doctor 1 para visualizar su información; en este caso se ingresó con el Doctor 2 y el familiar y si pudieron ver toda la información registrada en la red; el Doctor 1 intentó visualizar la información del paciente y no tuvo éxito.
- Cuarto, el paciente realizó 10 registros adicionales para el Doctor 2 pero esta vez se le brindó permisos también al Doctor1; para este caso, el primer Doctor ingresó y pudo visualizar la información del paciente.

Escenario II: Para este escenario, se planteó la utilización de 7 dispositivos (3 Laptops, 3 celulares y una Tablet). Asimismo, se definieron 2 doctores (laptops), 3 pacientes (celulares), 2 familiares (Tablet y laptop).

- Primero, el Paciente 1 ingresó 10 registros y se le envió al Doctor 1; para este caso, se ingresó con el Doctor 2 y el Familiar 2 dando como resultado el NO acceso a esta información registrada., para este mismo caso, se ingresó con el Doctor 1 pudiendo visualizar la información registrada.
- Segundo, el Paciente 2 ingresó 12 registros que los envió al Doctor 2; para este caso, se ingresó con el Doctor 1, el Familiar 1 y el Familiar 2 pero no se tuvo éxito para visualizar la información registrada por el segundo paciente, para este mismo caso, se ingresó con el Doctor 1 y este sí pudo visualizar la información que le fue enviada.
- Tercero, el Paciente 2 le otorga permisos al Familiar 2; para este caso, se ingresó con el segundo familiar y este ya pudo visualizar la información compartida por el segundo paciente.
- Cuarto, el Paciente 3 ingresa 10 registros y se los envía al Doctor 1; para este caso, se ingresó con el Doctor 2 y el Familiar 1 y ambos no pudieron visualizar la información.
- Quinto, el Doctor 1 realizó 2 diagnósticos del Paciente 3; para este caso, se ingresó con el Doctor 2 y el Familiar 2 y ambos no visualizaron los registros ni los diagnósticos.
- Sexto, el Paciente 1 ingresó 5 registros adicionales a los que tenía, pero en esta ocasión se los envió al Doctor 2 y le dio permisos al Familiar 1; pero, le quitó el permiso al Doctor1; para

este caso, se ingresó con el primer doctor y ya no pudo visualizar ninguna información, se ingresó con el Doctor 2 y el Familiar 1 y ambos pudieron visualizar toda la información.

- Séptimo, el Paciente 3 ingresa 7 registros y se los envía al Doctor 2 pero no le quita el permiso al Doctor 1; para este caso, se ingresó con el primer y segundo doctor y ambos doctores pudieron visualizar toda la información incluyendo los diagnósticos que fueron elaborados por el Doctor 1.
- Octavo, el Doctor 2 emite 4 diagnósticos del Paciente 3 y 3 diagnósticos del Paciente 2; para este caso, se ingresó con el Doctor 1 y este pudo visualizar los diagnósticos elaborados por el segundo doctor del Paciente 3, pero no pudo visualizar ninguna información del Paciente 2; se ingresó con el Familiar 2 y este sí pudo visualizar estos diagnósticos elaborados para el segundo paciente.
- Noveno, el Paciente 2 le quita accesos al Familiar 2 y se le brinda permisos al Familiar 1; para este caso, se vuelve a ingresar con el segundo familiar, pero ya no pudo visualizar ninguna información; pero se ingresó con el primer familiar, y este sí pudo visualizar toda la información del segundo paciente.

5.3.3 Integridad

Para esta validación, se utilizó Hyperledger Explorer, una interfaz web que permitió visualizar las transacciones, bloques, nodos e interacciones que se desarrollaron dentro de la red de Blockchain. Conforme se registraba un usuario, ingresaban registros médicos, se otorgaban o denegaban permisos, esta interfaz mostraba el registro de una nueva transacción en la red. Integramos Hyperledger Explorer con la aplicación para verificar que cada transacción registrada en la red contenía un hash único que proporciona automáticamente la tecnología Blockchain.

CAPÍTULO 6: RESULTADOS DEL PROYECTO

En este capítulo se presenta los resultados del proyecto respecto a las pruebas realizadas para cada atributo de seguridad durante su validación. Además, se muestra la planificación de costos y el plan de continuidad a considerar para este proyecto.

6.1 Autenticación

Para la validación de este atributo de seguridad, se realizó en dos fases, en el primero se estableció una conexión de 4 dispositivos y en el segundo 7. En ambos casos, el administrador de la red registró a los usuarios ingresando su DNI, nombre, correo y clave; en el cuál, por cada registro nuevo, se generó automáticamente un identificador único; posterior a ello, se compartió este identificador con cada participante de la red; finalmente, para poder acceder a la red, el usuario ingresaba con su cuenta GitHub, posteriormente tenía que importar la tarjeta (identificador único) que estaba alojado en su dispositivo; luego de ello, tenía que ingresar sus credenciales con las que se registró en la red. Para este caso, se intentó ingresar solo con las credenciales lo cual no fue posible, ya que el identificador tenía que estar alojado en el dispositivo; así como también, se ingresaron las credenciales incorrectas con el identificador alojado en el dispositivo, dando como resultado la restricción del acceso a la red. En las dos fases que se realizaron estas pruebas, era necesario que todos los dispositivos cuenten tanto con el identificador alojado en su dispositivo como el ingreso de sus credenciales correctas.

De acuerdo con los datos obtenidos, se determina la importancia de tener un manejo adecuado de la información mediante el uso de tecnologías que aportan a la seguridad de datos en beneficio de los pacientes y de la entidad sanitaria. Los dos factores de autenticación implementados permitieron demostrar que el 100% de usuarios registrados en la red, debieron ingresar sus credenciales correctamente y tener el identificador único alojado en el dispositivo para poder acceder a la red. Por otro lado, debido a la lógica de control de acceso a los datos (.ACL) que contiene la tecnología Blockchain, se demostró una gestión de permisos robusta al permitir a los doctores y familiares acceder a la información autorizada.

En la Figura 33 se muestra que los usuarios requieren de un identificador que debe estar alojado en el dispositivo móvil.

Figura 33. Solicitud del segundo factor de autenticación

6.2 Integridad de los datos

La integración de la herramienta Hyperledger Explorer con la aplicación, demostró la integridad de los datos alojados en la red debido a que cada transacción registrada, contenía un hash criptográfico generado por el algoritmo SHA-256 usado por la tecnología Blockchain.

En la Figura 34, se muestra la interfaz de la herramienta Hyperledger Explorer donde se evidencian los bloques generados durante la validación del proyecto, estos bloques se van añadiendo a la red a medida que se generan transacciones por parte de los actores del sistema.

Figura 34. Generación de bloques en la red Blockchain

En la Figura 35 se muestra el detalle del último bloque generado en la red de Blockchain, por lo que se evidencia la encriptación de los datos del bloque mostrado.

Figura 35. Detalle de un bloque de la red de Blockchain

6.3 Rendimiento del sistema

Otro factor importante, fue la evaluación del rendimiento del sistema relacionado a la escalabilidad y eficiencia en el procesamiento de datos. En la Figura 36, se muestran los resultados de la validación ante una alta carga de peticiones al sistema por parte de los usuarios. Se simuló un rango de 10 a 10,000 solicitudes. El sistema mostró un tiempo promedio de respuesta de 4.27 segundos con solicitudes de 10,000 usuarios al mismo tiempo.

En la ecuación (1) se muestra el cálculo del tiempo promedio de respuesta del sistema, siendo t el tiempo de respuesta por cada petición y, n el número de peticiones totales.

$$\bar{X} = \frac{\sum t}{n} \quad (1)$$

Figura 36. Tiempo promedio de respuesta de red de Blockchain

Por último, en relación con el punto anterior, se evaluó el rendimiento de las principales funciones del sistema: Autenticación del usuario, registro de datos, asignación de permisos y denegación de permisos. En la Figura 37 se indican los tiempos de respuesta promedio por cada funcionalidad del sistema, y se puede observar que la asignación y denegación de permisos presentan un alto rendimiento basado en el tiempo de respuesta al usuario. Los tiempos promedios de respuesta para la asignación y denegación de permisos para 10,000 usuarios simultáneos es de 4,13 segundos y 2,35 segundos respectivamente. De esta manera, se demostró que los usuarios pueden gestionar los accesos a sus datos de manera eficiente.

Figura 37. Tiempo promedio de respuesta basado en las funciones principales

6.4 Plan de Costos

Para obtener el costo del proyecto propuesto, se realizó la cotización de acuerdo con los requerimientos que se obtuvieron. A continuación, se presenta la estimación realizada:

						Tipo Cambio	3,33
COSTOS INTERNOS							
		Cantidad	Precio Unitario	Moneda	Periodo	Precio Total (S/.)	Costo Total
1. Implementación de la Herramienta							
Adquisición de la Infraestructura							
	Teléfono móvil	2	1200	Soles	1	S/ 2.400,00	S/ 2.400,00
	Laptop	3	2500	Soles	1	S/ 7.500,00	S/ 7.500,00
	Tablet	1	800	Soles	1	S/ 800,00	S/ 800,00
	Subtotal Infraestructura	-				S/ 10.700,00	S/ 10.700,00
2. Costos de Personal							
	Jefe de Proyecto	1	8000	Soles	4	S/ 32.000,00	S/ 32.000,00
	Analista de Sistemas	2	5000	Soles	4	S/ 40.000,00	S/ 40.000,00
	Desarrollador Back End	1	3500	Soles	2,5	S/ 8.750,00	S/ 8.750,00
	Desarrollador Front End	1	3000	Soles	1,5	S/ 4.500,00	S/ 4.500,00
	Analista QA	1	4000	Soles	0,5	S/ 2.000,00	S/ 2.000,00
	Tester	1	3000	Soles	1	S/ 3.000,00	S/ 3.000,00
	Subtotal Costos de Personal					S/ 90.250,00	S/ 90.250,00
TOTAL							S/ 100.950,00

Figura 38. Costos del proyecto

6.5 Plan de Continuidad

6.5.1 Post Implementación

Después de realizar las validaciones del modelo propuesto a través de una aplicación móvil en una red de Blockchain, es necesario analizar propuestas con respecto al alcance de los datos para que éste pueda ser compartido a diferentes entidades sanitarias a través del tiempo. Ello permitirá la interoperabilidad entre clínicas, hospitales y otros proveedores de servicios sanitarios. Las diferencias tecnológicas entre las compañías de salud complican la compartición de datos médicos entre organizaciones, por lo que con Blockchain esto puede ser solucionado al permitir a las partes autorizadas el acceso a una base de datos unificada que almacene toda la información clínica de los pacientes.

6.5.2 Adaptabilidad del modelo

El modelo propuesto se puede adaptar a la conexión entre diversas clínicas y/o hospitales. La interoperabilidad simplificaría el tiempo que llevan los procesos hospitalarios con respecto a la

solicitud de información médica o a los traslados entre entidades sanitarias. Uno de los principales problemas de seguridad de la interoperabilidad reside en vincular los registros de salud y las transacciones de los pacientes con los diversos proveedores de servicios de atención médica. Al tener un único repositorio de información en lo que los actores autorizados puedan acceder y compartir información médica, con autorización del paciente, sin intermediarios.

Figura 39. Propuesta del plan de continuidad del proyecto

CAPÍTULO 7: GESTIÓN DEL PROYECTO

En esta sección, se explican las acciones realizadas para la Gestión de todo el proyecto en curso y la documentación correspondiente que acompaña a cada fase.

7.1 Plan de Gestión de Alcance

Este proyecto se realizó durante los ciclos académicos 2018-1 y 2018-2, el alcance del mismo consideró los siguientes:

1. Documentación para la gestión del proyecto (PMBOK).
2. Reuniones con el cliente para las revisiones de los entregables, así como de la aprobación de estos y del diseño del modelo.
3. Análisis de la cadena del servicio de atención M-HEALTH.
  - a. Descripción de las actividades que se realizan en la clínica para gestionar los riesgos que abarcan los dispositivos M-Health.
  - b. Lista de activos de la clínica.
  - c. Lista de las vulnerabilidades.
  - d. Lista de escenarios de incidentes.
  - e. Lista de riesgos.
  - f. Establecer una estrategia de mitigación.
  - g. Plan de mitigación de riesgos.
  - h. Lista de controles.
  - i. Lista de acciones.
4. Modelo de Seguridad y Protección de datos clínicos.
5. Documentación de M-HEALTH.
6. Hoja de RUTA
7. Perfil del proyecto
8. Plan de Continuidad
9. Lecciones aprendidas
10. Paper

11. Memoria

12. Poster

Restricciones

- El Framework TOGAF es gratuito, no habrá inversión alguna.
- El tiempo de realización del proyecto no puede ser mayor a 1 año.
- Las reuniones se darán de acuerdo a la disponibilidad del profesor cliente y a la de los jefes de proyecto.

Suposiciones

- La clínica nos brindará información tanto para realizar el análisis y la implementación del proyecto.
- El equipo del proyecto se reunirá una vez por semana con el cliente, mostrándole los avances.
- Se contará con la participación del gerente de manera que apoya al proyecto en su totalidad.

7.2 Plan de Gestión de la Calidad

A continuación, se detalla el procedimiento a seguir para el aseguramiento de la calidad del proyecto.

PROCEDIMIENTOS PARA LLEVAR A CABO LA PLANIFICACIÓN, ASEGURAMIENTO Y CONTROL DE LA CALIDAD

Procedimientos para la Planificación de la Calidad

- ✓ Tormenta de ideas
  - ✓ Mapas de procesos
  - ✓ Plan de gestión de calidad
  - ✓ Planificar el proyecto con el profesor cliente
  - ✓ Benchmarking de modelos de seguridad
-

Procedimientos para Aseguramiento de la Calidad

- ✓ Revisión de calidad
- ✓ Versionado y mejora de los documentos

Procedimientos para el Control de la Calidad

- ✓ Diagramas de Flujo
- ✓ Estados de procesos
- ✓ Inspección del versionado y mejoras de los documentos

Procedimiento para mejora continua

- ✓ Gestión de requerimientos
-

7.3 Plan de Gestión de Comunicaciones

En esta sección, se detallan los canales de comunicación entre los involucrados del proyecto.

Información requerida	Contenido	Responsable de elaborarlo	Para su entrega a los Stakeholders	Método de comunicación a utilizar	Frecuencia
Iniciación del proyecto	Información de iniciación de proyecto – Project Charter.	Jefes de Proyecto	- Comité de proyectos - Gerente General - Profesor Cliente - Profesor Gerente	- Envío de documentos Word vía correo electrónico. - Presentación física de Project Charter. - Reuniones presenciales. - Exposición.	Una sola vez
Planificación del proyecto	Cronograma del Proyecto, Diccionario EDT, Matriz de Riesgos, Matriz de Trazabilidad, Matriz RAM,	Jefes de Proyecto	- Comité de proyectos	- Envío de documentos Word vía	Una sola vez

	Plan de Gestión de Calidad, Plan de Gestión de Comunicaciones, Plan de Gestión de Riesgos, Plan de Gestión de RRHH, Plan de Gestión del Cronograma, Plan de Gestión de Alcance, Registro de Interesados, Plan de Gestión del Alcance, Plan de Gestión del Cronograma, Benchmarking de las metodologías de análisis y gestión de riesgos y normas de seguridad informática.		- Gerente General - Profesor Cliente - Profesor Gerente	correo electrónico. - Reuniones presenciales y digitales. - Exposición.	
Ejecución del proyecto	Descripción de actividades realizadas por la empresa para gestionar los riesgos de seguridad de información, Lista de los activos, Lista de vulnerabilidades, Lista de escenarios de incidentes con sus respectivas	Jefes de Proyecto	- Comité de proyectos - Gerente General - Profesor Cliente	- Envío de documentos Word vía correo electrónico.	Semanal

	consecuencias, Lista de riesgos con prioridad., Lista de riesgos aceptados con su respectiva justificación, Plan de mitigación de riesgos, Lista de controles, Lista de acciones, Hoja de Ruta, Perfil de proyecto, Plan de Continuidad, Memoria, Lecciones aprendidas, Paper y poster.		- Profesor Gerente - Cliente	- Reuniones presenciales y digitales. - Exposición.	
Cierre de proyecto	Acta de Aceptación y Cierre.	Jefes de Proyecto	- Comité de proyectos - Gerente General - Profesor Cliente - Profesor Gerente	- Envío de documentos Word vía correo electrónico. - Reuniones presenciales y digitales. - Exposición.	Una sola vez

Tabla 22. Plan de Gestión de Comunicaciones

Fuente: Elaboración propia

7.4 Plan de Gestión de Riesgos

En el siguiente cuadro se incluyen los riesgos que pueden afectar al desarrollo del proyecto, su probabilidad, su impacto y su estrategia de mitigación.

N°	Riesgo	Probabilidad	Impacto	Estrategia de mitigación
1	Falta de contenido específico de información que nos sirva para los entregables del proyecto.	Bajo	Alto	Consultar antecedentes, trabajos realizados.
2	Mal alineamiento entre el asesor / cliente y el portfolio manager	Bajo	Alto	Mantener una comunicación constante y comunicar los cambios a tiempo cualquier cambio realizado en el proyecto.
3	Presentación de los entregables fuera del tiempo establecido	Bajo	Medio	Prolongar el tiempo de investigación al proyecto, tener una buena organización.
4	Recursos de IT Services no entregan las peticiones en el tiempo acordado.	Bajo	Medio	Enviar los documentos a IT Services con antelación para asegurar la pronta entrega de la revisión de los documentos.

5	Retiro de algún miembro del equipo del proyecto	Bajo	Alto	Tomar medidas consultando al profesor cliente y gerente.
6	Desaprobación del proyecto por parte del cliente mostrando disconformidad	Bajo	Alto	Cumplir con las expectativas que nos brinda el cliente en cada reunión semanal de manera que sea testigo de la calidad del producto.
7	Los miembros del equipo del proyecto muestran nerviosismo al momento de sustentar el proyecto	Bajo	Alto	Prepararse constantemente para la exposición y tener estudiada las fuentes que sirvan para sustentar la el proyecto para transmitir seguridad al jurado.
8	Cancelación de las reuniones semanales	Muy Bajo	Muy Alto	El participante que no pueda asistir a las reuniones debe avisar con antelación para reprogramar la reunión.

Tabla 23. Lista de riesgos del proyecto

Fuente: Elaboración propia

7.5 Plan de Gestión de Recursos Humanos

Para el presente proyecto se han definido los siguientes participantes mostrados en el cronograma a continuación.

Asimismo, en la siguiente tabla se detallan los roles y responsabilidades definidos dentro del proyecto.

Rol	Miembro	Responsabilidades
Comité de Proyecto	Rosario Villalta Jimmy Armas Pedro Shiguihara	● Aprobar los proyectos profesionales. ● Monitorear el cumplimiento de los entregables. ● Decidir la continuidad de los proyectos.

Jefe de Proyecto	Cristhian Natividad	● Realizar las funciones necesarias para llevar a cabo el cumplimiento del alcance e implementación del Proyecto.
Jefe de Proyecto	Angel Gutierrez	● Realizar las funciones necesarias para llevar a cabo el cumplimiento del alcance e implementación del Proyecto.
Profesor Gerente de Innova TI	Roy Perez	● Monitorear y controlar las actividades programadas del proyecto.
Profesor Cliente	Milton Chinchay	● Brindar los requerimientos y pautas del proyecto. ● Validar la calidad de los documentos del proyecto.
Recursos de Quality Services	Recursos asignados para los ciclos 2018-01 y 2018-02	● Brindar los servicios de validación y verificación para los documentos del proyecto.

Tabla 24. Plan de Gestión de Recursos Humanos

7.6 Plan de Gestión de Cronograma

Hito del proyecto	Fecha Estimada	Entregables incluidos	Prioridad
Fase de Inicio	Semana 8/ 2018-I	Project Charter	Alta
Fase de Planificación	Semana 16/ 2018-I	Project Charter, Plan de Trabajo, Entregables de Gestión	Alta
Fase de Implementación	Semana 24/ 2018-II	Diseño del modelo	Alto

Fase de Supervisión y Control	Semana 32/ 2018-II	Modelo de Seguridad y Protección de datos, documento que valide el modelo, cronograma actualizado, lista de recursos a solicitar para TP2	Alta
Fase de Cierre	Semana 32/ 2018-II	Evidencias del cumplimiento del objetivo 3	Alta

Tabla 25. Plan de Gestión del Cronograma

LECCIONES APRENDIDAS

A continuación, se mencionan los puntos a mejorar y a considerar en futuros proyectos:

- Al querer realizarse algún cambio en el enfoque y alcance del proyecto, debe realizarse con la aprobación del Gerente y del Asesor/Cliente mediante un acta.
- Establecer un cronograma de reuniones inicial con el Asesor/Cliente a lo largo del proyecto con la finalidad de establecer un mejor orden, y en caso una de las partes no pueda asistir manifestarlo con tiempo.
- Establecer un repositorio único colaborativo para que cada miembro del equipo pueda agregar y modificar información acerca del proyecto.

CONCLUSIONES

- El uso de este tipo de solución en un entorno controlado que simula parte de una entidad de salud permitió garantizar los principales atributos de seguridad respecto a los datos médicos como la autenticación, confidencialidad e integridad de los mismos.
- La evaluación realizada a los tiempos promedios de respuesta para la asignación y denegación de permisos para 10,000 usuarios simultáneos fueron de 4,13 segundos y 2,35 segundos respectivamente. Con ello, se demostró que los usuarios pueden gestionar sus accesos de manera eficiente.
- Los resultados obtenidos determinaron que cuando un nodo se altera, éste se reestablece y se sincroniza con los demás nodos para obtener todas las transacciones de la red. Por lo tanto, implementar la tecnología Blockchain hace que el sistema sea robusto al no tener un punto único de falla.
- Las pruebas de rendimiento realizadas, permitieron demostrar que un sistema mHealth con el uso de la tecnología Blockchain puede ser escalable en el tiempo soportando una alta cantidad de solicitudes por parte de los usuarios. Esto permitió realizar transacciones de manera eficiente para otorgar y denegar permisos al resto de los participantes.

RECOMENDACIONES

- Se recomienda que antes de realizar la implementación del modelo en una clínica, se explique a los encargados qué es lo que se va a realizar y cuáles son los beneficios que conllevaría esta implementación; además, es necesario contar con el respaldo del área de seguridad para que validen esta necesidad debido a que la información es altamente sensible.
- Para implementar soluciones de seguridad sobre un sistema mHealth, se recomienda analizar el flujo de la información para detectar vulnerabilidades en el cuidado de los datos médicos para que la propuesta tecnológica sea más efectiva.
- Se recomienda implementar la tecnología Blockchain en el sistema mHealth con una mayor cantidad de nodos, esto garantizará un nivel de seguridad robusto de los datos médicos que contiene la clínica.
- Incentivar a las entidades sanitarias al uso de la tecnología Blockchain de manera descentralizada, esto permite la interoperabilidad segura entre ellas, además de la interacción mediante una base de datos unificada que almacene la información de los pacientes con los permisos respectivos.

GLOSARIO

- **Data Security:** La seguridad de los datos se refiere a medidas de protección de privacidad digital que se aplican para evitar el acceso no autorizado a computadoras, bases de datos y sitios web.
- **Telemedicina:** Es la prestación de servicios de medicina a distancia, para la que se emplea las tecnologías de información y de comunicaciones.
- **E-Health:** Conjunto de Tecnologías de la Información y la Comunicación (TICs) que, a modo de herramientas, se emplean en el entorno sanitario en materia de prevención, diagnóstico, tratamiento, seguimiento, así como en la gestión de la salud, ahorrando costes al sistema sanitario y mejorando la eficacia de este (laesalud, s.f.)
- **Amenaza:** Surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información (Universidad Nacional de Luján, s.f.)
- **Riesgo:** Es la probabilidad que una amenaza aproveche una vulnerabilidad generando un impacto.
- **Vulnerabilidad:** Son las brechas o fallas que presenta un sistema, si no se corrige puede ser aprovechada por una amenaza.
- **Seguridad de la información:** Conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

- **Evaluación de riesgo:** Procedimiento científico que estima la probabilidad de que se materialice un riesgo.
- **Activos:** Es un objeto tangible o intangible con la cual permite la operatividad de diversas actividades.
- **M-health:** Es la práctica de la medicina y la salud pública soportada por dispositivos móviles como teléfonos móviles.
- **Blockchain:** Cadena de bloques.

BIBLIOGRAFÍA

- Al-Haj, A., & Abdel-Nabi, H. (2017). Efficient joint encryption and data hiding algorithm for medical images security. *IEEE*.
- Alibasa, M., Santos, M., Glozier, N., Harvey, S., & Calvo, R. (2017). Designing a Secure Architecture for m-Health Applications. *IEEE*, 91-94.
- Atat, R., Liu, L., Ashdown, J., Medley, M., Matyjas, J., & Yi, Y. (2017). A Physical Layer Security Scheme for Mobile Health Cyber-Physical Systems. *IEEE Internet of things Journal*, 1-15.
- Cifuentes, Y., Beltrán, L., & Ramírez, L. (2015). Analysis of Security Vulnerabilities for Mobile Health Applications. *World Academy of Science, Engineering and Technology International Journal of Health and Medical Engineering*, 1067-1062.
- Cusack, J. (1 de Agosto de 2017). *Standard Chartered*. Obtenido de Blockchain: a game-changer in the fight against financial crime?: <https://www.sc.com/en/explore-our-world/blockchain/>
- Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and Trustable Electronic Medical Records Sharing using Blockchain. 1-10.
- Esposito, C., De Santis, A., G., T., Chang, H., & Choo, K. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Computing*, 31-37.
- Evans, D. (2011). *Internet de las cosas: Cómo la próxima evolución*. Cisco Internet Business Solutions Group.
- Huang, K. (1 de Noviembre de 2015). *SlideShare*. Obtenido de <https://www.slideshare.net/KevinHuang23/wearables-devices-market-and-technology>
- Ichikawa, D., Kashiyama, M., & Ueno, T. (2017). Tamper-Resistant Mobile Health Using Blockchain Technology. *JMIR MHEALTH AND UHEALTH*, 1-10.
- Jaidi, F., Labbene-Ayachi, F., & Bouhoula, A. (2016). Advanced Techniques for Deploying Reliable and Efficient Access Control: Application to E-healthcare. *CrossMark*, 1-9.
- Kitchenham. (2007). Guidelines for performing systematic literature reviews in software engineering. *EBSE Technical Report*, 1-57.
- laesalud. (s.f.). *laesalud*. Obtenido de La eSalud, referencia en eHealth en español: <https://laesalud.com/que-es-esalud/>
- Linn, L., & Koo, M. (s.f.). Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research. 1-10.
- Liu, W., Zhu, S., Mundie, T., & Krieger, U. (2017). Advanced Block-Chain Architecture for e-Health Systems. *The 2nd IEEE International Workshop on Emerging Technologies for Pervasive Healthcare and Applications*, 32-43.

- Pagnotta, S. (31 de Julio de 2014). *Welivesecurity*. Obtenido de Internet de las Cosas: 70% de dispositivos son vulnerables: <https://www.welivesecurity.com/la-es/2014/07/31/internet-de-las-cosas-dispositivos-vulnerables/>
- Universidad Nacional de Luján. (s.f.). *Universidad Nacional de Luján*. Obtenido de Amenazas a la Seguridad de Información.
- Yang, Y., Liu, X., Deng, R., & Li, Y. (2017). Lightweight Sharable and Traceable Secure Mobile Health System. *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING*, 1-14.

ANEXO A - WASC

ENSAYO para alinear el trabajo final con la competencia de Pensamiento

Crítico

En el presente ensayo, se explicará cómo el pensamiento crítico forma parte del proyecto de un Modelo de Seguridad de los datos Clínicos para los dispositivos mHealth basados en Blockchain, Asimismo, se explicará las diferentes actividades que se realizaron en el proyecto partiendo de un problema identificado, teniendo como conclusión una propuesta de solución que se validará y evaluará la efectividad del mismo. El presente proyecto ha sido efecto de varias etapas que se han ido realizando cumpliendo con los estándares de calidad requeridos. En las primeras etapas, se realizó un análisis de diversas fuentes y enfoques sobre la naturaleza del sistema mHealth tomando como variables el nivel de seguridad, los dispositivos involucrados, tecnologías implementadas, entre otros. La variable que toma más relevancia para el proyecto, es la seguridad, tomando como referencia los datos clínicos de los pacientes que son confidenciales por naturaleza; esto debido a que el sector salud en el año 2017 ha experimentado un crecimiento de 210% en ciberataques comparándolos con un año anterior a este según el McAfee Labs Threats; además, el mismo laboratorio indica que el sector salud está ubicado entre los principales objetivos de los cibercriminales debido a un alto valor que actualmente tienen los datos clínicos de los pacientes. Luego, se realizó un análisis, mediante el descarte de artículos, revistas, documentos sobre soluciones actuales para el sistema mHealth. Entre las variables que influyeron en la selección de soluciones, se encuentran: antigüedad de la propuesta, activos involucrados, tipo de solución. Asimismo, se definieron criterios de evaluación para comparar las soluciones previamente indicadas como resultado de un análisis de la seguridad del sistema mHealth detallados en varios artículos científicos, considerando los principales atributos la Confidencialidad, Disponibilidad, Autenticación e Integridad. El proceso anterior tuvo como resultado el nivel de seguridad que aportan las soluciones actuales para la protección de los datos clínicos de los pacientes. En el resultado indica que la tecnología Blockchain involucra todos los criterios de seguridad previamente definidos garantizando un alto nivel en la protección de los datos clínicos, así como también permitir la integridad, privacidad y auditabilidad de los mismos. Por ello se ha llegado a la conclusión que para abordar seguridad de los datos clínicos de los pacientes la tecnología

Blockchain enfocado a un modelo de seguridad garantiza la confidencialidad e inmutabilidad de los datos clínicos de los pacientes, lo cual, generaría una mayor seguridad en los pacientes al momento de acudir a un establecimiento médico ya sea público o privado que cuente con esta tecnología; además la entidad tendría una mayor reputación debido a que no sólo ofrecería una mayor y mejor calidad de servicio, sino también la seguridad de que los datos sensibles que se manejan en dicha entidad serán sumamente confidenciales y que sólo los autorizados podrán acceder a ellos.

ANEXO C – Costos y Presupuestos

							Tipo de Cambio	3,33
COSTOS INTERNOS								
	Cantidad	Precio Unitario	Moneda	Horas	Precio Total (S/.)	Periodos	Costo Total	
1. Implementación de la Herramienta								
Adquisición de la Infraestructura								
	Teléfono móvil	2	1200	Soles	1	S/ 2.400,00	1	S/ 2.400,00
	Laptop	3	2500	Soles	1	S/ 7.500,00	1	S/ 7.500,00
	Tablet	1	800	Soles	1	S/ 800,00	1	S/ 800,00
	Subtotal Infraestructura				-	S/ 10.700,00		S/ 10.700,00
Plataforma Cloud								
	Licenciamiento del Cluster para alojar la aplicación a la nube (IaaS)	1	748,48	Dólares	-	S/ 2.492,44	2	S/ 4.984,88
	Subtotal Plataforma Cloud					S/ 2.492,44		S/ 4.984,88
2. Costos de Personal								
	Tester	1	18,75	Soles	8	S/ 150,00	1	S/ 150,00
	Desarrollador	1	8,75	Soles	40	S/ 350,00	2	S/ 700,00
	Jefe de Proyecto	1	60,1	Soles	16	S/ 961,60	10	S/ 9.616,00
	Analista Investigador	2	20,5	Soles	48	S/ 1.968,00	10	S/ 19.680,00
	Analista de Sistemas	2	20,5	Soles	48	S/ 1.968,00	10	S/ 19.680,00
	Documentador	1	12,5	Soles	32	S/ 400,00	10	S/ 4.000,00
	Diseñador	1	8,5	Soles	16	S/ 136,00	10	S/ 1.360,00
Subtotal Costos de Personal					S/ 500,00		S/ 55.186,00	
TOTAL								S/ 70.870,88

Fuente: Elaboración propia