

Universidad de Lima
Facultad de Ingeniería y Arquitectura
Carrera de Ingeniería de Sistemas



TRANSFORMACIÓN DIGITAL DE HISTORIAS CLINICAS EN EL SECTOR SALUD PRIVADO PARA LOS TIPOS DE ATENCIÓN MÉDICA HOSPITALARIA Y EMERGENCIA

Trabajo de suficiencia profesional para optar el Título Profesional de Ingeniero de
Sistemas

Michael Lexter Olaya Espinoza

Código 20011289

Asesor

Manuela Linares Barbero

Lima – Perú

Mayo de 2020

**DIGITAL TRANSFORMATION OF MEDICAL
HISTORIES IN THE PRIVATE HEALTH
SECTOR FOR THE TYPES OF HOSPITAL
HEALTH CARE AND EMERGENCY**

TABLA DE CONTENIDO

RESUMEN	VIII
ABSTRACT	IX
CAPÍTULO I: INTRODUCCIÓN	1
CAPÍTULO II: CONCEPTOS Y FUNDAMENTOS	4
CAPÍTULO III: FUNDAMENTACIÓN DEL PROYECTO	20
3.1 Fundamentación de la deseabilidad del proyecto	20
3.2 Fundamentación de la factibilidad del proyecto	23
3.3 Fundamentación de la viabilidad técnica	26
CAPÍTULO IV: DEFINICIÓN DEL PROYECTO	35
4.1 Objetivo general.....	38
4.2 Objetivos específicos.....	38
4.3 Diseño propuesta de valor	38
4.4 Modelo de negocio propuesto.....	40
CAPÍTULO V: DESARROLLO DEL PROTOTIPO	42
CONCLUSIONES	64
RECOMENDACIONES	67
GLOSARIO DE TÉRMINOS	68
REFERENCIAS	70
BIBLIOGRAFÍA	75
ANEXOS	79

INDICE DE TABLAS

Tabla 2.1 Diferencias entre Blockchain Pública y Privada	7
Tabla 3.1 Costos mensuales del equipo de trabajo para implementar el proyecto	27
Tabla 3.2 Precios de Cloud Computing para infraestructura Blockchain	27
Tabla 3.3 Pago de servicios básicos (Gastos Generales por mes con T.C. 3.4 soles) ...	27
Tabla 3.4 Muebles en General	28
Tabla 3.5 Gastos Varios.....	28
Tabla 3.6 Cálculo de costo total de la propuesta.....	28
Tabla 3.7 Cálculo de usuarios por año	29
Tabla 3.8 Proyección transacciones realizadas por año	29
Tabla 3.9 Proyección de ventas.....	30
Tabla 3.10 Proyección costo de mantenimiento de servicio anual	30
Tabla 3.11 Gastos de Operación	31
Tabla 3.12 Flujo de caja Económico	31
Tabla 3.13 Flujo de caja Financiero	32
Tabla 3.14 Indicadores Económicos	32
Tabla 5.1 Requerimientos No Funcionales.....	45
Tabla 5.2 Aspectos para cubrir la seguridad de información	55
Tabla 5.3 Componentes de la Arquitectura	59

INDICE DE FIGURAS

Figura 3.1 Flujo actual de solicitud de historia Clínica – Sector Privado	34
Figura 4.1 Modelo de Negocio	41
Figura 5.1 Características de lo que debe, debería y podría tener nuestro PVM.....	44
Figura 5.2 Participante - Instituciones.....	46
Figura 5.3 Participante - Paciente	46
Figura 5.4 Crear Institución.....	47
Figura 5.5 Institución.....	47
Figura 5.6 Paciente.....	48
Figura 5.7 Activo - Historia Clínica.....	48
Figura 5.8 Crear Historia Clínica.....	49
Figura 5.9 Historia Clínica.....	49
Figura 5.10 Estado Inicial de Paciente	50
Figura 5.11 Invoca transacción Autorizar	50
Figura 5.12 Confirmación de transacción.....	51
Figura 5.13 Paciente autoriza clínica	51
Figura 5.14 Clínica visualiza información del paciente	52
Figura 5.15 Paciente revoca acceso.....	52
Figura 5.16 Confirmación de transacción de revocatoria.....	53
Figura 5.17 Visualización del campo autorizado del paciente	53
Figura 5.18 Clínica ya no visualiza información del paciente.....	54
Figura 5.19 Seguridad Blockchain posibles casos	56
Figura 5.20 Diagrama de Arquitectura.....	58
Figura 5.21 Flujo de control de acceso en Blockchain.....	60
Figura 5.22 Infraestructura de Hyperledger Composer Fabric	62

INDICE DE ANEXOS

Anexo 1: Mapa de Empatía Doctores - Impresión de sistemas de información hospitalario.....	80
Anexo 2: Mapa de Empatía-Paciente y su impresión de sistemas hospitalarios	81
Anexo 3: Identificando usuarios extremos	82
Anexo 4: Diagrama Persona - Segmento Paciente.....	83
Anexo 5: Canvas Lienzo Propuesta de Valor	84
Anexo 6: Matriz de problemas - Resultado de las entrevistas para identificar problemas relevantes para el usuario.....	85
Anexo 7: Matriz de problemas - Determinar si el problema que seleccionamos es relevante para los segmentos de personas seleccionados	86
Anexo 8: Storyboard	87
Anexo 9: Resolución Ministerial N°120-2017/MINSA	91
Anexo 10: Ley N° 30024.....	93
Anexo 11: Ley N° 26842 - Ley General de Salud	119
Anexo 12: Decreto de Urgencia_Sistema Nacional de Transformación Digital	137
Anexo 13: Propuesta de pantallas PMV	143
Anexo 14: Ficha Técnica de Entrevista Abierta	145
Anexo 15: Guía de entrevista – Paciente y Médico	147
Anexo 16: Estado de Ganancias y Pérdidas	149
Anexo 17: Determinación del WACC.....	150
Anexo 18: Periodo de recuperación de la Inversión – Económico	151
Anexo 19: Periodo de recuperación de la Inversión – Financiero	152
Anexo 20: Componentes de la plataforma Blockchain de IBM	153
Anexo 21: Arquitectura de Hyperledger Fabric.....	154
Anexo 22: Codificación.....	155

RESUMEN

Actualmente cuando un paciente es derivado a otro centro de salud los familiares deben realizar trámites administrativos para obtener la historia clínica y llevarla al nuevo centro donde se va a atender, esto genera angustia, frustración y pérdida de tiempo tanto para los familiares y sobre todo al paciente.

Por otro lado, cuando los profesionales de la salud se enfrentan a una emergencia, deben actuar de inmediato y muchas veces sin conocer todo el historial del paciente debido a que no cuentan con dicha información.

La oportunidad es proponer una plataforma que permita al profesional de salud tener la información de las historias clínicas en línea y la puedan revisar desde un dispositivo portátil, sin necesidad de sentarse en una computadora de escritorio o laptop para realizar esta actividad. Para los pacientes darles la libertad de poder administrar su información, para que se muestre en las instituciones de salud donde se atiendan.

En este proyecto se va a proponer el uso de blockchain para la gestión de información de las historias clínicas mediante una demo desarrollada con hyperledger composer así como el control de accesos de los doctores a dicha información.

Palabras Clave:

Transformación digital, Blockchain, historia clínica electrónica, administración de control de accesos

ABSTRACT

Currently, when a patient is referred to another health center, family members must carry out administrative procedures to obtain the medical history and take it to the new center where they will be cared for; this generates anguish, frustration and loss of time both for family members and especially for the patient.

On the other hand, when health professionals face an emergency, they must act immediately and often without knowing the patient's entire history because they do not have such information.

The opportunity is to propose a platform that allows health professionals to have information from medical records online and can review it from a portable device, without having to sit at a desktop or laptop computer to carry out this activity. For patients, give them the freedom to manage their information, so that it is displayed in the health institutions where they are attended.

In this project, the use of blockchain for the management of information in medical records will be proposed through a demo developed with hyperledger composer, as well as the control of access by doctors to said information.

Key words:

Digital transformation, Blockchain, Electronic medical record, Access control administration

CAPÍTULO I: INTRODUCCIÓN

En la actualidad el estado peruano está en proceso de digitalizar muchos de sus procesos que aún se hacen de forma tradicional así como la adecuación de políticas y leyes para una correcta administración de la información. El sector salud no es ajeno a este cambio por lo que está adecuando su forma de trabajo e introduciendo el uso de tecnología para agilizar sus procesos y brindar un mejor servicio a sus usuarios, sin embargo, a pesar de las iniciativas, el avance no es muy significativo, pues aún se observa que el manejo de historias clínicas se realiza en papel. Cuando se necesita transferir un paciente a otra institución, se deben realizar trámites administrativos para poder trasladar la historia de institución a institución, generando pérdida de tiempo que muchas veces resulta vital para la atención al paciente que necesita ser atendido con prontitud.

Por otro lado, las instituciones de salud privado han tomado la delantera y ya existen algunas clínicas que cuentan con Sistemas de Información Hospitalaria (HIS por sus siglas en inglés) que les ayuda a almacenar, procesar y reinterpretar datos médicos administrativos lo que les permite generar reportes e informes dependiendo de los fines para los que se requiera. Gracias a estos sistemas las clínicas pueden tener una mejor organización de sus recursos como por ejemplo disposición de camas, agendas de los médicos, sala de operaciones, entre otros, para brindar una atención de calidad a los pacientes. No obstante, a pesar de los grandes pasos que están dando las clínicas aún no se puede contar con una base centralizada de historias que ayuden a pacientes a minimizar todos los trámites administrativos y pérdida de tiempo en el inicio de un tratamiento adecuado y a profesionales de salud para una mejor toma de decisiones en base a su historia en línea.

Bajo este contexto es necesaria una transformación digital que permita tener una plataforma en la cual se pueda empezar almacenando las historias clínicas de los pacientes de clínicas que ya cuentan con un HIS, dado que la transición a esta nueva plataforma sería más rápida, y que ayudará en los tipos de atención medica como hospitalización o emergencias.

El objetivo es que el sistema sea escalable y maneje toda la información relacionada a actividades asistenciales, sin embargo, iniciaremos con historias de pacientes de clínicas puesto que el grado de madurez en el tratamiento de información es más significativo que en el sector público. Por otro lado, al implementar la plataforma con una base reducida se puede mostrar la utilidad de la plataforma lo cual impulsará a que se pueda seguir sumando nuevas instituciones y funcionalidades. Se espera que en un primer momento se pueda consolidar los documentos (escritos) relacionados a la historia y posteriormente ir sumando imágenes y radiografías.

En el capítulo uno se da una introducción al actual contexto del país y los retos que se tiene para seguir con el desarrollo tecnológico del sector. Se exponen generalidades y principales definiciones así como el objetivo del proyecto.

En el capítulo dos se explican los conceptos y fundamentos de la tecnología que se propone para implementar este proyecto. Se da detalles del concepto de Blockchain, la diferencia entre una Blockchain pública y privada, conceptos claves para entender la tecnología así como los protocolos que actualmente existen. También se explican las distintas técnicas para entender las necesidades de los usuarios para ello explicaremos que es design thinking, Lean Startup y Lean Canvas como metodologías que se podrían aplicar durante su implementación.

En el capítulo tres se explica los fundamentos del proyecto en el cual se detalla la deseabilidad mediante la identificación de los problemas que para los usuarios (pacientes y médicos) son relevantes y que permitió llegar a la idea que se desea implementar, la factibilidad técnica y la explicación del modelo de negocio propuesto y viabilidad del proyecto en el cual se explican los costos, flujos de caja y beneficios funcionales.

En el capítulo cuatro se explica la definición del proyecto, la tecnología a utilizar, los integrantes del equipo que llevará a cabo la implementación, aspectos técnicos y económicos, se explica el objetivo general y los objetivos específicos que apoyan y ayudan a alcanzar la meta del proyecto. También se utilizarán herramientas de Lean Canvas para detallar la propuesta de valor y mostrar el Modelo de Negocio propuesto.

En el capítulo cinco, detallaremos como es que vamos a preparar nuestro prototipo, mostrando los requerimientos que cubriremos, pantallas de la interacción con

la demo, explicación del flujo y la codificación. Aquí puede corroborarse lo expuesto en el trabajo y mostrar su aplicabilidad.

Culminamos con las conclusiones y recomendaciones que se derivan de la elaboración del PMV, contrastando nuestra propia experiencia versus la literatura revisada proponiendo algunos temas a considerar cuando se intente implementar este tipo de proyecto y propuestas para futuras investigaciones.



CAPÍTULO II: CONCEPTOS Y FUNDAMENTOS

El cambio de paradigma que se presenta en la actualidad, gracias a la internet en especial después del auge de la Web 2.0 conocida como Web Social o Participativa a mediados de la década del 2000, la aparición de redes sociales nos muestra un ámbito interesante debido a que los consumidores son al mismo tiempo productores (Belatrix, 2019). A esta forma de utilización de internet, el futurólogo estadounidense Alvin Toffler, le acuñó el término de Prosumidor, que es cualquier usuario (consumidor) de internet que puede producir y compartir diferentes tipos de contenido. Según Belatrix (2019) indica lo siguiente:

Nos encontramos en un lugar en el tiempo donde todo tipo de industrias y economías están comenzando a desarrollar estrategias para migrar a esquemas más colaborativos, en los cuales los prosumidores juegan un papel importante, en el cual pueden participar y ofrecer productos o servicios de manera simultánea. Es un punto de partida interesante donde personas como tú y yo podemos formar parte de una red que desafía al establecimiento a través de un nuevo ámbito que promueve la transparencia y la equidad. (p.5)

Y en todo esto ¿cómo es que Blockchain interviene?, pues blockchain proporciona la tecnología. De acuerdo con Arroyo Guardado, Díaz Vico y Hernandez Encinas, (2019) indican: “Esta tecnología se está convirtiendo en una de las grandes protagonistas de la segunda década del siglo XXI, de forma que se le suele considerar como el gran motor de cambio de la esfera digital” (p.4).

Este protagonismo es debido a que en la actualidad se da mucha importancia a la información y la forma como se gestiona. Blockchain entre los problemas que resuelve esta la confianza. La confianza es un factor fundamental sobre todo en transacciones que realizan las diferentes empresas, lo que nos ofrece esta tecnología es la transparencia de las transacciones y confianza entre las organizaciones, aun si no se conocen entre ellas previamente (Linares Barbero, 2018).

El proyecto se basará en la utilización de la tecnología Blockchain, para ello vamos a describir que es Blockchain, la diferencia entre una Blockchain Pública y Privada, los principales conceptos relacionados a Blockchain y los protocolos.

2.1 ¿Qué es Blockchain?

De acuerdo con la literatura revisada, se puede definir Blockchain como un registro de trazabilidad público digital de transacciones y es incorruptible. Según Makhdoom, Abolhasan, Abbas, y Ni (2019) afirma: “Es la tecnología por debajo del Bitcoin” (p.255).

El funcionamiento en la Blockchain comprende una serie de bloques de tal manera que cada nuevo bloque se conecta criptográficamente al anterior. Gracias a sus beneficios inherentes como la inmutabilidad, capacidad de auditoría, integridad y autenticación de transacciones, la tolerancia a fallos y sobre todo el funcionamiento sin confianza, Blockchain está siendo concebido para jugar un papel vital en el ecosistema de seguridad de IoT. (Dinh, Liu, Zhang, Chen, Ooi y Wang, 2018).

2.1.1 Blockchain Pública

Puede ser un registro de trazabilidad digital sin restricciones que permite la participación libre e incondicional de cualquier nodo (Makhdoom et al., 2019).

La minería en Blockchain públicas se basa principalmente en incentivos, por lo que se alienta a los mineros a explotar un bloque. Por lo tanto, los registros de trazabilidad públicos tienen más costos de transacciones que los privados (Buterin, 2015). Considerando que, la conectividad entre nodos en una Blockchain pública es menor que en una privada, por lo tanto, se necesita más tiempo para finalizar las transacciones (Makhdoom et al., 2019).

Además, para lograr transparencia, todas las transacciones son visibles para el público. Por lo tanto, surgen cuestionamientos relacionadas con el anonimato del usuario y la privacidad de los datos. Por otro lado, las Blockchain públicas tienen un rendimiento de transmisión bajo debido a la baja finalización de transacciones, especialmente en Blockchain basadas en PoW (Lukas, 2018). Ejemplos reales de Blockchains públicas son; Bitcoin (Nakamoto, 2008), Ethereum, IOTA, Litecoin (Litecoin, 2011), entre otros.

2.1.2 Blockchain Privada

Puede ser un registro de trazabilidad digital con restricciones, en el que el número de nodos mineros es limitado y se conocen sus códigos de identificación (ID). Por lo tanto, el procesamiento de transacciones está restringido solo a los nodos validadores o mineros seleccionados o predefinidos. Además, un usuario puede tener acceso solo a los que están directamente relacionados con él (Makhdoom et al., 2019). Por ejemplo, Hyperledger-Fabric permite a las empresas y grupos de la competencia mantener la privacidad y confidencialidad de sus transacciones, utilizando los "canales privados" (*Hyperledger-Fabric Documentation*, 2019). Los canales privados pueden ser denominados rutas de mensajería restringidas que se pueden usar para proporcionar privacidad y confidencialidad de transacciones para subconjuntos específicos de miembros de la red. Todos los datos, incluida la información de transacciones, miembros y canal, son invisibles e inaccesibles para cualquier miembro de la red que no tenga acceso explícito a ese canal. Por lo tanto, en comparación con los registros de trazabilidad públicos, puede haber más privacidad de la información del usuario en este tipo de Blockchain (Makhdoom et al., 2019).

2.1.3 Diferencia entre Blockchain pública y privada

Antes de definir los tipos de Blockchain públicos y privados, es necesario resaltar que un Blockchain puede ser con restricciones (permissioned) o sin restricciones (permissionless) para procesar las transacciones o por ejemplo para crear nuevos bloques de transacciones.

En una Blockchain sin restricciones (Permissionless), cualquier nodo puede crear nuevos bloques de transacciones, mientras que, en una Blockchain con restricciones (Permissioned), el procesamiento de transacciones se realiza solo por los nodos seleccionados. En lo que respecta a la terminología de una Blockchain pública y privada, se relaciona con el acceso a los datos (Makhdoom et al., 2019).

A las diferencias ya descritas, también se puede mencionar que la información está centralizada y que se garantiza el anonimato (Makhdoom et al., 2019). Los costos de transacciones en las Blockchain privadas son bajos debido a que maneja una menor cantidad de nodos (Buterin, 2015). Debido a la necesidad de finalización inmediata de transacciones, las Blockchain privadas tienen un alto rendimiento de transmisión

(Lukas, 2018). Por ende, se puede decir que las Blockchain privadas son más rápidas que las públicas. Sin embargo, las Blockchain privadas con protocolos de consenso BFT sufren de problemas de escalabilidad respecto al número de nodos de validación, además, el registro de transacciones en estos tipos de Blockchain se puede alterar debido a su centralización parcial dado que se tiene un menor número de nodos de minería y son conocidos (Zheng, Xie, Dai, Chen, y Wang, 2017). Las diferencias entre las Blockchain públicas y privadas se muestran en la Tabla 2.1.

Tabla 2.1

Diferencias entre Blockchain Pública y Privada

Blockchain Pública (puede ser sin restricción)	Blockchain Privada (puede ser restringida)
Participación sin restricciones	Participación restringida
Se desconocen los ID's de los nodos (Uso de seudónimos para los ID's)	Se conocen los ID's de los nodos
Número ilimitado de nodos	Número limitado de nodos
Poca privacidad de los datos	Opciones disponibles para seguridad de datos
Pobre consenso de finalización (Buterin, 2016)	Consenso de finalización instantáneo (en Blockchain basado en BFT) (Buterin, 2016)
Bajo rendimiento de transmisión (Lukas , 2018)	Alto rendimiento de transmisión (Lukas , 2018)
Buena escalabilidad (en relación con el número de nodos mineros) (Lukas, 2018)	Mala escalabilidad (En Blockchain basadas en BFT) (Lukas , 2018)
Vulnerable a ataques al 51% de nodos (en el caso de Blockchain PoW y PoS)	Vulnerable a colisión de nodos (En Blockchain basadas en BFT)

Fuente: Makhdoom et al., (2019)

2.1.4 Blockchain con restricciones (Permissioned) y sin restricciones (Permissionless)

Las Blockchain, desde el punto de vista de la forma como se administran, se pueden describir como permissioned (con restricción) y permissionless (sin restricción).

Una Blockchain permissionless Pública permite que cualquiera participe de la red, incluso en el consenso para mantener el ledger con acceso irrestricto de lectura y escritura, por lo tanto, la confianza es mínima entre los participantes, pero aun así logra transparencia. Mientras en una Blockchain permissioned pública, permite leer a cualquier participante, pero para escribir o participar en el consenso, solo está permitido para algunos que tienen permisos y privilegios proporcionado por el administrador de la red.

Por otro lado, una Blockchain permissionless privada permite a las organizaciones colaborar sin necesidad de compartir información públicamente. Al no tener restricción, cualquier participante puede ingresar o salir de la Blockchain. En estas redes los contratos inteligentes (Smart contracts) definen quien puede leer los contratos y los datos relacionados al contrato. Las Blockchain permissioned privada se utilizan en organizaciones donde la información es almacenada con un control de acceso y autorizada por los miembros de la red. El administrador de la red es que permite ingresar o no a un participante y da los accesos de lectura o escritura a los datos (Raikwar, Gligoroski, y Krlevska, 2019)

2.1.5 Conceptos Claves

- *Distributed Ledger (Registro de trazabilidad distribuido)*

Las tecnologías de registro distribuido (Distributed Ledger Technology, en inglés), explicado técnicamente es como una base de datos que es gestionada por varios participantes y no es centralizada, no tiene una autoridad central que sea el árbitro y verificador, asimismo al tener registros distribuidos aumenta la transparencia y dificulta fraudes (Communications, 2018).

Un Ledger (Registro de trazabilidad) es una estructura de datos que contiene una lista ordenada de transacciones. Por ejemplo, un ledger puede registrar transacciones monetarias entre varios bancos o bienes intercambiados entre partes conocidas. En Blockchain, el ledger se replica en todos los nodos. Además, las transacciones se agrupan en bloques que luego se encadenan. Por lo tanto, el ledger distribuido es esencialmente añadir réplicas de estructura de datos. Un Blockchain comienza con algunos estados iniciales, y el ledger registra el historial completo de las operaciones de actualización realizadas a los estados (Dinh et al., 2018).

Blockchain es un tipo de registro distribuido (Distributed Ledger), sin embargo no todos los distributed ledger son una Blockchain. Los registros distribuidos usan computadoras independientes (denominadas nodos) para registrar, compartir y sincronizar transacciones en sus respectivos registros de trazabilidad, mientras que Blockchain organiza los datos en bloques los cuales se van agregando y encadenando (The World Bank Group, 2018).

El contenido del ledger refleja los estados históricos y actuales que se mantienen en el Blockchain. Al ser replicadas, las actualizaciones del ledger deben ser aceptadas por todas las partes. En otras palabras, múltiples partes deben llegar a un consenso.

Una propiedad clave de un sistema Blockchain es que los nodos no confían entre sí, lo que significa que algunos pueden comportarse de manera bizantina. Por lo tanto, el protocolo de consenso debe tolerar fallas bizantinas. Información sobre el consenso distribuido es vasta, y hay muchas variantes de los protocolos que se están desarrollando para Blockchain. Se pueden clasificar en gran medida a lo largo de un espectro, en un extremo está el protocolo basado en cómputo que usan la prueba de cómputo para seleccionar aleatoriamente un nodo que decide sin ayuda la próxima operación. La prueba de trabajo (proof of work o PoW) de Bitcoin es un ejemplo.

Al otro extremo están los protocolos basados en la comunicación, en los que los nodos tienen votos iguales y pasan por múltiples rondas de comunicación para llegar a un consenso. Estos protocolos, como ejemplo principal PBFT, se usa en configuraciones privadas porque supone una autenticación de nodos (Dinh et al., 2018).

- *Criptografía*

Se utiliza para identificar con confianza a todos los participantes de la red y permite la transparencia de las interacciones mientras se mantiene la privacidad de todos en la red. La criptografía es una parte integral del protocolo de consenso en las Blockchain (Voshmgir, 2019).

En Blockchain una de las principales propiedades es el uso de técnicas criptográficas para garantizar la integridad. Al hablar de integridad se refiere a la capacidad de detectar la manipulación de los datos en Blockchain. Esta propiedad es vital en entornos públicos donde no hay confianza preestablecida. En Blockchain privadas, la integridad es igualmente esencial, porque los nodos autenticados podrían actuar maliciosamente.

Hay al menos dos niveles de protección de integridad. El primero, los estados globales están protegidos por un árbol hash (Merkle) cuyo hash raíz se almacena en un bloque. Cualquier cambio de estado resulta en un nuevo hash de raíz. Las hojas del árbol contienen los estados, los nodos internos contienen los hashes de sus hijos. El segundo, el historial de bloques está protegido, es decir, los bloques son inmutables una vez que se agregan a Blockchain. La técnica clave es vincular los bloques a través de

una cadena de punteros hash criptográficos: el contenido del bloque número $n + 1$ contiene el hash del bloque número n . De esta manera, cualquier modificación en el bloque n invalida inmediatamente todos los bloques subsiguientes. Al combinar el árbol de Merkle y los punteros hash, Blockchain ofrece un modelo de datos seguro y eficiente que rastrea todos los cambios históricos realizados en los estados globales (Dinh et al., 2018).

- *Smart Contracts*

Para entender que es un Smart contract primero recordaremos que es un contrato. Un contrato es un acuerdo entre dos o más partes, en el que se define que se puede hacer, como se puede hacer, consecuencias si no se hace, es decir las reglas que permite entender a todas las partes en que va a consistir la interacción que van a realizar. Pues bien los contratos inteligentes son códigos informáticos escritos en algún lenguaje de programación que pueden ejecutarse y hacerse cumplir de forma autónoma y automática sin intermediarios ni mediadores (“Smart contracts, ¿Qué son, cómo funcionan y qué aportan?,” s.f.)

Un contrato inteligente se refiere al cálculo ejecutado cuando se realiza una transacción. Puede considerarse como un procedimiento (Store Procedure) invocado en una transacción. Las entradas, salidas y estados afectados por la ejecución del contrato inteligente (Smart Contract) están acordados por cada nodo. Todos los Blockchains tienen Smart contracts incorporados que implementan sus lógicas de transacción (Dinh et al., 2018).

De acuerdo a la literatura revisada, la principal idea de los Smart contract es permitir el desarrollo de objetos autónomos o dispositivos Internet of Thing (IoT) (Makhdoom et al., 2019).

2.1.6 Protocolos

- *Proof of work (PoW):*

Proof of work o prueba de trabajo, es un cálculo computacional de una función hash criptográfica con cierto grado de dificultad (Nakamoto, 2008). PoW es la base táctica de consenso en bitcoin y otras criptomonedas. Cuando un nodo minero resuelve el PoW, este es elegible para minar un nuevo bloque, mientras que los otros nodos en la

red que tienen una copia completa (full nodes), confirman mutuamente la exactitud del bloque (Zheng et al., 2017).

Otro autor indica que PoW es un algoritmo informático, que se utiliza para llegar a un acuerdo descentralizado, con el objetivo de determinar cuál de los bloques se agregara a la cadena después de minado. El objetivo, es evitar los ciberataques como los de denegación de servicio (DDoS) en los cuales se pretende agotar los recursos de un sistema informático, mediante el envío de múltiples solicitudes falsas (Herrera, 2018).

La forma como se ejecuta la prueba de trabajo se explica a continuación, primero se lleva a cabo mediante la resolución de problemas matemáticos (complejos y variables). Los mineros intentan darle la solución correspondiente para lograr obtener una recompensa en la cadena de bloques. Para minar un bloque de manera exitosa, es necesario ajustar el encabezado del bloque de tal manera que sea menor o igual que el objetivo (Hash). Los mineros llegan a este hash, variando una pequeña porción del encabezado del bloque, llamado “nonce”. Un nonce siempre comienza con “0” y se incrementa cada vez para obtener el hash requerido. Debido a que la variación del nonce es al azar, las posibilidades de obtener un hash en particular, que comienza con muchos ceros, es muy bajo. Por lo tanto, un minero debe hacer muchos intentos variando el nonce, lo que supone efectuar mucho trabajo. Para esto es necesario gran cantidad de energía eléctrica y poder computacional (hardware) que lleven a cabo toda la serie de operaciones (Herrera, 2018).

- *Proof of Stake (PoS):*

Proof of Stake o prueba de participación, busca lograr un consenso descentralizado para validar las transacciones entre los participantes de la red. Este protocolo es una alternativa al mecanismo anterior. Su creación fue el resultado de considerar que la prueba de trabajo desperdicia recursos, ya que los costos por el alto consumo eléctrico y los equipos necesarios para realizar la minería resultaban elevados. Un participante con la mayor cantidad de monedas y tomando en consideración la edad de las mismas, será elegible para minar un nuevo bloque. Además la dificultad para minar es inversamente proporcional a la edad y cantidad de monedas (Tschorsch y Scheuermann, 2016).

Con la prueba de participación, el creador de un bloque nuevo es elegido de manera determinística, dependiendo de su riqueza, definido como participación. En este

sistema, los mineros son llamados forjadores porque ellos siempre son quienes poseen las monedas acuñadas (Mitra, 2019).

Para la prueba de participación lo más relevante es la cantidad de monedas almacenadas en el sistema, lo que supone un interés por parte de la comunidad en que su rendimiento sea óptimo. Los cálculos no llevan tanta dificultad como en el protocolo anterior, basta con demostrar la posesión de un determinado porcentaje en las criptomonedas establecidas.

En este mecanismo los bloques no son minados por los usuarios, sino que se van acuñando según la participación predominante que tenga el usuario de la red y posteriormente se agregan a la cadena de bloques. Aunque el enfoque del mecanismo sea la participación, también se toman en cuenta otros factores como la selección aleatoria de bloques, la selección basada en la edad de monedas, los nodos principales, entre otros. Un aspecto característico de la prueba de participación es que todos los bloques ya fueron previamente minados, es decir, se fija una cantidad en suministro de criptomonedas desde el principio, por lo que no se pueden extraer nuevos bloques (Herrera, 2018).

- *Proof of Activity*

Prueba de actividad es una combinación de PoW y PoS. Los bloques se generan a través del mecanismo de minería PoW y luego se hace un cambio al mecanismo de prueba de participación donde los nodos validadores apilan tokens para ser elegidos y firmar los bloques minados (Bentov, Lee, Mizrahi y Rosenfeld, 2014). Proof of Activity se ha desarrollado a raíz de un supuesto basado en un fenómeno económico llamado "Tragedia de los comunes" (Tragedy of the Commons). Lo que implica que a lo largo del periodo la recompensa por el bloque en las criptomonedas basadas en PoW disminuirá, por lo tanto, los nodos mineros tendrán menos interés en garantizar la seguridad de la red, lo que la hará vulnerable a varios ataques.

El protocolo de prueba de actividad tiene como objetivo aumentar el costo de un ataque para un usuario malintencionado al forzarlo a lograr un índice de hash ocho veces más rápido que el de los mineros honestos en la red. Además, reduce la complejidad de cómputo a 1/10 del Bitcoin basado en PoW, por lo tanto, también minimiza el consumo de energía. Sin embargo, Proof of Activity tiene como objetivo proteger solo las aplicaciones de criptomoneda (Makhdoom et al., 2019).

- *Proof of Authority (PoA)*

Protocolo en el cual algunos nodos predefinidos se consideran autoridades confiables y pueden proponer los siguientes bloques (Makhdoom et al., 2019). Este protocolo utiliza programación round-robin para asignar a cada nodo autoridad una ventana de tiempo durante la cual puede proponer bloques (Dinh et al., 2018).

- *Proof of Elapsed Time (PoET)*

Para abordar los problemas de alto consumo de energía y latencia en los protocolos de consenso basados en PoW, Intel desarrolló un protocolo de consenso basado en lotería llamado "PoET". De acuerdo con este protocolo, el nodo minero que presenta el menor tiempo de espera se selecciona para extraer el siguiente bloque. El protocolo de elección del líder de PoET cumple con los criterios para un buen algoritmo de lotería, es decir, imparcialidad, inversión y verificación. Este protocolo distribuye la elección de liderazgo al azar en toda la población de validadores (Kastelein, 2016). La confianza esta puesta en el hardware que genera el tiempo de espera aleatorio.

- *Proof of Burn (PoB)*

Implica que los usuarios envían monedas a una dirección fiable e irreprochable en sentido figurado, se funde la cantidad de monedas, elegible para explotar un bloque (Iain, 2018). La diferencia entre PoW y PoB es que PoB no tiene costos de energía y sus implicaciones económicas se suman a la estabilidad de la red (Makhdoom et al., 2019).

- *BFT-based Consensus*

BFT es una familia de protocolos de replicación de estado de máquina, que protege contra fallas arbitrarias al replicar los servicios en múltiples nodos (Lamport, 1978; Schneider, 1990). A diferencia de PoW, los protocolos basados en BFT requieren que se conozcan los ID de los nodos de consenso, por lo que son adecuados para las Blockchain privadas (Makhdoom et al., 2019).

- *Practical Byzantine Fault Tolerance (PBFT)*

Está diseñado para ser más eficiente que un PoW en relación con la latencia y los costos de energía, pero solo puede tolerar hasta un 33% de nodos maliciosos. PBFT se considera un protocolo costoso en relación con la cantidad de mensajes necesarios para el consenso (Castro y Liskov, 2002).

La solicitud del cliente se procesa a través de 5 etapas diferentes, es decir, se transmite inicialmente desde el cliente a todas las réplicas, y luego se procesa a través de la etapa de preparación previa, preparación, confirmación y ejecución. Por lo tanto, en una red con cuatro réplicas, una sola solicitud requiere 32 mensajes entre el cliente y las réplicas (Makhdoom et al., 2019)

- *DBFT (Delegated Byzantine Fault Tolerance)*

El protocolo de consenso DBFT se basa en la votación por poder. Los titulares seleccionan los nodos delegados / tenedores de registros que mantienen el consolidado de registros de trazabilidad digital. Se selecciona un orador entre todos los nodos, y juntos estos nodos llegan a un acuerdo y generan nuevos bloques (Makhdoom et al., 2019).

- *Kafka*

Basado en votación autorizada. El líder hace los pedidos. Solo las réplicas sincronizadas se pueden votar como líderes. Kafka no es un Tolerante a Fallas Bizantinas, sino un algoritmo de consenso Tolerante a Fallas.

De acuerdo con la literatura consultada, existe la tecnología que nos puede ayudar a desarrollar este proyecto, ahora veamos las técnicas para llegar a entender las necesidades del usuario para ello explicaremos que es Design Thinking, Lean Startup y Lean Canvas como metodologías que se podrían aplicar para la elaboración de esta tesis.

2.2 ¿Qué es Design Thinking?

Es una herramienta creada por David Kelley, profesor de la universidad Stanford y fundador de IDEO (Consultora de innovación). “Design Thinking” o pensamiento de diseño es una metodología para dar solución a problemas. Se recurre a la empatía con el usuario, para desarrollar productos o servicios más funcionales” (PUCP, 2017). Hoy en día, las marcas grandes o pequeñas se están enfocando en fomentar el recurso que genera mayor valor en los productos y servicios: la innovación, por ende, se sabe que, en estos tiempos de transformación digital, alta competitividad y demandas de los usuarios y clientes, el negocio necesita innovar.

Esta metodología gira alrededor de la experiencia del usuario, permitiendo a los desarrolladores de productos o servicios ponerse en los zapatos de sus clientes o usuarios (TED, 2007). Para hacer este análisis se integran equipos multidisciplinarios, que generen tantas ideas como sea posible. El objetivo de este proceso es aprender a partir de las reacciones de los usuarios al interactuar con el producto (“¿Qué es el Design Thinking y cómo aplicarlo en el trabajo?”, 2018).

David Kalley indicó que el objetivo es enfocarse 100% en los usuarios de los productos y no del producto en sí. El proceso para desarrollar esta metodología consiste en cinco etapas. Dicho proceso no es lineal por lo que se puede ir hacia atrás o adelante si se cree oportuno, incluso saltando a etapas no consecutivas. Las características son (<https://mentorday.es/>; <http://www.ulima.edu.pe/>):

2.2.1 Empatizar:

- La clave en el proceso de design thinking es entender las circunstancias, problemas y necesidades de los usuarios, es decir tener una profunda comprensión de lo que necesitan los usuarios implicados en la solución que se esté desarrollando. Para lograr una buena empatía con el usuario se debe:
- Observar.- Fijarse en los usuarios, en sus usos y sus costumbres en su vida cotidiana siempre desde lejos y sin implicarse.
- Involucrarte.- Mantener conversaciones inesperadas o preparadas, pero siempre teniendo preguntas pensadas y mantener un dialogo mínimamente preparado.
- Mira y Escucha.- Lo mejor es combinar el dialogo y el compromiso, crear fidelidad y motivación para que las personas se sientan parte de un todo, pedir que expliquen cómo hacen su trabajo y que sienten al realizarlo (TiccJeGiga Segovia, 2014; <https://mentorday.es/>; <http://www.ulima.edu.pe/>).

2.2.2 Definir:

Se trata de un esfuerzo por sintetizar el conocimiento generado de la información recopilada durante la fase de Empatía. Es quedarse con lo que realmente aporta valor y perspectivas interesantes alrededor del producto.

Point of View (POV): Una vez determinado el problema se debe enfocar para que sea fácil y eficaz para todos los usuarios. Para que este método funcione correctamente se debe:

- Saber cuál es el problema
- Que genere interés en el grupo
- Calificar ideas y compararlas
- Que plasme las ideas de los usuarios estudiados
- Resolver problemas hasta ahora no corregidos creando una respuesta de fácil comprensión y adaptación (TiccJeGiga Segovia, 2014; <https://mentorday.es/>; <http://www.ulima.edu.pe/>)

2.2.3 Idear:

En esta etapa se generan gran cantidad de ideas y opciones. La primera idea no será la última. Se debe eliminar los juicios de valor, a veces las ideas más extravagantes son las que proporcionan soluciones visionarias. Es en esta etapa donde se puede usar Brainstorm o lluvia de ideas que es una técnica basada en la exposición informal y libre de todas las ideas entorno a un tema o problema planteado que ayuda a estimular la creatividad. Los trucos para una buena ideación son:

- Pensar en todas las ideas posibles
- Registrar todas las ideas
- No juzgar ni debatir las ideas
- Hacerlo en un ambiente cómodo sin presión mientras se tiene una conversación para elegir las mejores ideas (TiccJeGiga Segovia, 2014; <https://mentorday.es/>; <http://www.ulima.edu.pe/>).

2.2.4 Prototipar:

Es decir, materializar las ideas. Consiste en la creación de elementos informativos como son los bocetos, los modelos, las maquetas, los storytelling o una web beta. Esto nos ayuda a visualizar posibles soluciones, poniendo de manifiesto elementos que debemos refinar y mejorar antes del resultado final.

¿Cómo hacer prototipos? Se empieza a construir el prototipo del producto, que no es el producto final, ir evaluando las opciones anteriormente pensadas y enseñar el prototipo al usuario y estar atento a sus reacciones (TiccJeGiga Segovia, 2014; <https://mentorday.es/>; <http://www.ulima.edu.pe/>).

2.2.5 Testear o evaluar:

En esta fase se identifican fallos a resolver, mejoras significativas o posibles carencias. En esta fase, la idea irá evolucionando hasta convertirse en la solución deseada. Pero ¿Cómo evaluar? Entregando al usuario los prototipos sin comentarle nada, se le deja para que interactúe con él y después escuchar todos los comentarios al respecto y responder las preguntas que el usuario realice (TiccJeGiga Segovia, 2014; <https://mentorday.es/>; <http://www.ulima.edu.pe/>).

2.3 Lean Startup

Basándonos en el libro de Eric Ries, “Lean Startup es una metodología para desarrollar negocios y productos. La metodología apunta a acortar los ciclos de desarrollo de productos adoptando una combinación de experimentación impulsada por hipótesis para medir el progreso, lanzamientos de productos iterativos para ganar valiosa retroalimentación de los clientes y aprendizaje validado para medir cuánto se ha aprendido” (Ries, 2011).

Lean Startup se centra en 3 pilares como un círculo interminable y en constante movimiento, primero crea un producto, se continúa midiendo los resultados de lo creado y con el aprendizaje de lo medido volver a crear.

2.3.1 Construir

Una Startup no tiene datos suficientes del mercado para crear un producto completo y que cubra todas las necesidades del mercado, lo ideal es crear un producto mínimo viable (MVP por sus siglas en inglés), el cual tendrá características suficientes para darse a conocer en el mercado, testear la reacción del potencial cliente, que servirá para recopilar información y realizar las mejoras al producto. Este Producto mínimo viable

servirá para definir los clientes que pueden ser los que compren el producto que finalmente se lance al mercado (“¿En qué consiste la metodología Lean Startup?”, 2016)

2.3.2 Medir

Es necesario tener un método fiable y eficaz para realizar la medición del producto, para ello es necesario evaluar los datos de la empresa por ejemplo con cuanto se cuenta y los gastos previstos. Así mismo es necesario medir las necesidades de los potenciales clientes para ajustar el producto a lo que se quiere o espera de él. Conociendo el producto desde su interior (empresa) y exterior (lo que los clientes quieren) se puede elaborar un mejor producto que finalmente llegará al mercado. (“¿En qué consiste la metodología Lean Startup?”, 2016)

2.3.3 Aprender

La empresa aprende de los datos recopilados mediante el producto desarrollado. Esta información servirá para crear un nuevo producto con las mejoras identificadas lo que permite arrancar nuevamente el círculo de crear, medir y aprender.

La importancia del MVP en Lean Startup es:

- Evita crear un producto que nadie quiere
- Permite realizar pruebas sobre el producto y conseguir evidencias del Mercado antes que sea demasiado tarde
- Maximiza el aprendizaje con una inversión mínima (“¿En qué consiste la metodología Lean Startup?”, 2016)

2.4 Lean Canvas

Es una herramienta de visualización de modelos de negocio pensada para empresas que están dando sus primeros pasos. Se basa en la metodología Lean Startup para generar nuevas ideas, desarrollando sus prototipos, con la finalidad de obtener retroalimentación del mercado y validar si la solución planteada es lo que esperan los potenciales clientes.

Se basa en 9 componentes o pilares que son:

- Segmentos de cliente: Explica el segmento de cliente objetivo para la idea de negocio innovadora. En este punto es importante identificar los Early Adopters.
- Problema: Se especifica los 3 principales problemas del público objetivo y sus posibles alternativas de solución
- Proposición de valor única: Es la razón por la cual los potenciales clientes se van a interesar en el producto o servicio propuesto como solución.
- Solución: Se debe centrar en desarrollar las 3 características del producto que van a permitir dar solución a los problemas detectados, el resto se deja para más adelante.
- Canales: Son el medio de acceso a los clientes. Es la estrategia de canales a través de los cuales se va a vender, comunicarte con los segmentos de clientes y captar a los nuevos.
- Flujo de Ingreso: Es donde se define como va a generar dinero nuestro startup. Aquí se plantea la modalidad de compra/suscripción/alquiler, estrategia de recurrencia, barreras de salida, margen comercial, ticket medio, valor del cliente.
- Estructura de costos: Se muestra todo lo que genera gasto en el lanzamiento y puesta en marcha del negocio.
- Métricas: Indicadores relevantes que nos harán saber cómo va el negocio. Aquí se definen los Key Performance Indicators (KPIs), deben ser pocos, pero los datos que ofrecen deben ser relevantes.
- Ventaja Única o especial: Es lo que te hace estar un paso delante de tu competencia, que es difícil o imposible de copiar, por ejemplo, un diseño exclusivo, una patente, barreras de entrada o una tecnología específica (“Lean Canvas: un lienzo para emprendedores | Maestrías INCAE”, 2018)

En base a toda la literatura revisada, vamos a sacar lo mejor de cada metodología para sustentar el desarrollo de la tesis.

CAPÍTULO III: FUNDAMENTACIÓN DEL PROYECTO

3.1 Fundamentación de la deseabilidad del proyecto

El reto del estado peruano para su modernización es la implementación del gobierno electrónico en todos los niveles del Estado: nacional, regional y local, para crear lo que se conoce como valor público, es decir, mejorar la calidad de los bienes y servicios públicos que se brinda a los ciudadanos, para ello es necesario aplicar políticas públicas que tenga como aliada la tecnología y una infraestructura que permita la interconexión, especialmente en un país con una geografía tan diversa como la nuestra.

Los avances tecnológicos, internet y el desarrollo de software hacen posible que ciudadanos puedan hacer sus trámites vía online, ahorrando tiempo, dinero y evitando la burocracia, sin embargo, es importante contar con regulaciones para que las tecnologías sean soportadas en plataformas unificadas y en un mismo lenguaje, logrando interoperabilidad entre ellas y evitar problemas de incompatibilidad de versiones. Esta regulación es un paso importante para la modernización del estado, dado que se podrían aplicar normativas relacionadas a innovaciones tecnológicas. En el Perú tenemos el Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica (Concytec) que puede tener un papel más preponderante y ayude a aplicar las mejores prácticas en cuanto a normatividad y regulación del uso de tecnologías.

En la actualidad, dos de los indicadores de calidad de vida son la salud y la educación, entonces entendemos como la tecnología puede incidir de manera positiva en estos 2 indicadores y sobre todo para la ciudadanía. Es por ello que, en materia de salud, el estado peruano tiene una iniciativa en la cual se está implementando un sistema para tener una única base con información básica de la atención ambulatoria diaria de los pacientes que se atienden en los establecimientos de salud. Este sistema es el paso inicial para una posterior implementación de historias clínicas electrónicas.

Por otro lado, de acuerdo con el estudio de Indicadores Saratoga de PricewaterhouseCoopers (PWC), que se muestra en la web de Infocapitalhumano.pe, hace mención que el índice promedio de rotación laboral en el Perú es de 20,7%

mientras que en Latinoamérica llega a 10,9% y si hablamos solo de rotación voluntaria la proporción se mantiene, en Latinoamérica es de 5,4% mientras que en el Perú es de 9,8% lo que nos coloca como el país con el más alto índice de rotación laboral en Latinoamérica (<http://www.infocapitalhumano.pe>). En base a esta información sumado a que cuando se cambia de trabajo, la empresa aseguradora con la que trabaja nuestro nuevo empleador es diferente donde estuvimos y por ende la cobertura en determinadas clínicas no está incluida, teniendo que optar por ir a una diferente donde antes no te atendías, lo cual ocasiona que nuestras historias clínicas estén distribuidas en distintos centros de salud.

Otro punto que se tomó en consideración es el alto índice de delincuencia común o accidentes de tránsito, en el informe técnico Estadísticas de Seguridad Ciudadana Setiembre 2018 – Febrero 2019 del Instituto Nacional de Estadísticas e Informática (INEI, 2019) solo en Lima en el 2018 se tuvieron 49 336 accidentes de tránsito y a nivel nacional fallecieron 3244 en accidentes de tránsito, por tal motivo, ante alguna emergencia, los profesionales de salud necesitan tener la información necesaria para poder tomar decisiones acertadas y determinar diagnósticos y tratamientos eficaces.

Se realizaron entrevistas individuales no estructuradas con guía para obtener las perspectivas de los entrevistados (pacientes y médicos), relacionado a los principales problemas en la atención durante la hospitalización y/o emergencias y determinar si el problema seleccionado, sobre la importancia de tener disponible y en línea información relacionada a historias clínicas, era relevante para ellos (anexos 6 y 7). El trabajo de campo se realizó entre abril y mayo de 2019 (la ficha técnica se observa en el anexo 14) y se elaboró una guía, la cual se aplicó según el tipo de informante (anexo 15). Las respuestas obtenidas de los pacientes de diferentes hospitales y clínicas indican que tener información disponible relacionada a su historial clínico sería de utilidad pues entre tanto papel que tienen en manos terminan traspapelando o perdiendo algunas hojas de la historia y esto debido a que tienen la preocupación de estar enfermos y tener que afrontar un tratamiento o tener un familiar con alguna enfermedad y ellos asumen el trámite administrativo de mover la historia de un centro de salud a otro.

Otro dato que mencionaron es que en algunas clínicas tienen una especie de tramitador que, a fin de agilizar el trámite, se encargan de recopilar las historias e ingresarlas a la clínica lo cual ocasiona un gasto adicional para el paciente.

También indicaron que, en ese momento, en el que se necesita celeridad para tener toda la documentación a la mano e iniciar cuanto antes el tratamiento, los familiares y el mismo paciente se sienten estresados, frustrados por la burocracia que tienen que pasar para obtener su historia, aunque reconocen que en algunos casos por su carga emocional reaccionan airadamente por todo.

En el caso de profesionales de salud, se pudo observar cierta resistencia debido a que indicaban que probablemente iba a ser más carga administrativa y no les dejarían estar en contacto con sus pacientes. Sin embargo, si creen que es necesario dado que en caso tengan que transferir a algún paciente a otro centro de salud, la atención sería con información actualizada y el doctor que tome el caso podría tener más alternativas para un tratamiento efectivo.

Un punto que también se observó es que está bien interiorizado el concepto de “segunda opinión” (relacionado a que el nuevo médico tratante debe volver a evaluarlo), indican que a pesar de que el paciente llega con algún diagnóstico y exámenes ya realizados, lo que recomiendan es volver a realizar los mismos exámenes y/o complementarios a fin de dar un diagnóstico. Sin embargo, la revisión de toda información que tenga el paciente sirve de base para indicar el tratamiento a seguir.

Con la información recabada se empezó a acotar el alcance del proyecto de innovación, dado que se quería tener una plataforma de salud que abarque varios puntos en cuanto al cuidado preventivo y atención de enfermedades, sin embargo, esto sería muy difícil de realizar si es que antes no se empiezan a sentar las bases y para ello es necesario tener la información de las historias clínicas. Todo esto gracias a la interacción con los potenciales clientes (Pacientes y médicos). Por lo expuesto, nuestra propuesta es cubrir la necesidad de disponibilidad de información relacionada a historias clínicas, para los tipos de atención de emergencias y hospitalizaciones para pacientes de clínicas del sector privado, inicialmente se espera realizarlo con 2 clínicas de Lima que actualmente ya cuentan con un sistema hospitalario y posteriormente expandirlo a nivel nacional, el alcance ha sido acotado debido a que el cambio técnicamente es grande tanto para los pacientes, médicos y el sector salud en general.

3.2 Fundamentación de la factibilidad del proyecto

Para la implementación de la plataforma de salud se utilizará Blockchain que nos permitirá compartir entre instituciones de Salud el historial clínico de cada paciente, para establecer el registro único y distribuido, usando un registro de trazabilidad para probar la autenticidad de la información durante la atención del tipo hospitalización y emergencias, así como tener disponible la información. Con este esquema basado en Blockchain lo que se va a lograr es tener información inmutable, seguridad, transparencia (al paciente, entre instituciones, el estado) y confiabilidad distribuida relacionado a que no todo el procesamiento de las transacciones se realiza en el mismo lugar, por ende el nivel de confianza es mayor (Buterin, 2015).

Por otro lado, lo que se busca con esta plataforma de salud es sentar las bases para que sea escalable en el tiempo.

Respecto al financiamiento se presentará el proyecto al estado para que sea el principal colaborador y sobre todo regulador con la finalidad que las clínicas se adhieran a esta nueva plataforma y así aportar en la transformación que están realizando. Para lograr una alianza estratégica con el estado, se va a mostrar las funcionalidades que ofrece la Blockchain, la finalidad es que experimenten con el producto, generar confianza, compartir nuestro conocimiento en esta tecnología y obtener de ellos el conocimiento del sector. Para ello se va a recurrir al apoyo y soporte de la Universidad de Lima que nos brindará respaldo Teórico-práctico y contactos para organizar reuniones en las cuales podamos mostrar el producto. Por otro lado, también se participará en las convocatorias que realizan CONCYTEC y el mismo MINSa en la cual se va a proponer esta iniciativa. También se presentará a incubadoras como por ejemplo el SIE de la Universidad Católica, Wayra, y a las mismas clínicas para obtener el apoyo necesario y empezar a implementar el proyecto.

3.2.1 Modelo de Negocio

- **Antecedentes y actualidad de la Economía colaborativa en el Perú:**

Tenemos la opinión de Rolando Arellano (2018), en la que indica que la economía colaborativa se practica en el Perú desde hace mucho tiempo, pero ¿qué es economía colaborativa?, en palabras simples es una corriente orientada a prestar,

alquilar, cambiar o vender bienes o servicios y así reducir desperdicios e ineficiencias cuidando el medio ambiente y lo ejemplifica haciendo una comparativa de lo que hacíamos en el Perú y las “novísimas tendencias”:

- El servicio de reciclaje del ropavejero que es parecida a la plataforma de Mercado Libre donde se intercambian cosas usadas por monedas
- La novísima actividad económica Car-Sharing contra los autos colectivos que movilizan a muchas personas desde hace varios años en Perú.
- Los Wawahuasi cuya actividad es muy similar al movimiento “nursery co-ops” donde los padres crean guarderías para cuidar colectivamente a sus hijos.
- Las polladas pro-fondos donde se compra tickets para apoyar a algún conocido, a cambio de una buena presa de pollo y el compromiso de ayuda recíproca. Este es un ejemplo de “crowdfunding”

En la actualidad es necesario y vital comprender el comportamiento del consumidor digital peruano, por ello gracias a los datos proporcionados por Comscore que es una consultora líder en investigación y medición del mundo digital y sus audiencias, nos muestra que la población online peruana tiene rostro joven es decir que los visitantes a páginas web o plataformas online están entre las edades de 15 a 24 años de edad y representan un 30.2% de usuarios, mientras que el 21.1% está entre los 25 y 34 años. Según el estudio el peruano ocupa 25.5 por mes en internet y nos sitúa en el cuarto puesto en América Latina que más consume internet. Un dato importante son las preferencias de consumo y nos muestra que el usuario digital peruano dedica 4.8 horas mensuales en servicios digitales implementados por instituciones públicas o financieras (“¿Cómo es el consumidor digital peruano?”, 2019). Este dato nos ayuda a vislumbrar que en un futuro los nuevos consumidores digitales preferirán utilizar más y más los servicios digitales que las instituciones públicas implementen.

- **Monetización en una Blockchain**

Para Vaughan (2016), CEO de Tierion, menciona que las forma que las empresas blockchain ganan dinero son:

- Software como servicio: cobran una tarifa por usar su API e infraestructura.

- Servicios profesionales: algunas empresas crean proyectos personalizados para clientes empresariales. Muchas empresas existentes tienen áreas de práctica de blockchain. Ejemplos: IBM, Deloitte y Gem.
- Tarifas planas y tarifas por transacción: algunas empresas construyen y mantienen redes entre un consorcio de socios. Ganan dinero cobrando una tarifa de suscripción o una tarifa por transacción por la actividad en la red.
- Acuerdos de nivel de servicio: algunas empresas crean plataformas e infraestructura de host para clientes empresariales. Ofrecen un SLA para tiempo de actividad y mantenimiento.
- Criptomonedas: algunas empresas de Blockchain emiten su propio token o la administración posee grandes cantidades de una criptomoneda como Ethereum. Estas empresas realizan un trabajo que aumenta el valor de mercado de su token. Luego la venden a los especuladores.

Para nuestro proyecto innovador se espera obtener ingresos a través del cobro de tarifas por transacción relacionada al tráfico que se realice en la Blockchain. Por otro lado, también se espera cobrar por el uso de las APIs e infraestructura (Software como servicio). Lo que se propone es que nos encargaremos de la construcción y mantenimiento de la Blockchain.

3.2.2 Marco Legal

El Perú está en proceso de transformación, y ya se evidencia el interés por parte del estado, que mediante el decreto de Urgencia N° 006-2020 crea el sistema nacional de transformación digital establece el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno. Asimismo la ley 30024 creo el Registro Nacional de Historias Clínicas Electrónicas (RENHICE). Se trata de una plataforma que permite al paciente o su representante legal dar acceso a información clínica a profesionales de la salud que son previamente autorizados por ellos, con la finalidad de garantizar la calidad de la

atención en los establecimientos de salud y en los servicios médicos de apoyo públicos, privados, mixtos así como la protección de los datos personales del paciente, establecidos por la ley 29733 (Ley de protección de datos personales) (Rojas Mezarina, Leonardo Cedamano Medina & Vargas Herrera, 2015). Asimismo MINSA a través de resoluciones ministeriales como por ejemplo R.M. N° 120-2017/MINSA en la que se aprueba la directiva administrativa N°230-MINSA/2017/OGTI que establece los estándares y criterios técnicos para el desarrollo de sistemas de información en salud. Por lo expuesto, esta iniciativa cuenta con bases legales que la respaldan.

3.3 Fundamentación de la viabilidad técnica

En este punto vamos a explicar los costos asociados para la implementación de nuestro proyecto de innovación, el flujo de caja proyectado y los beneficios de implementar esta iniciativa.

En cuanto a los costos relacionados al personal, se tiene previsto contar con tres desarrolladores, dos con experiencia en Blockchain y el otro en temas de desarrollos web y/o aplicativos, dos analistas funcionales que apoye en la interacción y levantamiento de información con nuestros potenciales clientes y apoyo en las pruebas funcionales así como un Scrum Master. Respecto a los desarrolladores, se van a contratar desarrolladores freelance de la India, esto debido al costo y a que localmente aún no tenemos especialistas en desarrollo Blockchain. Los costos se aprecian en la tabla 3.1.

Para la infraestructura, almacenamiento y red, se está considerando el costo de configurar una Blockchain usando Hyperledger Fabric que incluye en general dos elementos: la infraestructura y el costo de desarrollo. Este enfoque es más fácil ya que los líderes del mercado de Cloud Computing ya proporcionan infraestructura de Hyperledger Fabric. En ese sentido se puede omitir los aspectos de infraestructura, almacenamiento y redes. Además, está utilizando una plataforma de Blockchain lista para usar, por lo tanto, no necesita centrarse en el intercambio de archivos, el cifrado, el algoritmo de consenso y la red P2P. Hyperledger Fabric tiene una arquitectura modular y proporciona algoritmos de consenso conectables. Como se observa en la tabla 3.2, se está optando por contratar el servicio de IBM en su plan inicial más 2 nodos "Igual" con la finalidad de poder crear 2 organizaciones más al momento de desarrollar el producto

mínimo viable de esta iniciativa. El plan inicial ofrece una red Blockchain pre configurada, es decir es una red permissionada (permissioned), dos organizaciones con un igual por cada organización, una entidad emisora de certificados (CA), un clasificador o nodo de ordenación y un canal de forma predeterminada. Los conceptos de CA, igual y nodo de ordenación se detallan en la sección Glosario.

En cuanto al lugar de trabajo, se tiene una tienda que puede servir para reunirnos a trabajar en equipo, se tendrá que pagar luz, agua e internet que es un aproximado de seiscientos soles mensuales.

Tabla 3.1

Costos mensuales del equipo de trabajo para implementar el proyecto

Roles	Costo / hora	Cantidad personas	Horas por día	Días por mes	Meses	Costo total(\$)
Desarrollador Blockchain	\$50	2	8	22	6	105600
Desarrollador Website	\$25	1	8	22	3	13200
Analista Funcional	\$15	2	8	22	5	26400
Scrum Master	\$20	1	8	22	6	21120

Fuente: Elaboración propia

Tabla 3.2

Precios de Cloud Computing para infraestructura Blockchain

Empresa	Costo por mes	Costo Total Aprox. (\$)
IBM Blockchain Platform(plan Inicial)	\$750	\$4500

Fuente: Elaboración Propia

Tabla 3.3

Pago de servicios básicos (Gastos Generales por mes con T.C. 3.4 soles)

Servicios	Monto mensual Estimado	Monto total Soles
Luz	150	900
Agua	100	600
Internet	300	1800

Fuente: Elaboración Propia

Tabla 3.4

Muebles en General

Inversión Tangible	Total(\$)
Muebles en General	4740

Fuente: Elaboración Propia

Tabla 3.5

Gastos Varios

Inversión Intangible	Total(\$)
Gastos de Organización	2500
Gastos de capacitación	10000

Fuente: Elaboración Propia

Tabla 3.6

Cálculo de costo total de la propuesta

Descripción	Total Proyecto (\$)
Muebles en General	4740
Gastos de Organización	2500
Gastos de Capacitación	10000
Pago de sueldos e infraestructura Blockchain (x6 meses)	170820
Gastos de Operación (x6 meses)	2452.94
Total Propuesta	190512.94

Fuente: Elaboración Propia

- Cálculo de la demanda potencial

A continuación, se presenta la demanda potencial considerando:

- Informe técnico: Situación del Mercado Laboral en Lima metropolitana (INEI, 2019)

En este informe nos indica que hasta abril del 2019 se tenía 4 millones 871 mil 500 personas ocupadas (con trabajo) y que el 52.6% del total de población ocupada está en el rango de edad de 25 a 44 años, lo que equivale a 2 millones 561 mil 800 personas.

Asimismo, el 68.2% (3 millones 323 mil 600 personas) cuentan con seguro de salud (EsSalud, Seguro privado de salud o Seguro integral de salud).

Dentro de este grupo el 6.6% tiene EsSalud y además Seguro Privado, lo que equivale a 219 mil 358 personas y el 1.9% solo Seguro Privado, lo que equivale a 63148 personas.

Por lo tanto, para efectos del proyecto se está asumiendo que la demanda potencial será de 282506 de personas.

Al cabo del primer año se estima tener el 2.5% del mercado potencial, los siguientes años se espera crecer a razón de 5%. Por ejemplo, para el segundo año el valor se obtiene de multiplicar 5% por 282506 menos 7063.

Tabla 3.7

Cálculo de usuarios por año

Descripción	Año 1	Año 2	Año 3	Año 4	Año 5
Usuarios por año	7,063	13,772	26,167	35,326	40,036

Fuente: Elaboración Propia

De acuerdo a la dirección de estadística de la Policía Nacional de Perú, nos muestra que en el 2018 la cantidad de heridos producto de un accidente de tránsito fue de 61512, haciendo un promedio se tiene que mensualmente hay 5126 accidentes aproximadamente (Rojas Medina, 2019)

Se ha determinado que los pacientes interactuarán 3 veces con la Blockchain, por lo cual este es nuestro ratio para determinar la cantidad de transacciones.

Tabla 3.8

Proyección transacciones realizadas por año

Periodos	Año 1	Año 2	Año 3	Año 4	Año 5
Por usuarios nuevos	7,063	13,772	26,167	35,326	40,036
Por usuarios antiguos		7,063	20,835	47,002	82,328
Total Transacciones	21,188	62,504	141,006	246,983	367,090

Fuente: Elaboración Propia

Se ha determinado que el precio promedio por transacción será de un dólar con 40 centavos, al tipo de cambio de 3.4, equivale a 4 soles 76 céntimos. Se espera ajustar el precio a medida que la cantidad de transacciones aumenten. Para determinar el precio se consideró el costo variable que tienen las transacciones financieras. En la actualidad

es de 2.99% con tarjetas de débito y 3.99% con tarjetas de crédito, sin embargo, en los últimos años la tasa era de 8%, pero se fue reduciendo gracias a la propagación de terminales en más de 200000 comercios, según lo indicó Victor Gonzales, Gerente de Nuevos Negocios Visanet Perú (Pagos con tarjetas: ¿Qué comisiones pagan los negocios que usan POS?, 2018). Es por ello que en base a los costos detallados líneas arriba se determinó el precio de transacción en la Blockchain y se espera ir ajustándola. Por otro lado también se debe tomar en cuenta que el proyecto está orientado a un emprendimiento social.

Tabla 3.9
Proyección de ventas

Periodos	Año 1	Año 2	Año 3	Año 4	Año 5
Precio Promedio	1.40	1.40	1.40	1.40	1.40
Cantidad de transacciones	21,188	62,504	141,006	246,983	367,090
Ventas (\$)	29,663.13	87,506.23	197,408.13	345,775.69	513,925.59

Fuente: Elaboración Propia

Para determinar el costo de mantenimiento del servicio se ha considerado 2 analistas funcionales y un desarrollador Blockchain. Por otro lado se estima que el precio de la plataforma Blockchain de IBM se incrementará 10% año a año, como se muestra en la siguiente tabla.

Tabla 3.10
Proyección costo de mantenimiento de servicio anual

Periodos	Año 1	Año 2	Año 3	Año 4	Año 5
MOD	47,040	49,392	51,862	54,455	57,177
Infraestructura Blockchain	9,000	9,900	10,890	11,979	13,177
Costo Mantenimiento	56,040	59,292	62,752	66,434	70,354

Fuente: Elaboración Propia

Dentro de los gastos generales se están incluyendo los gastos de servicios básicos, en los gastos administrativos se está considerando el pago a personal administrativo que soporta la operación y un aproximado de 100 dólares mensuales en cuanto a gastos de venta tal como se muestra en la siguiente tabla.

Tabla 3.11

Gastos de Operación

Periodos	Año 1	Año 2	Año 3	Año 4	Año 5
Gastos Generales	1,941.18	2,038.24	2,140.15	2,247.15	2,359.51
Gastos Administrativos	18,943.77	19,890.95	20,885.50	21,929.78	23,026.27
Gastos de Ventas	1,200.00	1,260.00	1,323.00	1,389.15	1,458.61

Fuente: Elaboración Propia

Con el detalle explicado, se obtiene el estado de ganancias y pérdidas que se muestra en el anexo 16. A continuación mostramos los flujos de caja proyectados a 5 años tanto económico como financiero. En el flujo económico se puede observar que a partir del segundo año los flujos futuros se vuelven positivos, mientras que en flujo financiero es a partir del tercer año.

Tabla 3.12

Flujo de caja Económico

RUBRO	AÑOS					
	Año 0 (\$)	Año 1 (\$)	Año 2 (\$)	Año 3 (\$)	Año 4 (\$)	Año 5 (\$)
Ingresos Por Ventas						
Ingresos		29663.13	87506.234	197408.13	345775.69	513925.59
Valor Rescate de Capital Trabajo						173272.94
Total Ingresos		29663.13	87506.234	197408.13	345775.69	687198.53
Costo mantenimiento del servicio		56040	59292	62751.6	66433.68	70354.31
Gastos operativos		22084.94	23189.19	24348.65	25566.08	26844.39
Impuestos		0.00	906.60	33,092.36	76,132.78	125018.07
Inversión	190512.941					
Total Egresos	190512.94	78124.942	83387.791	120192.61	168132.54	222216.77
Flujo Neto Económico (Dólares)	-190512.9	-48461.81	4118.44	77215.52	177643.15	464,981.77

Fuente: Elaboración Propia

Tabla 3.13

Flujo de caja Financiero

RUBRO	AÑOS					
	Año 0 (\$)	Año 1 (\$)	Año 2 (\$)	Año 3 (\$)	Año 4 (\$)	Año 5 (\$)
Ingresos por Venta						
Ingresos		29663.13	87506.234	197408.13	345775.69	513925.59
Valor Rescate de Capital Trabajo						173272.941
Préstamo	20000					
Total de Ingresos	20000	29663.13	87506.234	197408.13	345775.69	687198.53
Costo mantenimiento del servicio		56040	59292	62751.6	66433.68	70354.314
Gastos de operación		22084.94	23189.19	24348.65	25566.08	26844.39
Intereses		5013.33	2003.04	0	0	0
Amortización de Préstamo		8494.85	11505.15			
Impuesto		0	906.60108	33092.3644	76132.7788	125018.068
Inversión	190512.941					
Total Egresos	190512.94	91633.13	96895.98	120192.61	168132.54	222216.77
Flujo Neto Financiero (Dólares)	-170512.9	-61970	-9389.74	77215.52	177643.15	464981.77

Fuente: Elaboración Propia

Se muestran los cálculos del VAN y TIR Económico y financiero. Para el cálculo del VAN Económico se utilizó el WACC obtenido que se muestra en el anexo 17. Para el VAN Financiero se utilizó el KOE, el cual se asume que será de 15%.

Tabla 3.14

Indicadores Económicos

Indicadores Económicos	Valores
Valor Actual Neto Económico (VANE) en Dólares	521037.59
Valor Actual Neto Financiero (VANF) en Dólares	493042.61
Tasa Interna de Retorno Económico (TIRE)	29.62%
Tasa Interna de Retorno Financiero (TIRF)	29.84%

Fuente: Elaboración Propia

En base al análisis del VAN del proyecto podemos concluir que la ejecución de este genera ganancias por encima de la rentabilidad solicitada por los socios.

Al realizar el análisis de la TIR podemos concluir que el proyecto genera una rentabilidad mayor a la tasa solicitada por los socios de la empresa.

Por otro lado, el periodo de retorno de la inversión es de 4 años 5 meses, tal como se muestra en el anexo 18 y 19.

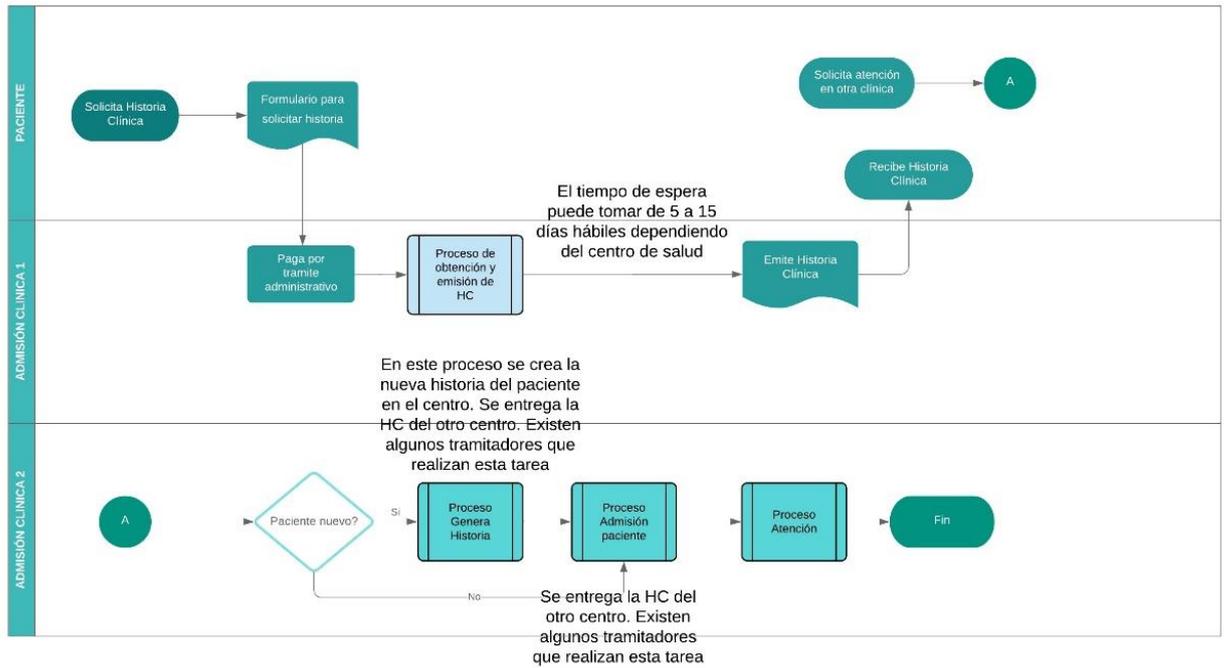
Los costos mostrados están relacionados a la implementación de una demo la cual se basa en varios supuestos. Posterior a la implementación de la demo se debe recalcular los costos contemplando los relacionados a la elaboración del caso de uso empresarial para lo cual se requiere considerar al equipo que se encargará de su definición y el tiempo que tomará dicho levantamiento de información y definición de alcance.

El beneficio que se lograría con la implementación de este proyecto es que las clínicas podrán ahorrar tiempo y dinero en la atención del paciente, generando satisfacción pues se les atenderá con rapidez y sin mucho trámite administrativo, por otro lado, las personas que antes realizaban la tarea de mantener las Historias clínicas ahora podrán enfocar su esfuerzo en otras tareas que le den valor al negocio. Se reducen costos operativos, al eliminar tareas de registro manual, almacenamiento y mantenimiento del lugar físico donde se almacenan las historias, control de las historias y distribución de las historias cuando el paciente se atiende. Sin contar el tiempo que le toma a las enfermeras obtener la historia antes de cada atención.

En la siguiente figura mostramos el flujo actual cuando el paciente solicita la Historia clínica en el sector privado, se puede observar que existe un tiempo mientras se le entrega la historia completa y la atención en el nuevo centro, asimismo en el nuevo centro al ingresar, necesariamente van a solicitar nuevos exámenes, lo cual también es un tiempo que el paciente pierde. De tener la historia clínica en línea se podría enfocar el esfuerzo, solicitando exámenes que complementen el diagnóstico u otros que permitan ampliar posibles tratamientos.

Figura 3.1

Flujo actual de solicitud de historia Clínica – Sector Privado



Fuente: Elaboración propia

CAPÍTULO IV: DEFINICIÓN DEL PROYECTO

El proyecto propone tener la información del paciente en línea y distribuida, para ello se va a apoyar en la tecnología Blockchain por las características ya descritas en el capítulo dos. Se espera que esta iniciativa ayude a cientos de pacientes que por diversos motivos pasan por el penoso momento de estar hospitalizados o por alguna emergencia, permitiendo que su historial clínico pueda ser consultado por cualquier institución privada en la cual el paciente se vaya a atender, así mismo permitir a los profesionales de salud tener información relevante y de base que permita dar continuidad a tratamientos, dar diagnósticos más acertados y explorar alternativas de tratamientos. Como parte de este proyecto se espera digitalizar los informes de diagnóstico, recetas médicas y tratamientos.

No es parte del proyecto las consultas ambulatorias o externas que son las citas que un paciente realiza de forma voluntaria como medida de precaución o reactivas ante alguna dolencia o enfermedad. Tampoco abarca Imágenes ni radiografías, debido a que los sistemas que actualmente existen manejan adecuadamente esta información, sin embargo en una próxima mejora se puede incluir dichos documentos. Se ha pensado que la integración con estos sistemas de imágenes y radiografías(RIS), laboratorios (LIS) se puede dar a través de un gestor documental en la nube y esto es factible gracias al creciente uso de servicios cloud públicos por parte de las empresas, la mayor virtualización de los entornos cloud privados y el aumento de conexiones M2M en la nueva era del Internet de las Cosas, son algunas de las razones por las que esta tendencia seguirá creciendo para multiplicarse en los próximos años.

Respecto a los integrantes del equipo, se propone tener un Scrum Master y un equipo de desarrollo conformado por 5 personas las cuales apoyaran en el diseño e implantación de la plataforma. Como Product Owner estarían nuestros potenciales clientes que son los pacientes y los profesionales de salud que nos van a guiar en cuanto a lo que debe tener nuestro prototipo. Referente a los materiales, contamos con Pizarra plumones, papelógrafos, post-it, equipos de cómputo (3), mobiliario de oficina y un local el cual servirá como centro de labores.

En cuanto a los aspectos técnicos del proyecto, de acuerdo con la literatura revisada, optamos por usar Blockchain por el nivel de seguridad que brinda con el uso de claves de encriptación en conjunto con Infraestructura clave pública (KPI por sus siglas en inglés) para autenticar y autorizar a las partes y encriptar comunicaciones, esto debido a lo sensible de la información que se va a manejar al tratarse de Historias clínicas. Inicialmente solo serán de instituciones privadas ya que las clínicas cuentan con sistemas hospitalarios y sus historias ya están digitalizadas. El objetivo del proyecto es presentarlo al estado, mostrarle las bondades de esta tecnología y lograr una alianza estratégica para que ellos como ente regulador nos ayuden a que las instituciones privadas de salud se adhieran al uso de la plataforma. Lo que se espera es que el estado observe los resultados de primera mano, se convenza y asuma las actividades de adecuación de procesos, de tecnología y digitalización de documentos, para que en un futuro los hospitales nacionales también la adopten.

A continuación, explicaremos a alto nivel el funcionamiento de la Blockchain:

- Cuando una institución de salud quiere crear o agregar un formulario a una historia clínica. En la red la historia es el activo que se va a transaccionar.
- La transacción se representa en la red como un bloque.
- Dicho bloque se transmite a todos los nodos de la red
- Los nodos validadores que están en la red aprueban la transacción y la dan por válida
- El bloque puede agregarse a la cadena, lo que proporciona un registro indeleble y transparente sobre las transacciones.

El principal aspecto económico para considerar en este proyecto es que la mano de obra es costosa y poco asequible, esto debido a que se debe tener un nivel de especialización en cuanto a desarrollo de Blockchain. En la actualidad se puede contar con desarrolladores con experiencia en EEUU., Europa, India y África y los costos por hora varían entre 50 a 100 dólares, lo que eleva los costos del proyecto (<https://www.howtotoken.com/>; <https://www.workana.com/>). El equipo de proyecto debe estar preparado para trabajar en un ambiente intercultural, la diferencia horaria y sobre todo a la barrera del idioma con la finalidad que la comunicación sea efectiva.

Haciendo una revisión de experiencias en el mercado internacional, existen iniciativas que están soportadas en la tecnología Blockchain en distintos rubros, por ejemplo:

- El gobierno de Japón ha iniciado un proyecto para unificar el registro de propiedades urbanas y rústicas con tecnología Blockchain.
- La empresa Ernst & Young (EY) está desarrollando un sistema llamado carsharing basado en la tecnología Blockchain para compartir coches de manera sencilla.
- En la música, Spotify está apostando a su propia Blockchain para gestionar su reproducción, distribución y disfrute (Pastor, 2018).

Sin embargo aún se considera que esta tecnología tiene mucho más por explotar y descubrir, sobre todo en temas de velocidad de procesamiento de transacciones, cyber seguridad, por ejemplo, el fallo en el token “the DAO” (Decentralized Autonomous Organization) que tenía dos fallos de seguridad y que la solución provocó la división de la cadena principal en dos criptomonedas (Rodríguez G, 2017), entre otros.

Por otro lado, analizando el mercado peruano, en la actualidad nuestra información financiera ya se encuentra expuesta y centralizada por una entidad (Equifax) así como la información de nuestros números telefónicos relacionado a portabilidades numéricas en telecomunicaciones, con lo cual ya somos conscientes que nuestra información personal se encuentra en la web.

De las entrevistas realizadas, se observa que hay profesionales de salud que aún tienen resistencia al uso de los sistemas hospitalarios, indicando que el hecho de dar muchos “clicks” en las pantallas de los sistemas de salud los distrae en su objetivo principal que es el de atender al paciente, sentir la cercanía que tenían con él cuando las anotaciones las hacían en papel. Esta información la obtuvimos producto de las entrevistas realizadas a los médicos y que se muestra en la matriz de problemas del Anexo 6. En otros casos, mencionaron que a pesar de que la clínica tiene el sistema, ellos escriben en papel y es el personal administrativo o los técnicos de farmacia quienes actualizan el sistema acorde a sus indicaciones. Por otro lado, tenemos a los pacientes que están en diferentes rangos de edades. Los mayores a cincuenta y cinco años no ven necesario el uso de tecnología para la administración de sus historias, por temor a no saber cómo utilizarla, sin embargo, tenemos a los más jóvenes que ven con

buenos ojos el hecho de empezar a transformar digitalmente algunas actividades administrativas burocráticas. Es a este grupo de pacientes entre el rango de edades de 25 a 40 años que denominaremos nuestros “Early adopters” (primeros clientes que adoptan un producto para solucionar su problema y están dispuestos a dar ideas para mejorarlo) a quienes estará dirigido nuestro esfuerzo. Seleccionaremos pacientes en ese rango de edad y les comunicaremos a ellos o familiares cercanos que su historia clínica está siendo unificada de todas las clínicas donde se atendió alguna vez y se le está dando acceso a la institución donde está hospitalizado.

4.1 Objetivo general

- Proponer la transformación digital de historias clínicas en el sector salud privado para los tipos de atención médica hospitalaria y emergencias utilizando tecnología Blockchain con el objetivo de gestionar documentos sensibles y mejorar la experiencia de los pacientes.

4.2 Objetivos específicos

En base al objetivo general se han propuesto los siguientes objetivos específicos:

- Definir una propuesta de transformación digital de historias clínicas utilizando tecnología Blockchain con la cual se va a desarrollar la plataforma.
- Evaluar técnica y económicamente la factibilidad de la propuesta.
- Mejorar la calidad de vida de los pacientes utilizando la tecnología como apoyo para gestionar su historial clínico independientemente del lugar donde se atienda sin invertir mucho tiempo.
- Explicar cómo funciona la plataforma con tecnología Blockchain
- Mostrar un prototipo de las principales funciones de la Blockchain.

4.3 Diseño propuesta de valor

En este punto hablaremos de:

4.3.1 Perfil del cliente

El cliente realiza los siguientes trabajos:

- Buscar referencias de las clínicas donde se va a hospitalizar para tratamientos específicos
- Visita frecuente a centros de salud
- Ir a todas las instituciones donde se atendió para obtener su historia clínica
- Solicitar historial clínico
- Pagar por la atención

Las frustraciones del cliente son:

- Inconformidad por el proceso para obtención de Historias clínicas
- Desconfianza en el personal que va a recabar la información de la Historia clínica
- Desconocer como es el proceso administrativo para obtener la información
- Inconformidad por la burocracia
- Deficiente tiempo de respuesta

Las alegrías del cliente son:

- Obtener la historia clínica en el menor tiempo posible
- Diagnóstico y tratamiento efectivo
- Capacidad de modificar el tratamiento que iba recibiendo el paciente, en base a la revisión de la historia clínica y del nuevo diagnóstico
- Tener la información del historial clínico actualizada y consolidada.
- Sentir que la Atención será personalizada y de Calidad

4.3.2 Perfil del valor del producto

El cliente sentiría aliviadas sus frustraciones si tan solo lograra:

- Conocer el proceso administrativo para obtener la información
- Que alguien explique los pasos a seguir
- Que siempre esté disponible la información de la historia clínica
- Desarrollar procesos para relacionar al paciente con la institución de salud y conseguir mejorar el desempeño del servicio
- Que la información de historias clínicas pueda ser consultada a demanda

Un servicio que logre solucionar las molestias del cliente y ofrecerle resultados y beneficios debería:

- Ser un servicio de administración y consultas de historias clínicas
- Tener un portal web con información de los historiales clínicos
- Administrar la información de las historias clínica y que el cliente no tenga que preocuparse de ese aspecto y sus impactos legales
- Tener disponible la información
- Ser confidencial y ofrecer seguridad de información

Los beneficios y los resultados que tendría el cliente con un servicio de este tipo serían:

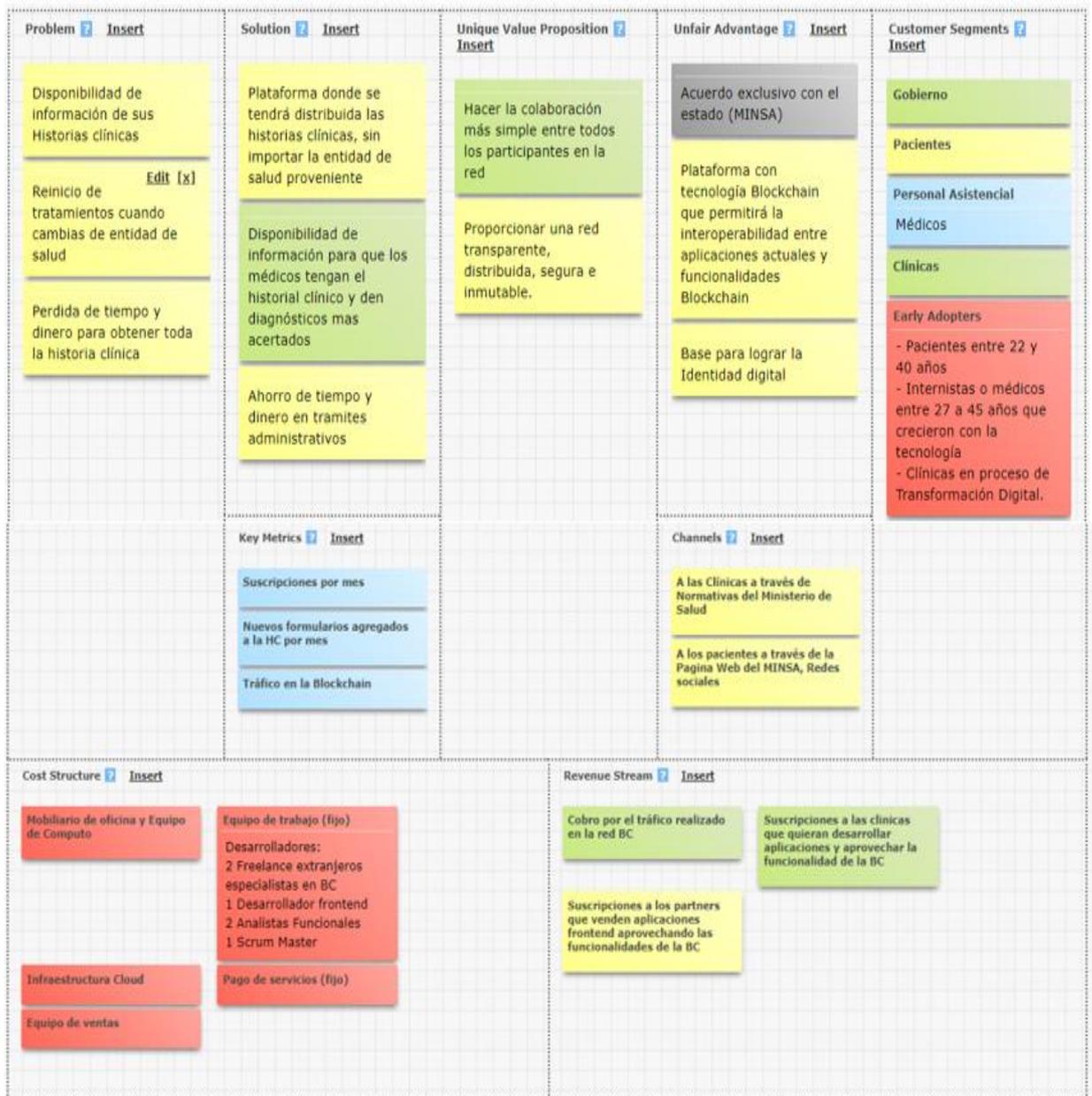
- Desapego en temas administrativos relacionados a la historia clínica
- Facilidad para acceder a la información del paciente
- Disposición de la información por el tiempo deseado y en el momento indicado

Después de realizar la observación y diseño de las hipótesis, hacemos una revisión detallada de la propuesta de valor, como resultado nuestra propuesta de valor es: Proporcionar una red transparente, distribuida, segura e inmutable así como hacer la colaboración más simple entre todos los participantes en la red. Ver Anexo 5.

4.4 Modelo de negocio propuesto.

Para poder explicar el modelo de negocio, lo hemos plasmado en el lienzo de Lean Canvas que nos ayuda a mostrar de manera rápida, concisa y efectiva nuestra propuesta. Ver figura 4.1.

Figura 4.1
Modelo de Negocio



Elaboración propia

CAPÍTULO V: DESARROLLO DEL PROTOTIPO

En este capítulo vamos a desarrollar la etapa clave en design thinking. Como explicamos en el capítulo dos, prototipar es generar elementos informativos que pueden ser dibujos, objetos o artefactos con los que se pretende responder a las inquietudes o dudas que nos permitan acercarnos a la solución final. Prototipar es crear un producto mínimo viable (PMV) que tengan la funcionalidad mínima requerida por el cliente y/o usuario para que pueda trabajar o experimentar sin necesidad de usar materiales o software complejos, se busca siempre la simplicidad. De acuerdo con lo que se indica en design thinking, puede ser cualquier cosa con la que se pueda interactuar, por ejemplo, un post-it, cartones doblados, alguna actividad o un storyboard. Entre las características básicas que debe tener el prototipo es que se realice de forma rápida y que sea económico, pero debe tener contenido para que pueda generar retroalimentación del equipo y de clientes y/o usuarios.

Para poder conceptualizar la idea del proyecto y comunicarla de manera fácil y comprensible a todo tipo de público, se elaboró un storyboard en base a las experiencias tanto de los pacientes como de los médicos. En ella se describe la experiencia de un paciente llamado “Jose” que siempre se atiende en la clínica “A” y debido a una enfermedad que le detectaron debe ser hospitalizado y le recomiendan seguir su tratamiento en otra clínica especializada en ese tipo de enfermedades. En la clínica “B” inicia tratamiento, pero no se siente cómodo debido a que no siente confianza en lo que le están realizando por lo que sus familiares le recomiendan que vaya a la clínica “C” y así lo hace, sin embargo, se encuentra con un problema debido a que tiene que trasladar su historia de clínica en clínica. Y ¿Qué hacer en estos casos?, pues nuestra idea es tener disponible y en línea la historia clínica del paciente, independientemente del lugar donde se atienda, con esto se beneficia el paciente si es que necesita hospitalizarse en la clínica “D” y también para el personal médico que podrá atenderlo revisando la historia en línea y sin necesidad de esperar el trámite administrativo que actualmente se hace. Ver Anexo 8.

Con este storyboard obtuvimos retroalimentación de los pacientes y médicos para definir los requerimientos necesarios e iniciar con la construcción de nuestro

producto mínimo viable. Nos sirvió para identificar distintas variables y descomponer el problema de data que tiene el sector y así acotar nuestra solución a lo que se está planteando en este proyecto.

5.1 Perspectiva del prototipo

El prototipo que se propone consiste en configurar una red Blockchain que nos permita definir los participantes, el activo a transaccionar, los permisos por participante así como los eventos y transacciones a realizar en la Blockchain.

Se va a mostrar una propuesta de mockups de interfaces para el paciente (una secuencia de como el paciente podrá consultar su historial y como se va a mostrar la información), pero no se desarrollará ninguna lógica ni integración con la Blockchain por no ser el objetivo principal de este proyecto.

5.2 Características del producto mínimo viable

En este punto es importante resaltar la importancia de lograr un equilibrio entre lo que quiere el cliente y las características que debe tener el producto mínimo viable, para ello se va a adaptar una herramienta para que nos ayude a priorizar y como consecuencia a validar las características que se deben desarrollar para el PMV y validar nuestra idea con los potenciales clientes.

La matriz que vamos a utilizar será adaptada a 3 bloques, que son los siguientes:

- Debe tener: Los requisitos mínimos que debe tener la solución en función de lo que necesitan los clientes.
- Debería tener: Relacionado a las funcionalidades que debería desarrollar a continuación. Son funcionalidades que se cree que el usuario necesita. Para enumerarlas podría tener criterios de tiempo y cantidad de personas y aspectos económicos.
- Podría tener: En este bloque se coloca las funcionalidades que desea el cliente, pero por los recursos que se dispone en este momento, se podrían desarrollar en el mediano o largo plazo.

En todos los bloques se debe validar con los clientes. Ver Figura 5.1 para revisar los resultados obtenidos en cada bloque luego de realizar el análisis con los pacientes.

Figura 5.1

Características de lo que debe, debería y podría tener nuestro PVM

Debe tener...	Debería tener...	Podría tener...
<ul style="list-style-type: none"> - Confidencialidad - Seguridad - Disponibilidad de la historia clínica - Carga asíncrona de historias clínicas -Consultas de historias 	<ul style="list-style-type: none"> - Validación biométrica del paciente para permitir compartir información. - Sincronización de H.C cerca al tiempo real. - Ingresar a la red por medio de dispositivos móviles. 	<ul style="list-style-type: none"> - Identidad digital de pacientes y Médicos - Actualización en línea de signos vitales en conectividad con Apps. De salud. - Alertas de sugerencias de citas dependiendo de antecedentes de salud o de los datos recabados con las Apps de salud. - Registrar citas previa autorización del paciente.

Elaboración propia

5.3 Requerimientos

No se recopilamos ni consideramos los requerimientos funcionales debido a que no es parte del alcance de este proyecto. Solo se realizó un esbozo de las pantallas frontend con las cuales interactuará el paciente y se muestran en el Anexo 13

Así mismo para la demostración de la tecnología seleccionada nos enfocaremos en cubrir los siguientes requerimientos no funcionales.

Tabla 5.1

Requerimientos No Funcionales

ID	Tipo	Descripción
1	Disponibilidad	La herramienta de consulta debe estar disponible a todos los usuarios y podrá ser utilizado en cualquier momento que se requiera (24x7), sin importar horarios, se resalta que únicamente podrán acceder los usuarios que previamente se registraron. Se espera que sea 99.9% de disponibilidad
2	Desempeño	No importa la cantidad de usuario que inicien sesión, la herramienta será capaz de soportar hasta 5000 usuarios realizando consultas en línea al mismo tiempo.
3	Interoperabilidad	Los componentes del prototipo no funcional de consultas podrán interactuar con otros aplicativos mediante API que expondrá la plataforma.
4	Usabilidad	El prototipo será fácil de usar inclusive por personas sin experiencia en ambientes informáticos. Se espera que no tarde más de media hora en aprender a usar el sistema
5	Rendimiento	El tiempo de ejecución de transacciones, almacenar y recuperar la historia clínica será menor a 1 segundo.
6	Confiabilidad	Se realizarán pruebas para comprobar la veracidad de los datos obtenidos en las consultas de las historias clínicas. Estas pruebas se realizarán al momento de su implementación y tendrá como objetivo demostrar la calidad de la herramienta. Se espera un nivel de confianza del 95% de los datos obtenidos.

Elaboración Propia

5.4 Funcionalidad del prototipo

El prototipo tendrá la capacidad de crear participantes (Pacientes e Instituciones de salud), crear el activo que en nuestro caso es la Historia Clínica y simular transacciones para que el paciente permita el acceso a su información y luego revocar el permiso.

El prototipo fue desarrollado en Hyperledger Composer, sin embargo, por problemas ajenos a la implementación, en la actualidad la herramienta ha quedado en desuso, lo que no permite tener un soporte en caso de consultas como antes si se tenía. Por otro lado, las adecuaciones que se realizan, la herramienta muestra que son correctas sin embargo al momento de ejecutar las transacciones se visualizan alertas que no se pueden realizar seguimiento para resolverlos.

A continuación, se va a detallar el funcionamiento del prototipo el cual consiste en que la institución crea al paciente y la historia clínica del paciente, internamente la historia está asociada a la institución que la creó y al paciente. El identificador del paciente será su número de DNI. El identificador de la institución será el RUC y para la historia clínica se está dejando el Numero de historia clínica, sin embargo, esta forma

de trabajo en un futuro cercano cambiará dado que el identificador de la historia clínica del paciente será su número de DNI.

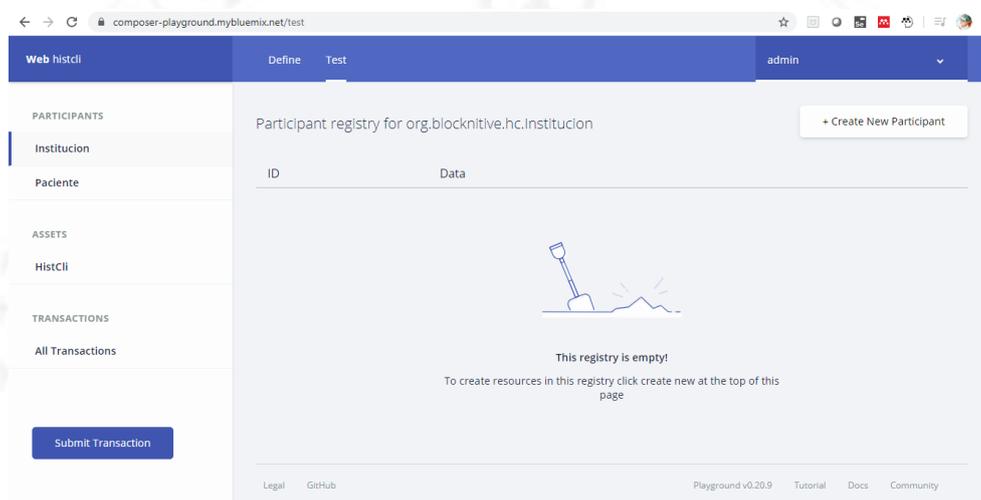
Cuando el paciente empiece a utilizar la blockchain, va a poder determinar a quién le da permiso para que vea su historia clínica y luego revocar el acceso, lo que permitirá un mayor control sobre su historial.

- Creación de Participantes:

Se muestra la Blockchain creada en blanco para los participantes así como las transacciones:

Figura 5.2

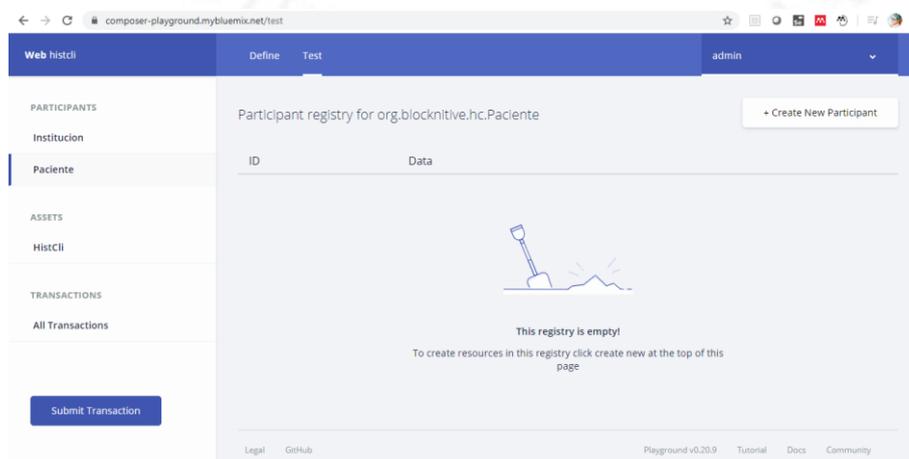
Participante - Instituciones



Fuente: Elaboración propia

Figura 5.3

Participante - Paciente

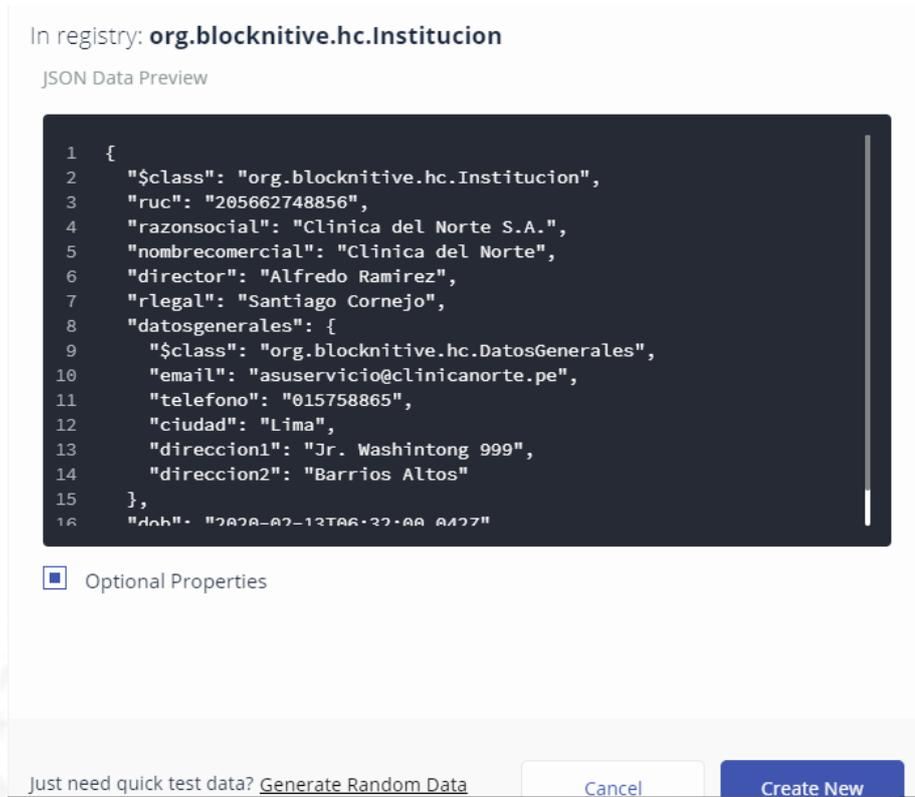


Fuente: Elaboración propia

Simularemos la creación de una Institución de salud

Figura 5.4

Crear Institución

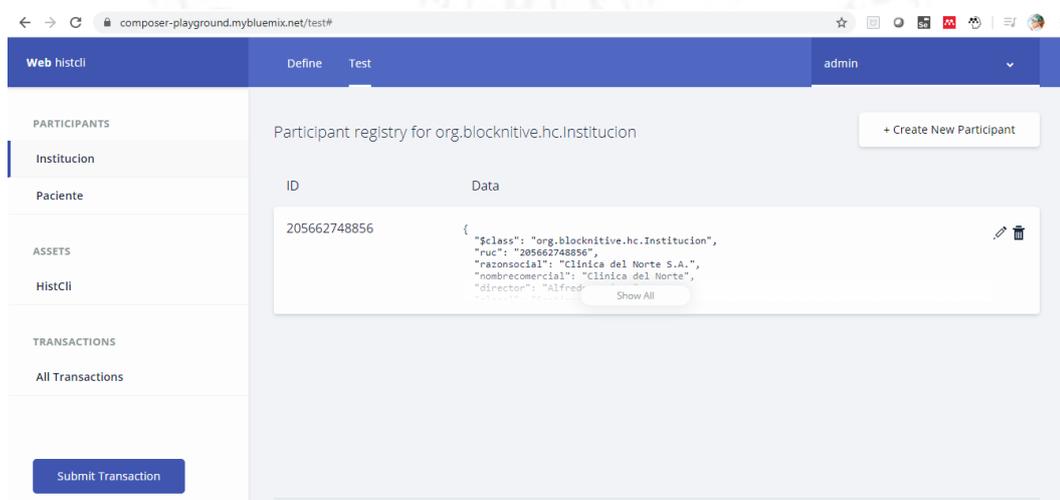


Fuente: Elaboración propia

Clic en Create New y se observa lo siguiente

Figura 5.5

Institución

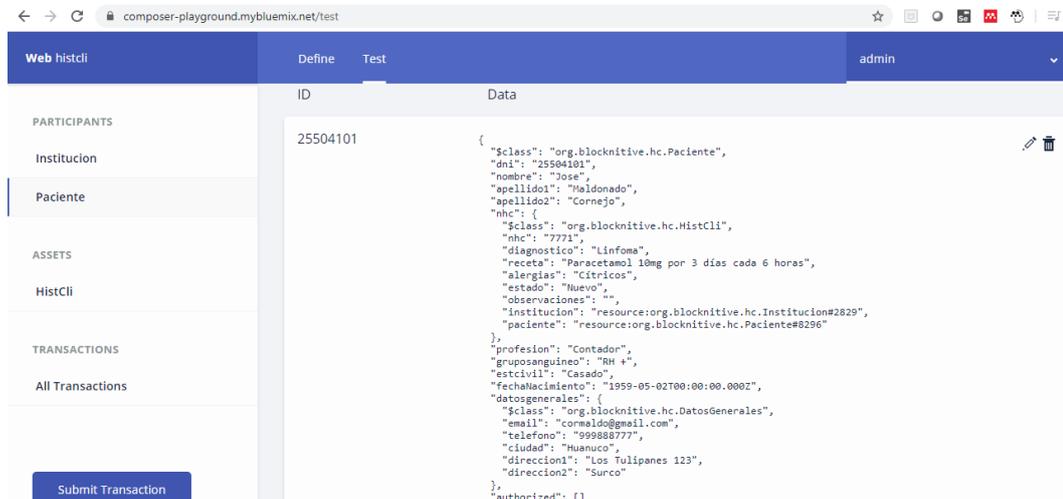


Fuente: Elaboración propia

Ahora creamos Paciente

Figura 5.6

Paciente



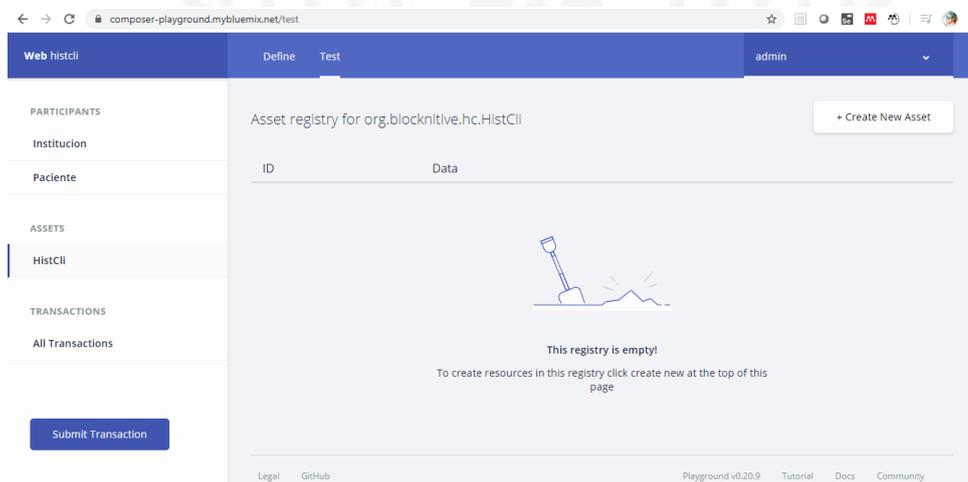
Fuente: Elaboración propia

- Creación de Activo

Inicialmente no se tiene ningún activo:

Figura 5.7

Activo - Historia Clínica



Fuente: Elaboración propia

Simularemos la creación del activo Historia Clínica

Figura 5.8

Crear Historia Clínica

In registry: **org.blocknitive.hc.HistCli**

JSON Data Preview

```
1 {
2   "$class": "org.blocknitive.hc.HistCli",
3   "nhc": "7771",
4   "diagnostico": "Linfoma",
5   "receta": "Paracetamol 10mg por 3 días cada 6 horas",
6   "alergias": "Cítricos",
7   "estado": "Nuevo",
8   "institucion": "resource:org.blocknitive.hc.Institucion#3612",
9   "paciente": "resource:org.blocknitive.hc.Paciente#2781"
10 }
```

Optional Properties

Just need quick test data? [Generate Random Data](#) Cancel Create New

Fuente: Elaboración propia

Asocio la institución y el paciente, la creación de la historia queda de la siguiente manera

Figura 5.9

Historia Clínica

ID	Data
7771	<pre>{ "\$class": "org.blocknitive.hc.HistCli", "nhc": "7771", "diagnostico": "Linfoma", "receta": "Paracetamol 10mg por 3 días cada 6 horas", "alergias": "Cítricos", "estado": "Nuevo", "institucion": "resource:org.blocknitive.hc.Institucion#205662748856", "paciente": "resource:org.blocknitive.hc.Paciente#25504101" }</pre>

Collapse

Fuente: Elaboración propia

- Autorizar acceso a la información del paciente

Para el Paciente 1 cuyo identificador es su correo electrónico (a modo de ejemplo se colocó el correo como id), va a autorizar para que la clínica Tesano pueda ver si información para ello primero va a observar si ya ha dado permiso a dicha clínica:

Figura 5.10

Estado Inicial de Paciente

ID	Data
Paciente@tesano.pe	<pre>{ "\$class": "org.acme.pii.Member", "email": "Paciente@tesano.pe", "firstName": "Mike", "lastName": "Ol", "dob": "2019-10-24T04:38:17.607Z", "address": { "\$class": "org.acme.pii.Address", "street": "Alameda Los Misioneros", "house": "564", "city": "Lima", "county": "Lima", "country": "Peru", "zip": "1" }, "authorized": [] }</pre>

Fuente: Elaboración propia

Como se observa en el campo authorized está en blanco. Invocamos la transacción para dar acceso a su información

Figura 5.11

Invoca transacción Autorizar

Submit Transaction

Transaction Type: **AuthorizeAccess**

JSON Data Preview

```
1 {
2   "$class": "org.acme.pii.AuthorizeAccess",
3   "memberId": "clini@tesano.pe"
4 }
```

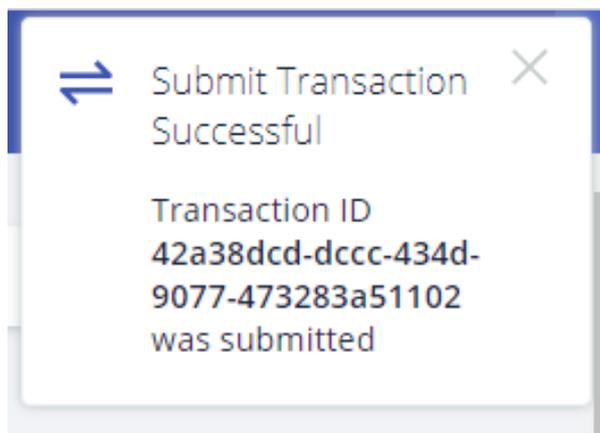
Optional Properties

Fuente: Elaboración propia

Al enviar la transacción, se muestra el siguiente mensaje:

Figura 5.12

Confirmación de transacción



Fuente: Elaboración propia

Ahora se visualiza que se ha autorizado a la clínica Tesano

Figura 5.13

Paciente autoriza clínica



Fuente: Elaboración propia

Al Ingresar a la clínica ahora visualiza los datos del paciente:

Figura 5.14

Clínica visualiza información del paciente

ID	Data
clini@tesano.pe	<pre>{ "\$class": "org.acme.pii.Member", "email": "clini@tesano.pe", "firstName": "Tesano", "lastName": "Clinica", "dob": "2019-10-24T..." }</pre> <p>Show All</p>
Paciente@tesano.pe	<pre>{ "\$class": "org.acme.pii.Member", "email": "Paciente@tesano.pe", "firstName": "Mike", "lastName": "Ol", "dob": "2019-10-24T04:38:17.607Z", "address": { "\$class": "org.acme.pii.Address", "street": "Alameda Los Misioneros", "house": "564", "city": "Lima", "country": "Lima", "country": "Peru", "zip": "1" }, "authorized": ["clini@tesano.pe"] }</pre>

Fuente: Elaboración propia

- Revocar acceso

Ahora vamos a revocar el acceso, para eso entramos a la sesión del paciente y ejecutamos el Smart contract:

Figura 5.15

Paciente revoca acceso

Submit Transaction

Transaction Type: RevokeAccess

JSON Data Preview

```
1 {
2   "$class": "org.acme.pii.RevokeAccess",
3   "memberId": "clini@tesano.pe"
4 }
```

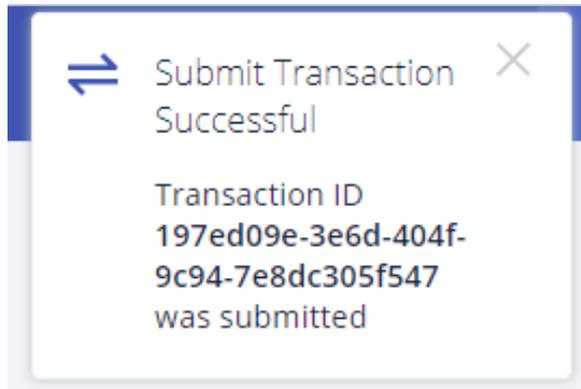
Optional Properties

Fuente: Elaboración propia

Aparece el mensaje de que se realizó la transacción y ahora se visualiza de esta forma el campo autorizado de paciente. Como se observa el paciente ya no está compartiendo su información:

Figura 5.16

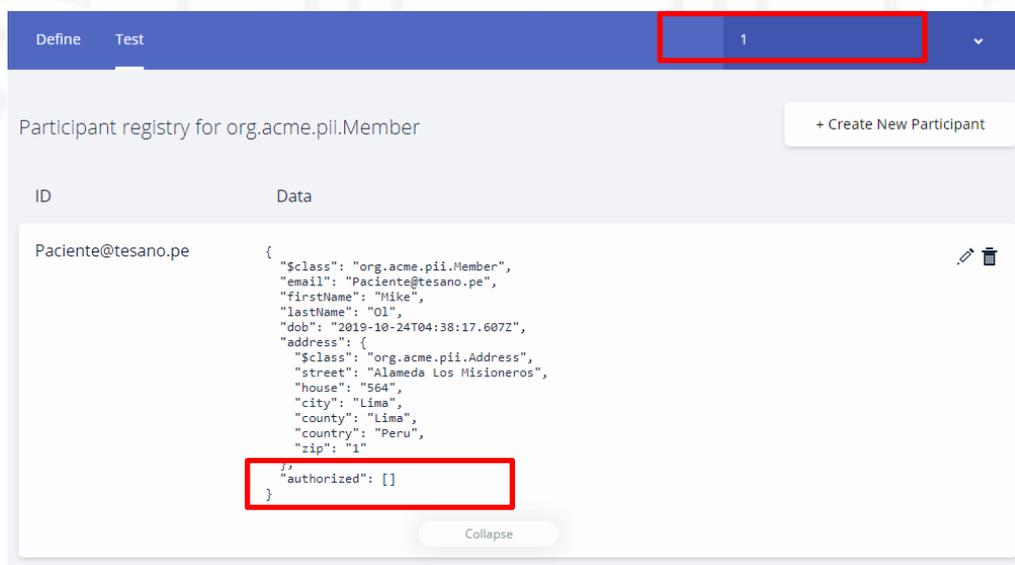
Confirmación de transacción de revocatoria



Fuente: Elaboración propia

Figura 5.17

Visualización del campo autorizado del paciente

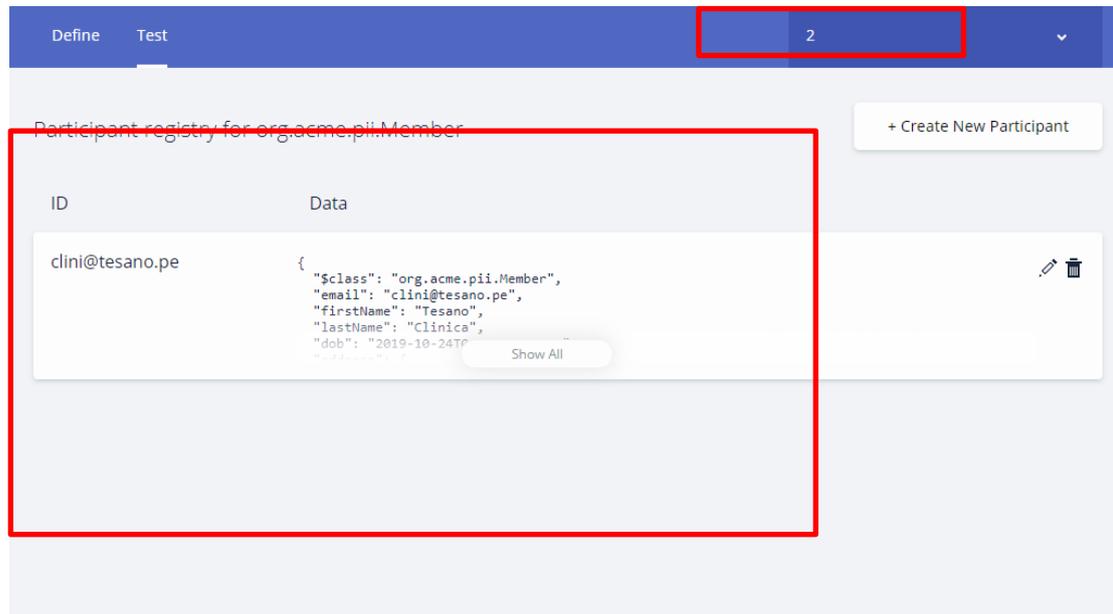


Fuente: Elaboración propia

Ahora vamos a volver a entrar al usuario de la clínica y ya no se ve los datos del paciente:

Figura 5.18

Clínica ya no visualiza información del paciente



Fuente: Elaboración propia

5.5 Diseño

- **Seguridad y control de acceso**

Hyperledger permite varios aspectos para cubrir el tema de privacidad de data, entre ellos destacamos los que se muestran en la siguiente tabla:

Tabla 5.2

Aspectos para cubrir la seguridad de información

Aspectos	Descripción
Segregar la red en canales	Cada canal representa un subconjunto de participantes que están autorizados para ver los datos de los chaincodes que se implementan en ese canal
Usar datos privados	Usar datos privados para mantener privado los datos del ledger de otras organizaciones sobre el mismo canal. Una recopilación de datos privados permite a un subconjunto definido de organizaciones en un canal la capacidad de respaldar, confirmar o consultar datos privados sin tener que crear un canal separado. Otros participantes en el canal reciben solo un hash de los datos. La aplicación cliente puede hacer hash o cifrar los datos antes de llamar al chaincode.
Aplicación cliente encripta la data	Si utiliza los datos hash, deberá proporcionar un medio para compartir los datos de origen. Si encripta los datos, deberá proporcionar un medio para compartir las claves de descifrado.
Restringir acceso a información a ciertos roles	Se puede restringir el acceso a datos a ciertos roles en la organización, incorporando el control de acceso en la lógica de chaincode.
Encriptar datos del Ledger	Los datos del Ledger que no están siendo usados (en reposo) se pueden cifrar a través del cifrado del sistema de archivos en el par (P2P), y los datos en tránsito se cifran a través de TLS.

Fuente: Elaboración propia

Por otro lado blockchain ofrece diferentes tipos de casos de uso respecto a la seguridad la cual se resume en la siguiente figura:

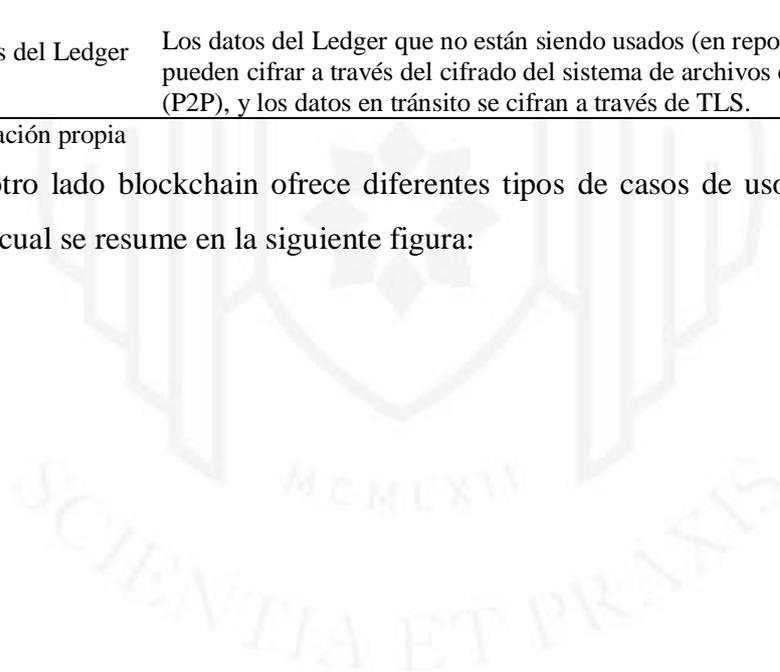


Figura 5.19

Seguridad Blockchain posibles casos



Fuente: Recuperado de <https://101blockchains.com/es/seguridad-blockchain/>, Seguridad Blockchain: Protección Premium para empresas (2019)

- **Marco Legal**

En el cumplimiento del marco legal, Para cumplir con la ley 29744 de protección de datos y normativas relacionadas con las aplicaciones digitales y economías colaborativas, pondremos los “disclaimers” correspondientes en los términos y condiciones que deberán aceptar los pacientes y prestadores de servicios médicos al momento de registrarse. Cada actualización de las normas deberá ser implementada, actualizadas e informadas oportunamente a todos los

involucrados, por lo que se notificará vía correo electrónico cualquier cambio en las políticas y términos y condiciones de uso.

Toda información que proporcione el Paciente y el prestador de servicios médico deberá ser de carácter privado y confidencial debiendo resguardar dicha información utilizando mecanismos de seguridad que garanticen el cumplimiento de las normas y leyes vigentes. Se deberá contar con el almacenamiento de documentos en formato electrónico en medios digitales siguiendo las reglas y procedimientos establecidos de ley.

- **Tecnología: Contenedores para agilizar el despliegue**

La característica principal de los contenedores es poder empaquetar una aplicación con todas las partes que necesita, como bibliotecas, archivos de configuración y otras dependencias. Esto permite tener la seguridad y garantía de que la aplicación se ejecutará en cualquier otro ambiente (máquina física o virtual) de manera exitosa. Esta tecnología difiere de las máquinas virtuales debido a que la imagen del “contenedor” es mucho más ligera al no cargar con el sistema operativo y la interfaz gráfica.

La tecnología más utilizada en este medio es “Docker”, cuenta con el soporte de la comunidad y cuenta con un gran número de imágenes disponibles, listas para ser utilizadas sin mucho esfuerzo.

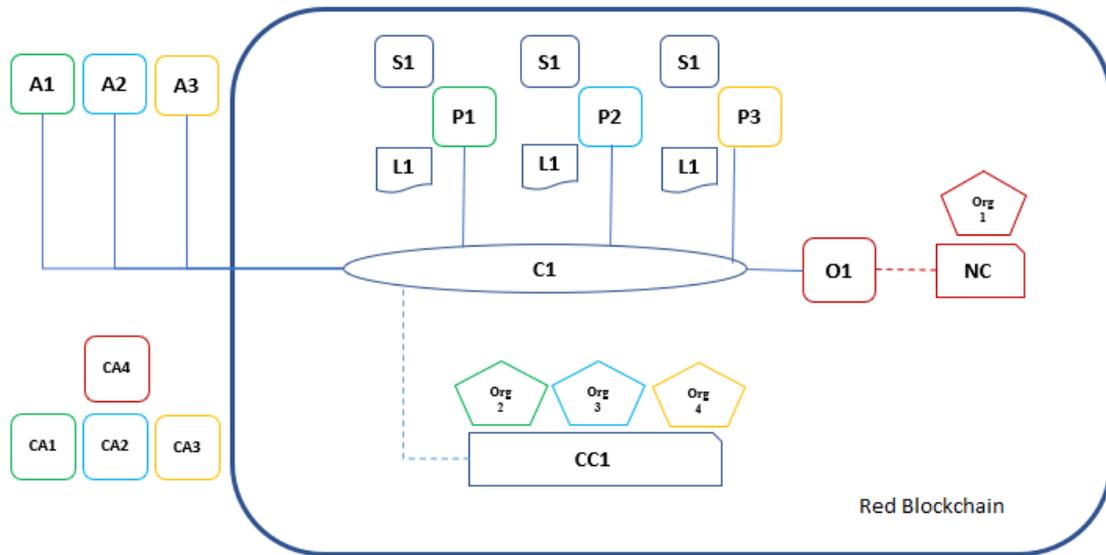
Esta tecnología facilita la creación, implementación y ejecución de aplicaciones, por lo que consideramos imprescindible adoptarla como parte del desarrollo del PMV.

- **Diagrama de Arquitectura**

La arquitectura definida para la implementación de la solución es la siguiente:

Figura 5.20

Diagrama de Arquitectura



Fuente: Elaboración propia

El diagrama de arquitectura representa lo siguiente:

Cuatro organizaciones, Org1, Org2, Org3 y Org4 han decidido en conjunto que establecerán y explotarán una red Hyperledger Fabric. Org1 ha sido asignado para ser el iniciador de la red; se le ha dado el poder de configurar la versión inicial de la red. Org1 no tiene intención de realizar transacciones en la red. Org2, Org3 y Org4 necesitan comunicaciones privadas dentro de la red general. Las organizaciones Org2, Org3 y Org4 tienen una aplicación cliente (respectivamente) que puede realizar transacciones dentro del canal C1.

Los nodos pares P1, P2 y P3 mantienen una copia del libro mayor L1 asociado con C1. La red se rige de acuerdo con la política de reglas especificadas en la configuración de red (NC), la red está bajo el control de las organizaciones Org2, Org3 y Org4. El canal C1 se rige de acuerdo con las políticas especificadas en la configuración del canal CC1. Hay un servicio de Ordenamiento O1 que sirve como un punto de administración de red y usa el canal del sistema. El servicio de ordenación también es compatible con el canal de aplicación C1, con el fin de ordenar transacciones en bloques para su distribución. Cada una de las cuatro organizaciones tiene una Autoridad de certificación Preferida (CA1, CA2, CA3, CA4).

Tabla 5.3

Componentes de la Arquitectura

Componente	Descripción
Org 1, 2,3,4	Representan las Organizaciones en la Blockchain
NC	Network Configuration, son las políticas de reglas con las que se rige la red
O1	Servicio de Ordenación, sirve como punto de administración de la red. Este servicio es compatible con el canal de aplicación, el fin es ordenar transacciones en bloques para su distribución.
CC1	Configuración del canal, son políticas especificadas en la configuración del canal. El canal está bajo el control de las organizaciones 2,3,4
P1,P2,P3	Nodos P2P o Iguales
L1	Es la copia del Ledger en cada nodo
S1	Es el SmartContract en cada nodo
CA1, CA2, CA3, CA4	Entidad emisora de certificados de cada organización
A1, A2, A3	Aplicaciones que se interconectan con la Blockchain

Elaboración propia

5.6 Implementación

En esta sección, mostraremos como se realizará el control de acceso a la información de la HC mediante el uso de Blockchain.

Primero enumeramos las siguientes entidades que participan en el proceso.

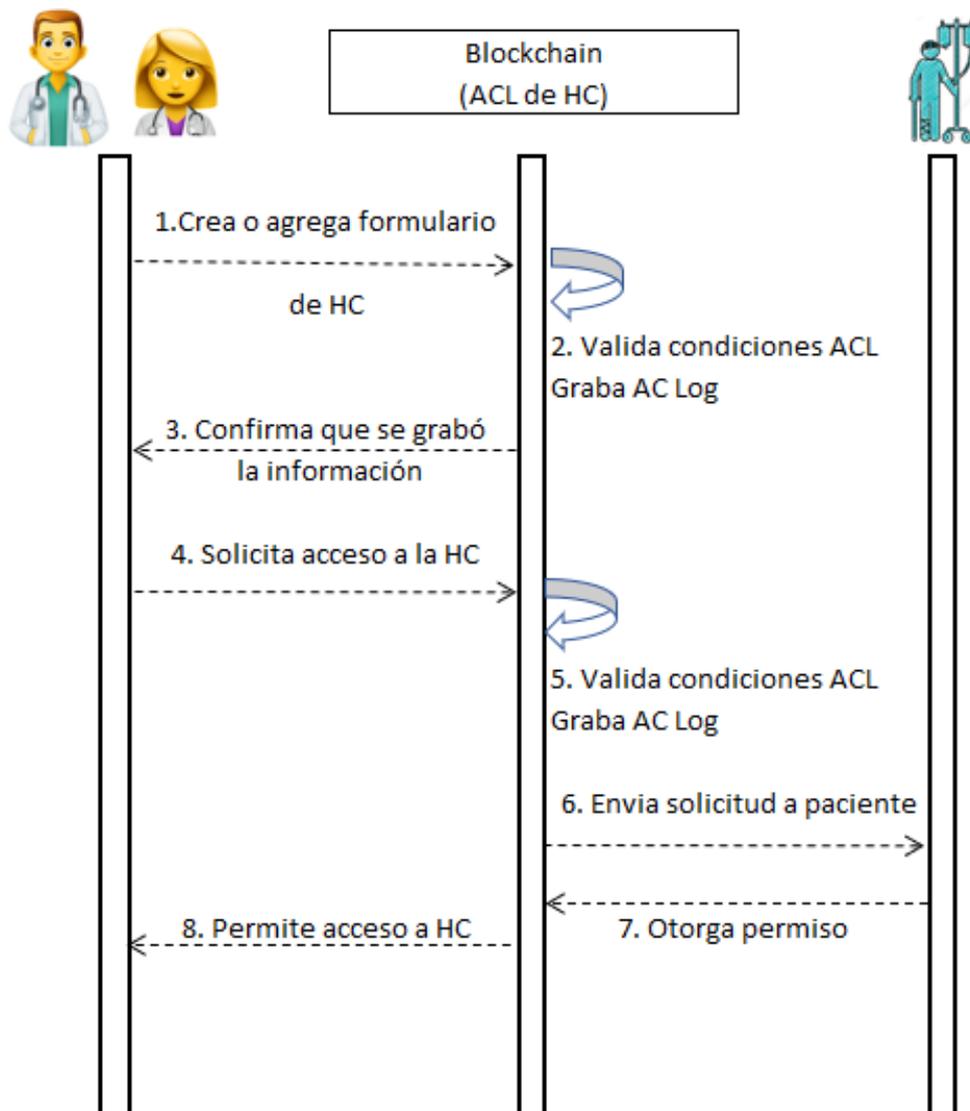
- **Paciente:** un paciente es una entidad del cual se obtiene la información que será almacenada en la historia clínica a la que se debe acceder. Un paciente puede especificar las políticas de acceso para los datos a su HC.
- **Proveedor de atención médica:** un proveedor de atención médica (por ejemplo, Institución, médico o enfermera) es una entidad que necesita acceder a los datos de la HC que pertenecen a los pacientes. Un proveedor de atención médica busca activamente autorizaciones de acceso de los pacientes.
- **Datos de HC:** los datos de la HC es la información que pertenece a un paciente y los proveedores de atención médica autorizados pueden acceder a ellos.
- **Blockchain:** Blockchain se utiliza como el controlador de la arquitectura que administra las políticas de control de acceso y sirve como un registro de acceso a prueba de manipulaciones.

El flujo de trabajo de control de acceso en la Blockchain se representa como en la Figura 5.20. Primero, los proveedores de atención médica crean o agregan

formularios en la HC del paciente. El nodo validador aprueba la transacción y la da por válida, el bloque se agrega a la cadena. En segundo lugar, la institución de salud (Médico o enfermera) pueden enviar la solicitud de acceso a través de un contrato inteligente que verificará la información de identidad con la política de ACL. Si se cumple la condición, se le solicita al paciente que apruebe el acceso, el paciente aprueba el acceso y el contrato inteligente devolverá la información de la HC del paciente consultado. Finalmente, la institución de salud accede a los datos de la HC.

Figura 5.21

Flujo de control de acceso en Blockchain



Elaboración Propia

En el resto de esta sección, primero ilustramos la red Blockchain de Hyperledger Composer Fabric y describimos el diseño de la política de ACL para nuestro PMV.

Para implementar y evaluar el mecanismo de control de acceso, diseñamos y desarrollamos en Hyperledger Composer Fabric, que es una aplicación basada en web.

Como se muestra en la Figura 5.21, la infraestructura de Hyperledger Composer Fabric contiene cuatro partes programables. La primera parte es definir las características de la red en un archivo de modelo (.cto), que incluye:

- Participantes: Paciente, Institución de Salud
- Activo: Estamos definiendo la Historia clínica como activo
- Transacciones: Actualizar Historias clínicas, Autorizar acceso a Historia y revocar acceso a Historia.
- Eventos: Creamos un evento al actualizar la historia clínica, al autoriza y al revocar acceso.

La segunda parte es escribir contratos inteligentes (chaincode como se les llama en Hyperledger) en el archivo de script (.js), que contiene funciones de procesamiento de transacciones. Se crearon los siguientes:

- Actualiza Historia:
- Autorizar acceso a la Historia Clínica
- Revocar acceso a la historia clínica

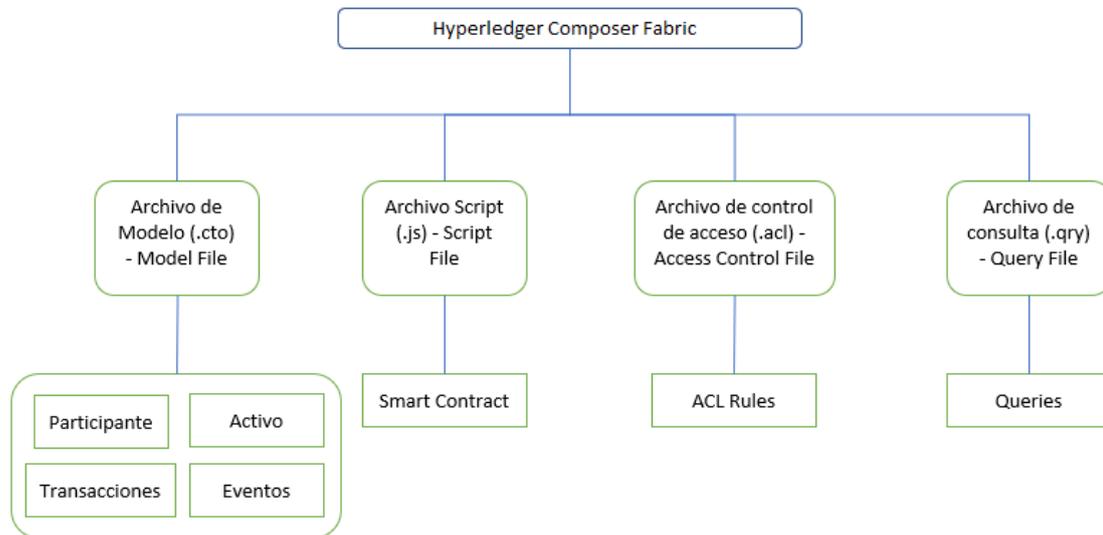
La tercera parte es definir las reglas de ACL para diferentes participantes en el archivo de control de acceso (.acl), para lo cual se han definido las siguientes reglas:

- Paciente ve su historia
- Institución de salud puede crear y actualizar historias
- Medico puede crear y actualizar historias
- Paciente autoriza acceso a la Historia Clínica
- Paciente revoca acceso a la historia clínica

Finalmente, las consultas de la base de datos se definen en el archivo de consulta (.qry).

Figura 5.22

Infraestructura de Hyperledger Composer Fabric



Fuente: Guo, Li, Nejad y Shen (2019)

Hyperledger Composer Fabric proporciona una plataforma de desarrollo para aplicaciones basadas en Blockchain, como las criptomonedas. En esta arquitectura, la red Blockchain todavía está limitada al caso de uso de criptomonedas. En nuestro sistema propuesto, los participantes representan a pacientes y médicos. La historia clínica de los pacientes se guarda como un activo personal en la red Blockchain. En otras palabras, el paciente y el activo HC tienen una relación de uno a uno, que se identifica por el ID del paciente autorizado por ACL, un médico puede recuperar la HC de sus pacientes, mientras que el paciente solo puede recuperar su propia HC.

La función de recuperación se define como el proceso de transacción en el contrato inteligente e invocada por los participantes que envían sus solicitudes.

Finalmente, todos los eventos de recuperación históricos se guardan como registro de control de acceso inmutable y rastreable en la red Blockchain.

Al definir las políticas de ACL, puede determinar qué usuarios pueden leer, escribir y actualizar el contenido. Cuando la política de ACL está disponible en la red Blockchain, los usuarios que consumen la información pueden enviar la solicitud de acceso al paciente para obtener la aprobación de acceso y recibir la información de la

HC almacenada. En el anexo 21 se muestra los scripts usados en la elaboración del PMV.



CONCLUSIONES

- Para este proyecto, proponemos una arquitectura en la que se impone el control de acceso a los datos de la Historia clínica (HC). La arquitectura utiliza Blockchain para ejecutar contratos inteligentes aprovechando la política Access Control List (ACL). Utilizamos la cadena de bloques Hyperledger Composer Fabric programada con contratos inteligentes y políticas de ACL para evaluar el rendimiento y la forma como trabaja. De acuerdo con los resultados con data de prueba, este sistema podría incorporarse en marcos de control de acceso a datos seguros y en tiempo real.
- El prototipo nos ayuda a realizar pruebas de concepto y nos demuestra cómo los principios de descentralización y arquitecturas Blockchain podrían contribuir a sistemas seguros e interoperables. Este nuevo enfoque demuestra que la integración con sistemas existentes de proveedores de salud es posible, para ello se debe trabajar en preparar la Blockchain proporcionando APIs para la interconexión con otros sistemas.
- De acuerdo con la literatura revisada, en los Blockchain permissioned el riesgo de ataque sobre los contratos inteligentes es menor debido a que el acceso al código es restringido a los participantes admitidos en la Blockchain. Sin embargo, se debe contemplar el riesgo dado que algún nodo legítimo puede verse comprometido debido a un fallo en la implementación que permita a un nodo atacante formar parte del sistema. La vulnerabilidad en los contratos inteligentes es que una vez introducido en la cadena no es posible eliminarlo o modificarlo, por lo que los mecanismos para solucionar los efectos de un posible ataque son limitados, y se podría dar el caso de que la única forma de parar un ataque contra un contrato inteligente sea detener el Blockchain y esto debido a que no se tienen muchas Blockchain implementadas y puestas en producción que nos permita estimar el riesgo y tener alternativas de solución, por lo tanto este es un punto importante a considerar al momento de diseñar la solución.
- Uno de los retos de las Blockchain, está relacionada con la confidencialidad de la información que incluso también se presenta en Blockchain permissioned ya que no necesariamente se quiere o se puede compartir toda la información con todos los

nodos de la red. En nuestro caso, que manejaremos datos de carácter personal, según la legislación actual, obliga a cumplir una serie de requisitos para el almacenamiento y tratamiento de la información y la forma como trabaja Blockchain aún no está contemplada en la norma dado que manejan registros compartidos por varias entidades. Por tal motivo distintas plataformas que manejan Blockchain permissioned, implementan mecanismos que permitan mantener las ventajas del uso de registros distribuidos, pero con cierto nivel de confidencialidad y una de estas plataformas es Hyperledger.

- Es importante considerar al responsable de mantener el código, el cual se actualiza con frecuencia, para la implementación de un proyecto con Blockchain. Esto debido a que en el mundo Blockchain predomina el software mantenido por comunidades de desarrolladores, lo cual es ventajoso, pero también trae inconvenientes, por ejemplo, la dificultad a la hora de acordar los tiempos de respuesta para corregir los incidentes que se presenten en el ambiente productivo.
- La falta de madurez de la tecnología, que está orientada a la seguridad y eliminación de intermediarios, es una de las consideraciones técnicas que dificultan la adopción de este tipo de soluciones en un entorno productivo. Asimismo, la capacidad de almacenamiento es limitada, debido a la cantidad de información almacenada en la Blockchain, por esa razón es necesario mantener sistemas externos para almacenar información lo que conlleva a elevar los costos en la implementación.
- Un punto para resaltar es que, durante la ejecución del proyecto, nos topamos con la dificultad de no contar con técnicos especializados a nivel local. Al tratarse de una tecnología reciente, no resulta fácil encontrar especialistas en Blockchain para desarrollar proyectos a gran escala y en general se trata de perfiles caros dado que tendríamos que contratar en el extranjero.
- En cuestiones organizativas, la adopción de esta tecnología implica que las organizaciones cambien la forma de relacionarse con otras e internamente cambien procesos de negocio. Esta transformación requiere el soporte a nivel directivo y sobre todo necesita tiempo para implementarla.
- Por lo expuesto líneas arriba, todos estos puntos deben contemplarse a la hora de decidir por la implementación de un proyecto con tecnología Blockchain, para ello es necesario conocer las características de esta tecnología al realizar el análisis de

riesgo. Sin embargo, ninguno de estos riesgos es suficiente para bloquear la adopción de esta tecnología. Considero que esta tecnología no es una moda y probablemente en los siguientes años experimente una evolución importante, en este momento es difícil saber el camino que tomará esta tecnología.

- Respecto a Blockchain permissioned, esta tecnología es muy reciente y aún está en proceso de dar el salto de pruebas de concepto a una puesta en producción.



RECOMENDACIONES

- Para futuros proyectos podrían integrarla con Internet of things (IoT) y asociar los dispositivos como pulseras inteligentes que permitirá recolectar información y almacenarla para una posterior refrendación de un especialista de salud; diagnosticar en base a algunos signos vitales y programar una cita, o si es que ya cumpliste la cantidad de azúcar, bloquear la apertura del refrigerador hasta el día siguiente a determinada hora, entre otras bondades que nos permite la tecnología. Todo esto será posible pero primero se deben sentar las bases e ir mostrando avances que permitan creer en la plataforma.
- Así mismo, se podría integrar machine learning para identificar los tratamientos que esté realizando el paciente y pueda mostrarle opciones de interés como por ejemplo tipo de alimentación para un paciente de diabetes o en caso una persona este siguiendo un tratamiento por obesidad, indicarles que alimentos y en qué horas debe consumirlos, entre otras utilidades.
- Se plantea investigar los nuevos protocolos de consenso diseñados para el mecanismo propuesto o alguno relacionado al sector salud para lograr un mejor rendimiento de la red.

GLOSARIO DE TÉRMINOS

ACL: Lista de control de Accesos

CA: Abreviatura de "entidad emisora de certificados"; es el componente que emite certificados a todos los miembros participantes. Estos certificados representan la identidad de un miembro. Todas las entidades de la red (iguales, nodos de ordenación, clientes, etc.) deben tener una identidad para comunicarse, autenticarse y, finalmente, realizar transacciones. Estas identidades son necesarias para cualquier participación directa en la red Blockchain.

eHC: Historia Clínica electrónica

HC: Historia Clínica, Es el documento médico legal, que registra los datos, de identificación y de los procesos relacionados con la atención del paciente, en forma ordenada, integrada, secuencial e inmediata de la atención que el médico u otros profesionales brindan al paciente.

HIS: Son sistemas de información hospitalaria (HIS por sus siglas en inglés), que permite una gestión integrada de todos los factores que inciden en el sistema sanitario.

Igual: Recurso de la red Blockchain que proporciona los servicios para ejecutar y validar transacciones y para mantener libros mayores. El igual ejecuta código de encadenamiento y es el titular del historial de transacciones y del estado actual de los activos en los canales de la red, es decir, del libro mayor. Los iguales son propiedad de las organizaciones, que los gestionan, y se unen a canales.

LIS: Sistemas de información de Laboratorio

MINSA: Ministerio de Salud

Nodo de Ordenación: El nodo que recopila transacciones de los miembros de la red, ordena las transacciones y las empaqueta en bloques. También se conoce como clasificador. A continuación, se distribuyen estos bloques a los iguales, que verificarán luego los bloques y los añadirán a los libros mayores de cada canal. Los nodos de ordenación contienen el material de identidad de cifrado que está vinculado a cada miembro y autentican la identidad de clientes e iguales para que puedan acceder a la

red. La función global que proporciona un nodo o una recopilación de nodos clasificadores se conoce como servicio de ordenación.

PVM: Producto Mínimo Viable o MVP (Minimum Viable Product por sus siglas en inglés)

RENHICE: Registro Nacional de Historias Clínicas Electrónicas

RIS: Sistemas de información de Radiología



REFERENCIAS

- ¿Cómo es el consumidor digital peruano? (30 de Octubre de 2019). Recuperado de <https://www.peru-retail.com/onsumidor-digital-peruano/>
- ¿En qué consiste la metodología Lean Startup? (07 de marzo de 2016). [mensaje en un blog]. Recuperado de <https://www.antevenio.com/blog/2016/03/en-que-consiste-la-metodologia-lean-startup/>
- Pagos con tarjetas: ¿Qué comisiones pagan los negocios que usan POS? (16 de febrero de 2018). *Gestión*. Recuperado de <https://gestion.pe/economia/empresas/pagos-tarjetas-comisiones-pagan-negocios-pos-227409-noticia/?ref=gesr>
- ¿Qué es el Design Thinking y cómo aplicarlo en el trabajo? (02 de diciembre de 2018). *Gestión*. Recuperado de <https://gestion.pe/economia/management-empleo/design-thinking-aplicar-metodo-innovar-empresas-nnda-nnlt-250663>
- Smart contracts, ¿Qué son, cómo funcionan y qué aportan? (s.f.). Recuperado de <https://academy.bit2me.com/que-son-los-smart-contracts/>
- Arellano, R. (27 de agosto de 2018). La pollada y el wawahuasi, por Rolando Arellano. *El Comercio*. Recuperado de <https://elcomercio.pe/opinion/rincon-del-autor/pollada-wawahuasi-rolando-arellano-noticia-550905>
- Arroyo Guardado, D., Díaz Vico, J., y Hernandez Encinas, L. (2019). *¿Qué sabemos de? Blockchain*. Recuperado de <https://books.google.com.pe/books?id=UduVDwAAQBAJ&printsec=frontcover&dq=BLOCKCHAIN&hl=es&sa=X&ved=0ahUKEwjtrGmz-fiAhUJjVkkHUtjAJsQ6AEINDAC#v=onepage&q=BLOCKCHAIN&f=false>
- Belatrix. (2019). Blockchain en acción: casos de uso disruptivos clave para el 2019. Recuperado de https://cdn2.hubspot.net/hubfs/5078049/Media_files/Whitepaper_Blockchain_accion_casos_uso_disruptivos_clave_2019.pdf?utm_source=hs_automation&utm_medium=email&utm_content=69200810&_hsenc=p2ANqtz--Cidd64SR-3qQtSTDucVhETK8D5QoP_QQCesg5mm6NIi17Wbp_MvIBO-1uzu

- Bentov, I., Lee, C., Mizrahi, A. y Rosenfeld, M., 2014. Proof of activity: extending bitcoin's proof of work via proof of stake [extended abstract] y. *ACM SIGMETRICS Performance Evaluation Review*, 42(3), 34–37. doi: 10.1145/2695533.2695545
- Buterin, V. (12 de abril de 2015). Visions, Part 1: The Value of Blockchain Technology [mensajes en un blog]. Recuperado de Ethereum Blog website: <https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/>
- Castro, M. y Liskov, B., 2002. Practical byzantine fault tolerance and proactive recovery. *ACM Trans. Comput. Syst.* 20(4), 398–461.
- Communications. (26 de abril de 2018). ¿Cuál es la diferencia entre una DLT y 'blockchain'?. Recuperado de <https://www.bbva.com/es/diferencia-dlt-blockchain/>
- Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., y Wang, J. (2018). Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Transactions on Knowledge and Data Engineering*, 30(7), 1366–1385. <https://doi.org/10.1109/TKDE.2017.2781227>
- Estadísticas de Seguridad Ciudadana (2019). Recuperado del sitio de internet del Instituto Nacional de Estadísticas e Informática: https://www.inei.gob.pe/media/MenuRecursivo/boletines/02-informe-tecnico-n02_estadisticas-seguridad-ciudadana_set2018-feb2019.pdf
- Guo, H., Li, W., Nejad, M., y Shen, C. C. (2019). *Access Control for Electronic Health Records with Hybrid Blockchain-Edge Architecture* (ArXiv: 1906.01188v1). Recuperado de <https://arxiv.org/pdf/1906.01188.pdf>
- Herrera, C. (03 de marzo de 2018). ¿Qué es Proof of Work y Proof of Stake? Recuperado de <https://www.tekcrispy.com/2018/03/03/proof-of-work-stake-pow-pos/>
- Hyperledger-Fabric Documentation. (20 de Junio de 2019). Recuperado de <https://buildmedia.readthedocs.org/media/pdf/hyperledger-fabric/latest/hyperledger-fabric.pdf>
- Iain, S. (15 de enero de 2018). Proof of burn. Recuperado de https://en.bitcoin.it/wiki/Proof_of_burn

- INCAE. (21 de mayo de 2018). Lean Canvas: un lienzo para emprendedores [mensaje en un blog]. Recuperado de <https://www.incae.edu/es/blog/2018/05/21/lean-canvas-un-lienzo-para-emprendedores.html>
- Kastelein, R. (09 de abril de 2016). Intel Jumps into Blockchain Technology Storm with ‘sawtooth Lake’ Distributed Ledger. Recuperado de <https://www.the-blockchain.com/2016/04/09/>
- Lamport, L., 1978. Time, clocks, and the ordering of events in a distributed system. *Communications of the ACM*, 21(7), 558–565. doi: 10.1145/359545.359563
- Linares-Barbero, M. (2018). Revisión de la capacidad de transparencia y confianza que ofrece la tecnología blockchain. *Interfases*, 11, 119–133. <https://doi.org/10.26439/interfases2018.n011.2957>
- Litecoin. (2011). Litecoin - Open source P2P digital currency. Recuperado de <https://litecoin.org/>
- Lukas, K. (03 de abril de 2018). In-depth on differences between public, private and permissioned blockchains - Medium. Recuperado de <https://medium.com/@lkolisko/in-depth-on-differences-between-public-private-and-permissioned-blockchains-aff762f0ca24>
- Makhdoom, I., Abolhasan, M., Abbas, H., y Ni, W. (2019). Blockchain’s adoption in IoT: The challenges, and a way forward. *Journal of Network and Computer Applications*, 125(2019), 251-279. <https://doi.org/10.1016/j.jnca.2018.10.019>
- Mitra, R. (Febrero de 2019). Prueba de trabajo vs Prueba de participación: Guía básica de minado. Recuperado de <https://blockgeeks.com/guides/es/prueba-de-trabajo-vs-prueba-de-participacion/>
- Nakamoto, S. (31 de octubre de 2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Recuperado de www.cryptovest.co.uk
- Pastor, J. (23 de setiembre de 2018). Qué es blockchain: la explicación definitiva para la tecnología más de moda. Recuperado de <https://www.xataka.com/especiales/que-es-blockchain-la-explicacion-definitiva-para-la-tecnologia-mas-de-moda>

- PUCP. (21 de agosto de 2017). *¿Qué es Design Thinking?-PUCP* [archivo de video]. Recuperado de <https://www.youtube.com/watch?v=O7dmix015rU>
- Raikwar, M., Gligoroski, D. y Krlevska, K. (2 de Setiembre de 2019). SoK of Use Cryptography in Blockchain. Recuperado de <https://eprint.iacr.org/2019/735.pdf>
- Ries, E. (2011). *El Método Lean Startup: Como crear empresas de éxito utilizando la innovación continua*. (8.a ed.). Nueva York: Crown Busines.
- Rodríguez G., M. (2017). *Análisis de tecnologías Bitcoin y Blockchain* (tesis de maestría). Universidad Autónoma de Barcelona, Barcelona, España
- Rojas Medina, Y. (2019). *Situaciones de las lesiones causadas por accidentes de transito en el Perú 2° Trimestre 2019*. Recuperado del sitio de internet del MINSA: <http://www.minsa.gob.pe>
- Rojas Mezarina, L., Cedamanos Medina, C.A. y Vargas Herrera, J. (2015). Registro Nacional De Historias Clínicas Electrónicas En Perú [Carta]. *Revista Peruana de medicina experimental y salud pública*, 32(2), 395–396. Recuperado de <https://rpmesp.ins.gob.pe/index.php/rpmesp/article/view/1639/1820>
- Schneider, F.B., 1990. Implementing fault-tolerant services using the state machine approach: a tutorial. *ACM Comput. Surv.* 22(4), 299–319.
- The World Bank Group. (12 de abril de 2018). Blockchain & Distributed Ledger Technology (DLT). Recuperado de <https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt>
- TiccJeGiga Segovia. (01 de abril de 2014). *¿Qué es el Design Thinking? #TicSg* [archivo de video]. Recuperado de <https://www.youtube.com/watch?v=7ZJHdwzfo7A>
- Tschorsch, F. y Scheuermann, B. (2016). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, 18(3), 2084-2123. DOI:10.1109/COMST.2016.2535718
- Vaughan, W. (15 de Junio de 2016). How do blockchain businesses make money? [comentario en un foro en línea]. Recuperado de <https://www.quora.com/How-do-blockchain-businesses-make-money>

Voshmgir, S. (Julio de 2019). Token Security: Cryptography – part 2 [mensaje en un blog]. Recuperado de <https://blockchainhub.net/blog/blog/cryptography-blockchain-bitcoin/>

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., y Wang, H. (2017). Blockchain Challenges and Opportunities: A Survey. Recuperado de <https://pdfs.semanticscholar.org/305e/dd92f237f8e0c583a809504dcec7e204d632.pdf>



BIBLIOGRAFÍA

- Bittrich, C. (10 de agosto de 2017). Blockchain Construyendo confianza, demoliendo barreras. Recuperado de <http://repositorio.pucp.edu.pe/index/bitstream/handle/123456789/71316/309>
Carlos Bittrich - Blockchain. Construyendo confianza%2C demoliendo barreras %28A203 10.08.2017 12.00%29.pdf?sequence=1&isAllowed=y
- Casino, F., Dasaklis, T. K. y Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, 55-81. <https://doi.org/10.1016/j.tele.2018.11.006>
- Dannen, C. (2017). Introducing Ethereum and Solidity Foundations of Cryptocurrency and Blockchain Programming for Beginners. doi:10.1007/978-1-4842-2535-6
- Davies, A. (s.f.). How Much Does It Cost to Build a Blockchain Project? [mensaje en un blog]. Recuperado de <https://www.devteam.space/blog/how-much-does-it-cost-to-build-a-blockchain-project/>
- Dhar Dwivedi, A., Malina, L., Dzurenda, P. y Srivastava, G. (2019). Optimized Blockchain Model for Internet of Things based Healthcare Applications (arXiv:1906.06517v1). Recuperado del sitio de internet de arXiv: <https://arxiv.org/pdf/1906.06517.pdf>
- Ekblaw, A., Azaria, A., Halamka, J. y Lippman, A. (Agosto de 2016). A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data. Recuperado de https://pdfs.semanticscholar.org/56e6/5b469cad2f3ebd560b3a10e7346780f4ab0a.pdf?_ga=2.198858927.1611694562.1568177415-987984368.1568177415
- EY. (Abril de 2019). Total cost of ownership for blockchain solutions. Recuperado de [https://www.ey.com/Publication/vwLUAssets/ey-total-cost-of-ownership-for-blockchain-solutions/\\$File/ey-total-cost-of-ownership-for-blockchain-solutions.pdf](https://www.ey.com/Publication/vwLUAssets/ey-total-cost-of-ownership-for-blockchain-solutions/$File/ey-total-cost-of-ownership-for-blockchain-solutions.pdf)
- Hernández Blázquez, J. (2017). *Aplicando Lean Canvas para la generación del modelo de negocio de un producto innovador* (tesis de maestría). Universidad Carlos III de

Madrid. Madrid. España

HISMINSA. (2014). *Registro y codificación de la atención en la consulta externa* (Oficina General de Estadística e Informática). Recuperado de:
http://www.diresatumbes.gob.pe/phocadownload/Manuales_HIS_2016/Manual_General_HIS.pdf

HISMINSA. (2016). *Registro y codificación de diagnósticos de consulta externa y otras actividades de salud* (Oficina General de Estadística e Informática).
Recuperado de:
https://www.academia.edu/12530696/DOCUMENTO_T%C3%89CNICO_REGISTRO_Y_CODIFICACION_DE_DIAGNOSTICOS_DE_CONSULTA_EXTERNA_Y_OTRAS_ACTIVIDADES_DE_SALUD_Health_Information_System_-HIS_en_peru

HISMINSA. (2017). *Guía de uso y registro de la hoja HIS* (Oficina General de Tecnologías de la Información). Recuperado del sitio de internet del Ministerio de Salud:
http://www.diresatumbes.gob.pe/phocadownload/Manuales_HIS_2016/Guia%20de%20registro%20HIS.pdf

IBM Blockchain Platform. (18 de junio de 2019). Precios. Recuperado de
<https://cloud.ibm.com/docs/services/blockchain?topic=blockchain-ibp-pricing&locale=es>

Instituto Nacional de Estadística e Informática-INEI.(2019). *Condiciones de vida en el Perú* (Trimestre: Enero-Febrero-Marzo 2019). Recuperado del sitio de internet del INEI:
https://www.inei.gob.pe/media/MenuRecursivo/boletines/informe_condiciones_vida_enero-marzo2019.pdf

Instituto Nacional de Estadística e Informática-INEI.(2019). *Situación del Mercado Laboral en Lima Metropolitana* (Trimestre móvil: Febrero-Marzo-Abril 2019). Recuperado del sitio de internet del INEI:
<https://www.inei.gob.pe/media/MenuRecursivo/boletines/informe-tecnico-de-empleo-lima-metropolitana-feb-mar-abr2019.pdf>

Leonardos, S., Reijsbergen, D. y Piliouras, G. (2019). *PREStO: A Systematic*

- Framework for Blockchain Consensus Protocols* (arXiv:1906.06540v1).
Recuperado del sitio de internet de arXiv: <https://arxiv.org/pdf/1906.06540.pdf>
- Ley N° 26842, Ley General de Salud. (09 de julio de 1997). Recuperado del sitio de internet de Essalud:
<http://www.essalud.gob.pe/transparencia/pdf/publicacion/ley26842.pdf>
- Maheshwari, S. (14 de diciembre de 2018). Aspectos básicos de blockchain: Hyperledger Fabric e Hyperledger Composer ¿Cuál es la diferencia?. Recuperado de <https://www.ibm.com/developerworks/ssa/library/cl-blockchain-hyperledger-fabric-hyperledger-composer-compared/cl-blockchain-hyperledger-fabric-hyperledger-composer-compared-pdf.pdf>
- Meléndez Cuauro, R. (08 de abril de 2016). Sistema de Información Hospitalario (SIH). Recuperado de <https://www.slideshare.net/melendezcuauro/sistemas-de-informacin-hospitalaria-sih-exposicin>
- MINSA. (2013). *Indicadores de gestión y evaluación hospitalaria para hospitales, institutos y DIRESA* (Oficina General de Estadística e Informática). Recuperado de: <http://bvs.minsa.gob.pe/local/MINSA/2739.pdf>
- Novo, O. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet of Things Journal*. 5(2). 1184-1195.
doi:10.1109/JIOT.2018.2812239
- Precios de IBM Blockchain Platform for IBM Cloud. (s.f.). Recuperado de <https://cloud.ibm.com/docs/services/blockchain?topic=blockchain-ibp-saas-pricing&locale=es>
- Preukschat, A. (2017). *Blockchain: la revolución industrial de internet* [versión PDF]. Recuperado de <https://books.google.com.pe/books?id=Lb7DDgAAQBAJ&pg=PP21&dq=BLOCKCHAIN&hl=es&sa=X&ved=0ahUKEwjbrGmz-fiAhUJjVkJHUtjAJsQ6AEITDAG#v=onepage&q=BLOCKCHAIN&f=false>
- Ríos, M. (28 de setiembre de 2018). ¿Por qué la rotación laboral de los millennials es buena?, según Mercer. *Gestión*. Recuperado de <https://gestion.pe/economia/management-empleo/rotacion-laboral-millennials-buena-mercero-245533>

Simply Explained - Savjee. (18 de julio de 2017). *Creando una cadena de bloques con Javascript (Blockchain, parte 1)* [archivo de video]. Recuperado de <https://www.youtube.com/watch?v=zVqczFZr124>

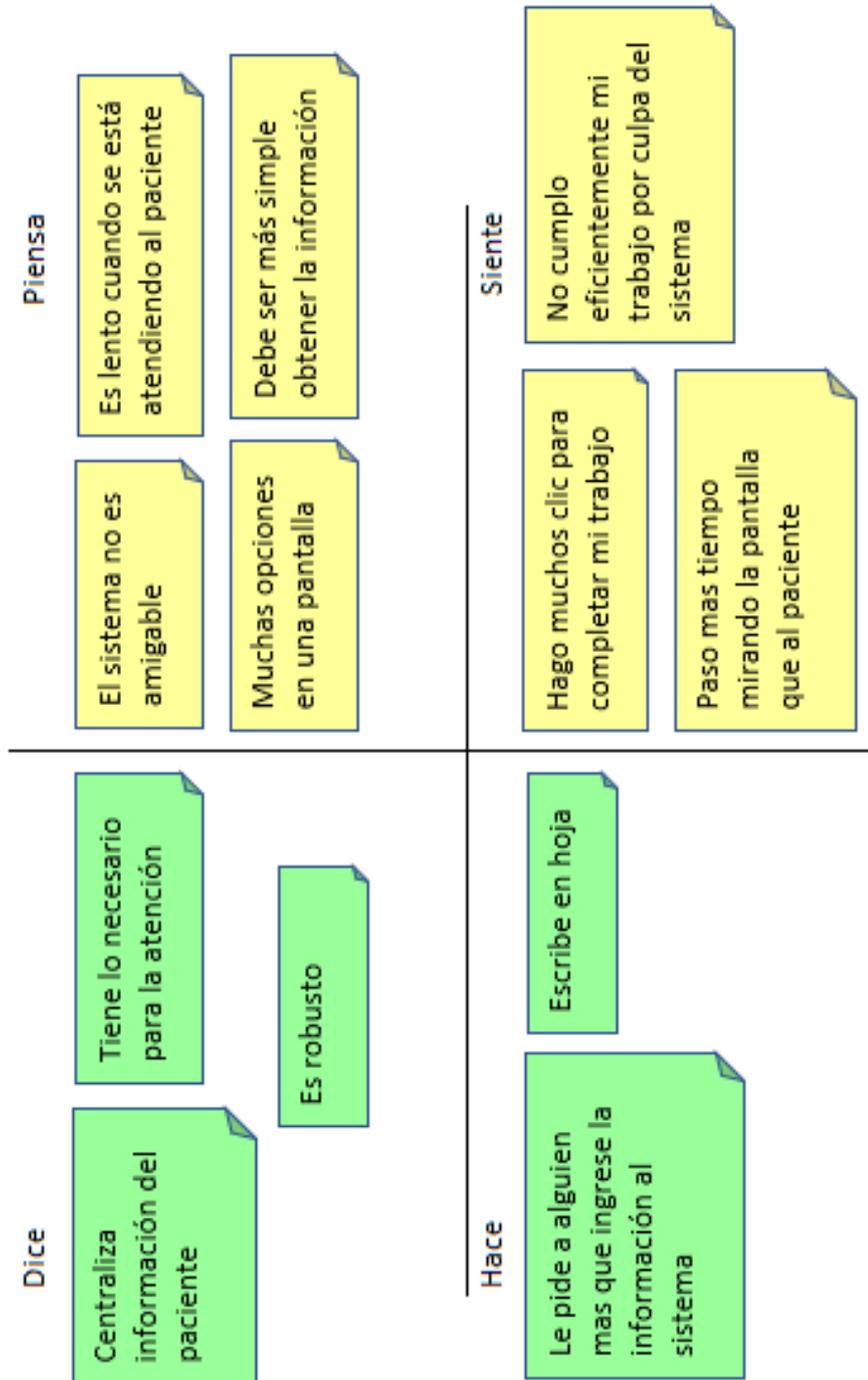
Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., y Wang, F.-Y. (2019). Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 1–12. <https://doi.org/10.1109/tsmc.2019.2895123>



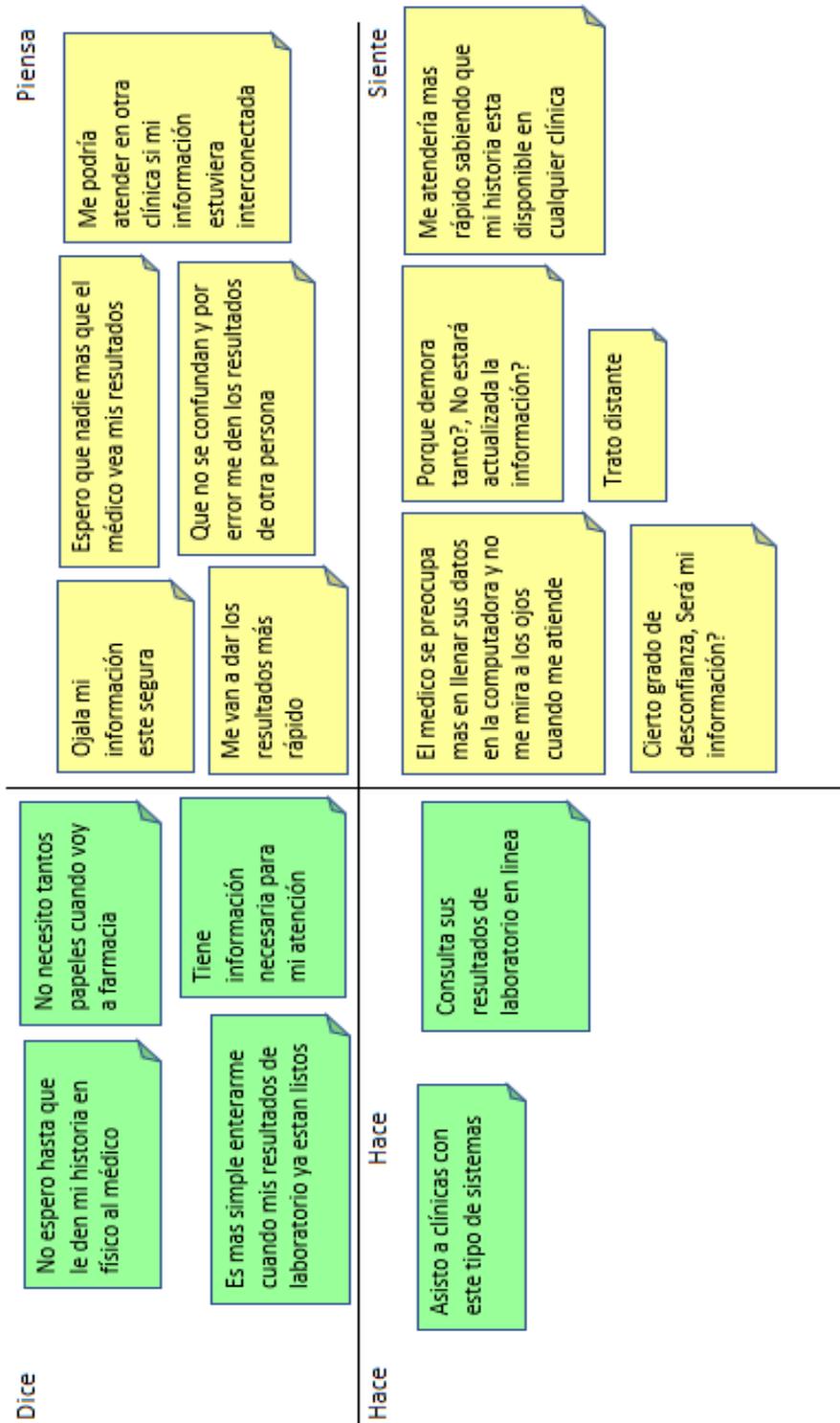


ANEXOS

Anexo 1: Mapa de Empatía Doctores - Impresión de sistemas de información hospitalario



Anexo 2: Mapa de Empatía-Paciente y su impresión de sistemas hospitalarios



Anexo 3: Identificando usuarios extremos



- Extreme

- Médicos con basta experiencia, Eminencias y que hacen poco uso de la tecnología, prefieren la atención mediante conversación y escribir a estar haciendo "Clic" en el sistema.
- Pacientes mayores de 55 años

Most people

+ Extreme

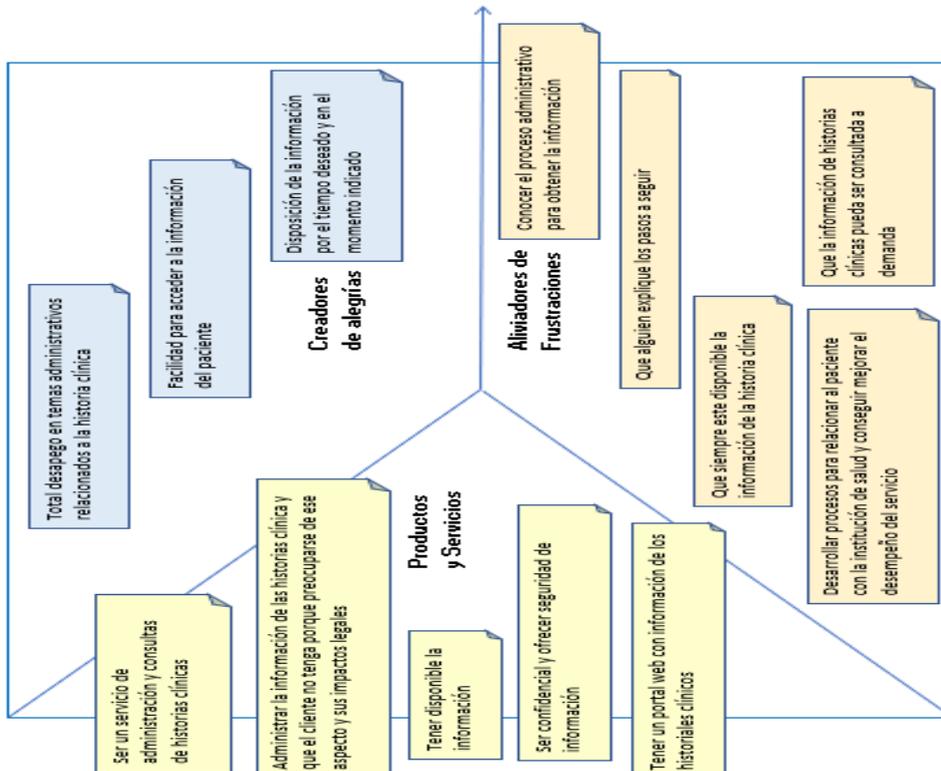
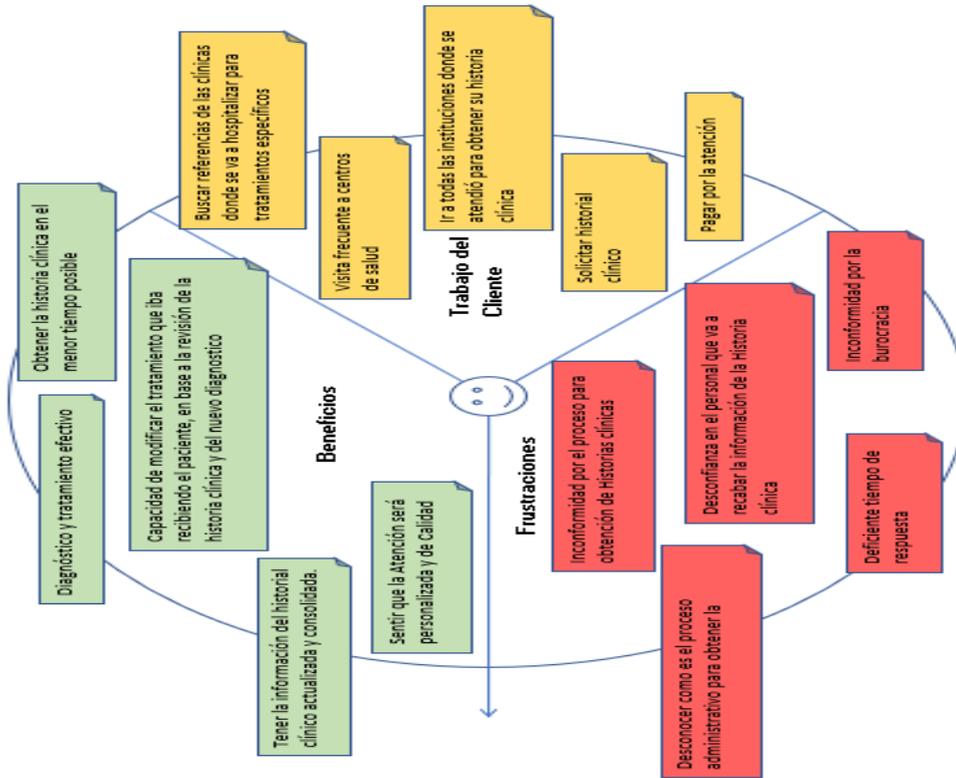
- Medicos Internistas entre 27 a 45 años que crecieron con la tecnología.
- Pacientes entre 22 y 40 años

SCIENTIA ET PRAEIXIS

Anexo 4: Diagrama Persona - Segmento Paciente

<p>"José"</p>  <ul style="list-style-type: none"> - Joven trabajador - Entre los 25 y 40 años - Paciente que necesitan seguimiento y requieren hospitalización 	<p>Behaviors</p> <ul style="list-style-type: none"> - Le gusta cuidar su salud y prevenir enfermedades - Visita frecuentemente la clínica - Necesita tratamiento específico 	<p>Main Problems</p> <ul style="list-style-type: none"> - Disponibilidad de su historia clínica - Confidencialidad de su información - Encontrar una mejor opinión a la enfermedad a tratar - Burocracia en cada institución para proporcionar información de su historial clínico - Tiempos de espera
<p>Demographics</p> <ul style="list-style-type: none"> - Mayor de 25 años - Vive en periferias de Lima o en provincia - Casado - Con posibilidad de pagar EPS 	<p>Need & Goals</p> <ul style="list-style-type: none"> - Tener disponible su información - Que la información sea confiable y segura - Iniciar tratamiento lo mas pronto posible - Sentir que el tratamiento brindado es efectivo y no repetitivo 	<p>Where to find</p> <ul style="list-style-type: none"> - Clínicas - Hospitales - Centros de salud

Anexo 5: Canvas Lienzo Propuesta de Valor



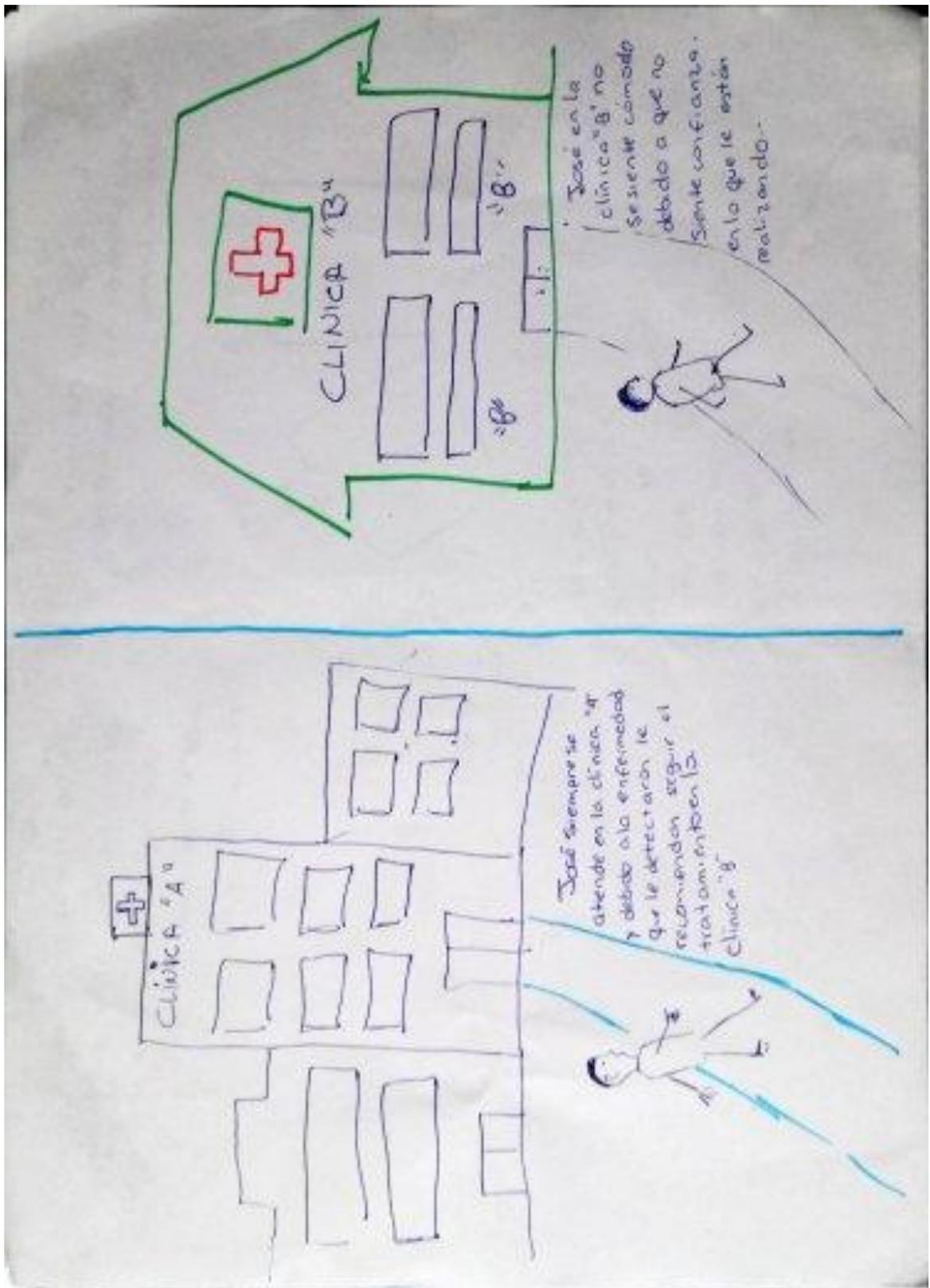
**Anexo 6: Matriz de problemas - Resultado de las entrevistas
para identificar problemas relevantes para el usuario**

	Paciente	Médico
Burocracia en temas administrativos	Lidia Aranda Santiago Cornejo Renán Guzmán RosseMarie Espinoza Jahan Silva Ángelo Danielli	
Resistencia al cambio en el proceso asistencial		Claudia Fuentes Javier Vásquez Miguel Díaz Carlos Villanueva
Inseguridad de compartir información sensible	Lidia Aranda Claudia Díaz Christian Burgos Gerardo Florindez Elisa Escudero Lisset Juárez	Claudia Fuentes Javier Vásquez Miguel Díaz Carlos Villanueva Fiorella Aguilar Kelly Moscoso
Carga administrativa al Médico		Fiorella Aguilar Kelly Moscoso
Seguridad y confiabilidad de la información	José Atoche José Araujo Maritza Yesenia Flores Renán Guzmán RosseMarie Espinoza Jahan Silva David Pauta	

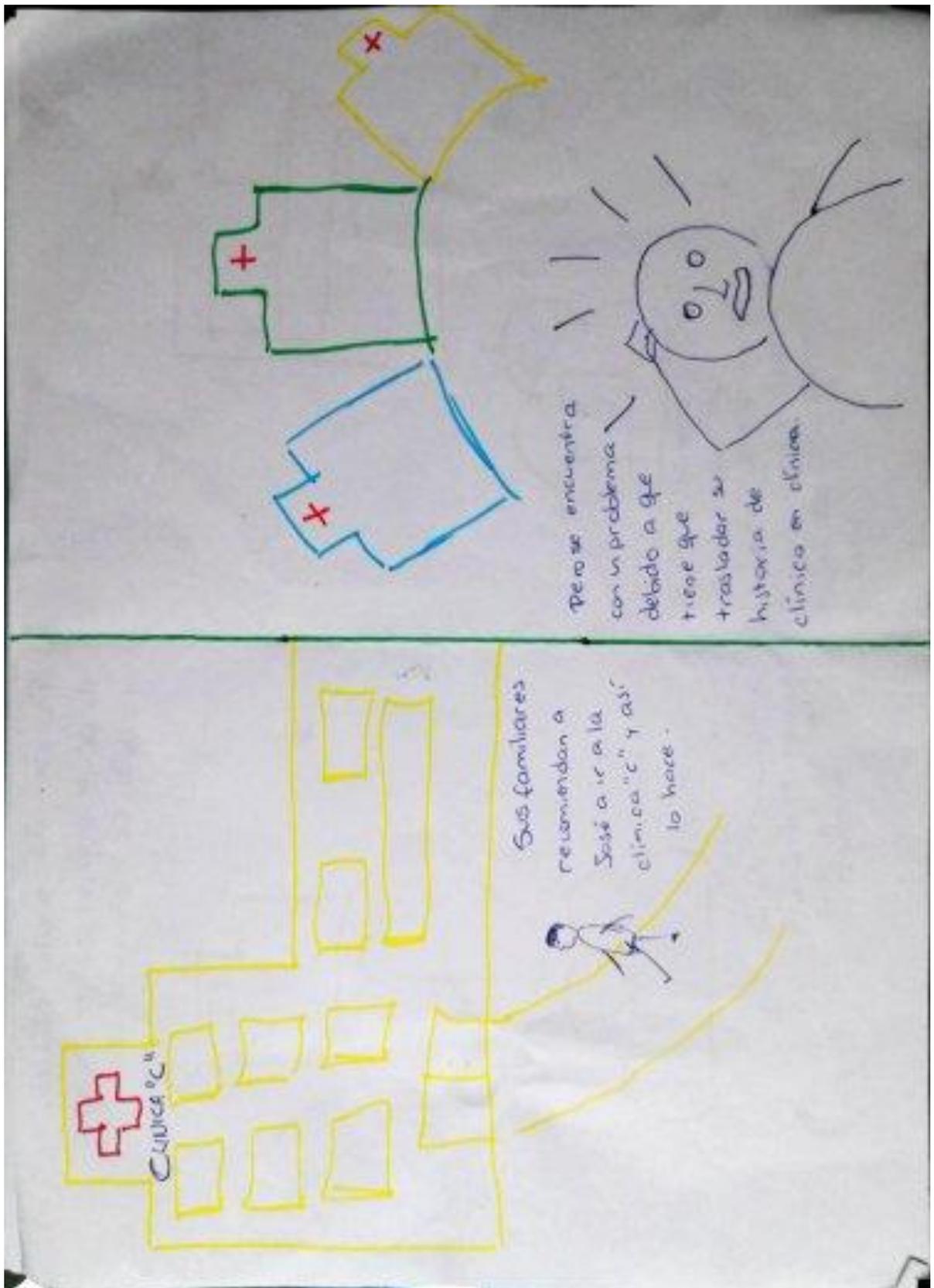
**Anexo 7: Matriz de problemas - Determinar si el problema
que seleccionamos es relevante para los segmentos de
personas seleccionados**

	Paciente	Médico
Disponibilidad de Historias Clínicas para los tipos de atención de emergencias y hospitalizaciones para pacientes de clínicas	Santiago Cornejo Renán Guzmán RosseMarie Espinoza Christian Burgos Gerardo Florindez Elisa Escudero José Atoche José Araujo Maritza Yesenia Flores	Claudia Fuentes Fiorella Aguilar Kelly Moscoso Miguel Díaz
Debo tener una solución para este problema	Ricardo Pachas Lily Muro Iveth Ramírez Paul Palacios Aseneth Uriona	Fiorella Núñez del Prado

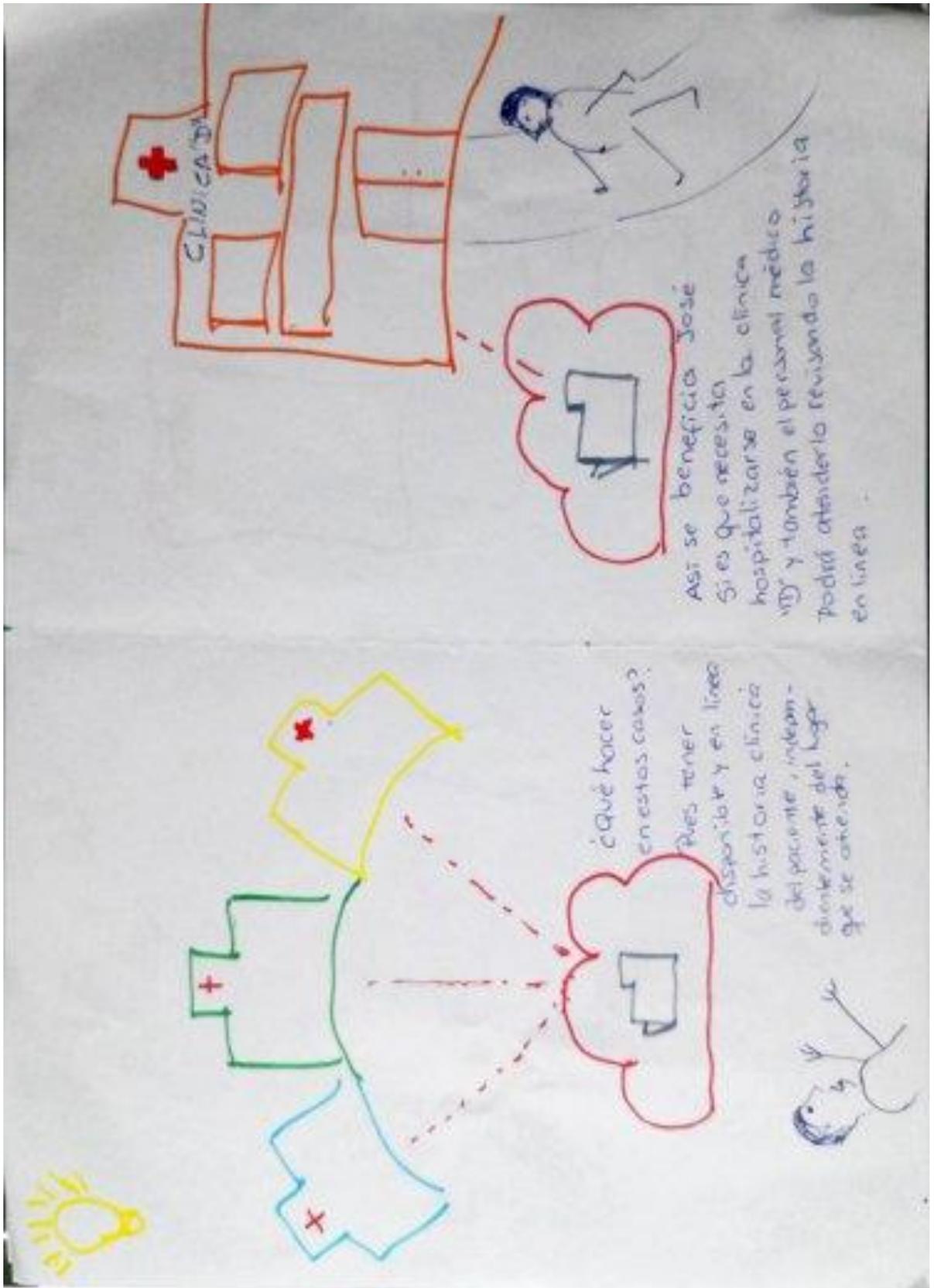
Anexo 8: Storyboard



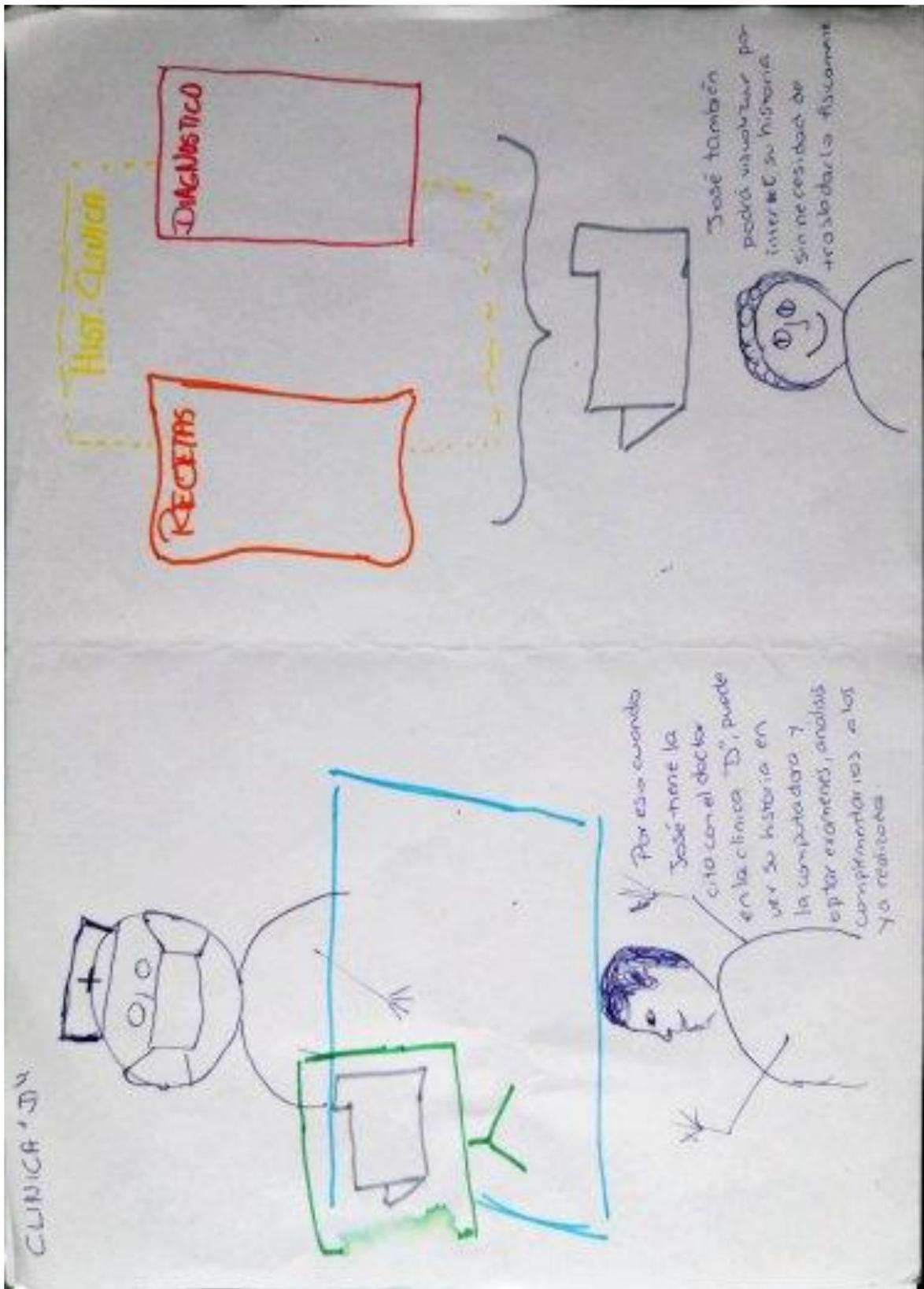
Storyboard (Continuación)



Storyboard (Continuación)



Storyboard (Continuación)



Anexo 9: Resolución Ministerial N°120-2017/MINSA

RESOLUCIÓN MINISTERIAL

N° 120-2017/MINSA

Lima, 23 de febrero del 2017

Visto, el Expediente N° 17-004551-001 que contiene el Informe N° 011-2017-OGTI-ODT/MINSA, de la Oficina General de Tecnologías de la Información;

CONSIDERANDO:

Que, los numerales I y II del Título Preliminar de la Ley N° 26842, Ley General de Salud, señalan que la salud es condición indispensable del desarrollo humano y medio fundamental para alcanzar el bienestar individual y colectivo, por lo que la protección de la salud es de interés público, siendo responsabilidad del Estado regularla, vigilarla y promoverla;

Que, los numerales 1) y 9), del artículo 3 del Decreto Legislativo N° 1161, Ley de Organización y Funciones del Ministerio de Salud, dispone como ámbitos de competencia del Ministerio de Salud, la salud de las personas, y la investigación y tecnologías en salud;

Que, el artículo 4 de la Ley precitada, dispone que el Sector Salud está conformado por el Ministerio de Salud, como organismo rector, las entidades adscritas a él y aquellas instituciones públicas y privadas de nivel nacional, regional y local, y personas naturales que realizan actividades vinculadas a las competencias establecidas en dicha Ley, y que tienen impacto directo o indirecto en la salud, individual o colectiva;

Que, los literales a) y b) del artículo 5 de la acotada Ley, señalan que son funciones rectoras del Ministerio de Salud, el formular, planear, dirigir, coordinar, ejecutar, supervisar y evaluar la política nacional y sectorial de Promoción de la Salud, Prevención de Enfermedades, Recuperación y Rehabilitación en Salud, bajo su competencia, aplicable a todos los niveles de gobierno; así como dictar normas y lineamientos técnicos para la adecuada ejecución y supervisión de las políticas nacionales y sectoriales;

Que, el artículo 49 del Reglamento de Organización y Funciones del Ministerio de Salud, aprobado por Decreto Supremo N° 007-2016-SA, establece que la Oficina General de Tecnologías de la Información es el órgano de apoyo del Ministerio de Salud, dependiente de la Secretaría General, responsable de implementar el gobierno electrónico; planificar, implementar y gestionar los sistemas de información del Ministerio; administrar la información estadística en salud; realizar la innovación y el desarrollo tecnológico, así como del soporte y las telecomunicaciones. Es responsable de diseñar, desarrollar y mejorar las plataformas informáticas de información en el Sector Salud. Establece soluciones tecnológicas, sus especificaciones y requerimientos técnicos para la adquisición, aplicación, mantenimiento y uso de las mismas, en el ámbito de competencia del Ministerio de Salud;

Que, asimismo los literales a), b), i) y k), del artículo 50 del Reglamento precitado, disponen que son funciones de la Oficina General de Tecnologías de la Información, el proponer la política institucional en materia de desarrollo de tecnologías de la información, estadística, gobierno electrónico y su operatividad en el Ministerio de Salud, en concordancia con las políticas nacionales; proponer y supervisar los lineamientos, normas, planes, estrategias, programas y proyectos, en el marco de la Política Nacional de Gobierno Electrónico en el Ministerio de Salud; gestionar el proceso de gestión integrada de la información del Sector Salud proponiendo y supervisando lineamientos, normas o afines para su logro, y coordinar con los órganos la estandarización de la información que producen;

Que, con Resolución Ministerial N° 1942-2002-SA/DM, se aprueba la Directiva N° 001-2002-OGEI: Normas Generales sobre Acciones de Sistemas de Información, Estadística e Informática en el Ministerio de Salud, con el objetivo de establecer las normas generales para las actividades que se realicen en el

campo de los Sistemas de Información, Estadística e Informática en las dependencias del Ministerio de Salud;

Que, con Resolución Ministerial N° 537-2011/MINSA, se aprueba la Directiva Administrativa N° 180-MINSA/OGEI-V.01, Directiva Administrativa que Establece los Criterios Técnicos para la Incorporación de Tecnologías de Información y Comunicaciones en Salud, con el objetivo de establecer los criterios técnicos que permitan integrar la información institucional y articular la información sectorial en salud;

Que, con Resolución Ministerial N° 554-2011/MINSA, se aprueba la Directiva Administrativa N° 181-MINSA/OGEI-V.01, Directiva Administrativa denominada Estándares de Plataforma Informática para Software Aplicativo en el Ministerio de Salud”, con el objetivo de definir los estándares para los componentes de la plataforma informática sobre la que se desarrollará y pondrá en producción el software aplicativo en el Ministerio de Salud;

Que, mediante el documento del visto, la Oficina General de Tecnologías de la Información, en el marco de sus competencias ha elaborado la “Directiva Administrativa que establece los estándares y criterios técnicos para el desarrollo de los sistemas de información en salud”, con la finalidad de contribuir a la integración y articulación de la información en salud, a través de los sistemas de información que se desarrollen en las entidades públicas comprendidas en el ámbito de aplicación de dicha Directiva Administrativa;

Estando a lo propuesto por la Oficina General de Tecnologías de la Información;

Que, mediante el Informe N° 078-2017-OGAJ/MINSA, la Oficina General de Asesoría Jurídica ha emitido opinión legal;

Con el visado del Director General de la Oficina General de Tecnologías de la Información; del Director General de la Oficina General de Asesoría Jurídica y del Secretario General del Ministerio de Salud; y,

De conformidad con el Decreto Legislativo N° 1161, Ley de Organización y Funciones del Ministerio de Salud, y el Reglamento de Organización y Funciones del Ministerio de Salud, aprobado por Decreto Supremo N° 007-2016-SA;

SE RESUELVE:

Artículo 1.- Aprobar la Directiva Administrativa N° 230 – MINSA/2017/OGTI, “Directiva Administrativa que establece los estándares y criterios técnicos para el desarrollo de los sistemas de información en salud”, que en documento adjunto forma parte integrante de la presente Resolución Ministerial.

Artículo 2.- Encargar a la Oficina General de Tecnologías de la Información, la difusión, monitoreo, supervisión y evaluación del cumplimiento de la presente Directiva Administrativa.

Artículo 3.- Derogar las siguientes Resoluciones Ministeriales:

- Resolución Ministerial N° 1942-2002-SA/DM, que aprueba la Directiva N° 001-2002-OGEI: Normas Generales sobre Acciones de Sistemas de Información, Estadística e Informática en el Ministerio de Salud.

- Resolución Ministerial N° 537-2011/MINSA, que aprueba la Directiva Administrativa N° 180-MINSA/OGEI-V.01, Directiva Administrativa que Establece los Criterios Técnicos para la Incorporación de Tecnologías de Información y Comunicaciones en Salud.

- Resolución Ministerial N° 554-2011/MINSA, que aprueba la Directiva Administrativa N° 181-MINSA/OGEI-V.01, Directiva Administrativa denominada Estándares de Plataforma Informática para Software Aplicativo en el Ministerio de Salud.

Artículo 4.- Encargar a la Oficina General de Comunicaciones la publicación de la presente Resolución Ministerial en la dirección electrónica <http://www.minsa.gob.pe/transparencia/index.asp?op=115>, del Portal Institucional del Ministerio de Salud.

Regístrese, comuníquese y publíquese

PATRICIA J. GARCÍA FUNEGRA

Ministra de Salud

Anexo 10: Ley N° 30024

DECRETO SUPREMO

N° 009-2017-SA

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, los artículos 7 y 9 de la Constitución Política del Perú señalan que todos tienen derecho a la protección de su salud, la del medio familiar y la de la comunidad, así como el deber de contribuir a su promoción y defensa. El Estado determina la política nacional de salud y el Poder Ejecutivo norma y supervisa su aplicación y es responsable de diseñarla y conducirla en forma plural y descentralizadora para facilitar a todos el acceso equitativo a los servicios de salud;

Que, los numerales II y XIV del Título Preliminar de la Ley N° 26842, Ley General de Salud, establecen que la protección de la salud es de interés público y responsabilidad del Estado regularla, vigilarla y promoverla. La información en salud es de interés público y que toda persona está obligada a proporcionar a la Autoridad de Salud la información que le sea exigible de acuerdo a ley. La información que el Estado tiene en su poder es de dominio público, con las excepciones que establece la ley;

Que, asimismo, el artículo 123 de la Ley N° 26842, modificada por la Única Disposición Complementaria Modificatoria del Decreto Legislativo N° 1161, Ley de Organización y Funciones del Ministerio de Salud, precisa que el Ministerio de Salud es la Autoridad de Salud de nivel nacional. Como Organismo del Poder Ejecutivo, tiene a su cargo la formulación, dirección y gestión de la política de salud y actúa como la máxima autoridad normativa en materia de salud;

Que, el artículo 4 del Decreto Legislativo N° 1161, Ley de Organización y Funciones del Ministerio de Salud, establece que el Sector Salud está conformado por el Ministerio de Salud, como organismo rector, las entidades adscritas a él y aquellas instituciones públicas y privadas de nivel nacional, regional y local, y personas naturales que realizan actividades vinculadas a las competencias establecidas en dicha Ley, y que tienen impacto directo o indirecto en la salud, individual o colectiva;

Que, asimismo, el literal b) del artículo 5 de la Ley precitada, dispone como una de las funciones rectoras del Ministerio de Salud, dictar normas y lineamientos técnicos para la adecuada ejecución y supervisión de las políticas nacionales y sectoriales, la gestión de los recursos del sector; así como para el otorgamiento y reconocimiento de derechos, fiscalización, sanción y ejecución coactiva en las materias de su competencia;

Que, el artículo 1 de la Ley N° 30024, Ley que Crea el Registro Nacional de Historias Clínicas Electrónicas, señala que el objeto de dicha Ley es crear el Registro Nacional de Historias Clínicas Electrónicas y establecer sus objetivos, administración, organización, implementación, confidencialidad y accesibilidad;

Que, mediante el Decreto Legislativo N° 1306, Decreto Legislativo que optimiza procesos vinculados al Registro Nacional de Historias Clínicas Electrónicas, se modificaron diversos artículos de la Ley N° 30024, Ley que Crea el Registro Nacional de Historias Clínicas Electrónicas;

Que, asimismo, el citado Decreto Legislativo N° 1306 establece en su Primera Disposición Complementaria Final, que el Poder Ejecutivo en el plazo de sesenta (60) días calendario adecua el reglamento de la Ley N° 30024, Ley que Crea el Registro Nacional de Historias Clínicas Electrónicas;

Que, en virtud de ello, corresponde efectuar la adecuación de la normativa reglamentaria referida al Registro Nacional de Historias Clínicas Electrónicas, lo cual permitirá organizar y mantener el registro de las Historias Clínicas Electrónicas, estandarizar los datos y la información clínica, asegurar la disponibilidad de la información clínica para el paciente o su representante legal y para los profesionales de salud autorizados en el ámbito estricto de la atención de salud al paciente entre otras, a fin de mejorar la calidad de la atención en los establecimientos de salud y en los servicios médicos de apoyo;

De conformidad con lo dispuesto en el numeral 8 del artículo 118 de la Constitución Política del Perú y en la Ley N° 29158, Ley Orgánica del Poder Ejecutivo;

DECRETA:

Artículo 1.- Aprobación del Reglamento

Apruébese el “Reglamento de la Ley N° 30024, Ley que Crea el Registro Nacional de Historias Clínicas Electrónicas”, que consta de siete (7) Títulos, ochenta y tres (83) Artículos, tres (3) Disposiciones Complementarias Finales y seis (6) Disposiciones Complementarias Transitorias, que forman parte del presente Decreto Supremo.

Artículo 2.- Derogatoria

Deróguese todo aquello que se oponga al presente Decreto Supremo.

Artículo 3.- Refrendo

El presente Decreto Supremo, será refrendado por la Ministra de Salud.

Dado en la Casa de Gobierno, en Lima, a los veintidós días del mes de marzo del año dos mil diecisiete.

PEDRO PABLO KUCZYNSKI GODARD

Presidente de la República

PATRICIA J. GARCÍA FUNEGRA

Ministra de Salud

“REGLAMENTO DE LA LEY N° 30024, LEY QUE CREA EL REGISTRO NACIONAL DE HISTORIAS CLÍNICAS ELECTRÓNICAS”

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1.- Objeto del Reglamento

El presente Reglamento tiene como objeto establecer las disposiciones para la aplicación y adecuado cumplimiento de la Ley N° 30024, Ley que Crea el Registro Nacional de Historias Clínicas Electrónicas y su modificatoria.

Cuando en el presente Reglamento se haga mención a la Ley, se entenderá que se refiere a la Ley N° 30024, Ley que crea el Registro Nacional de Historias Clínicas Electrónicas y su modificatoria.

Cuando en el presente Reglamento se haga mención al RENHICE, se entenderá que alude al Registro Nacional de Historias Clínicas Electrónicas.

Artículo 2.- Ámbito de aplicación

Las disposiciones del presente Reglamento son de aplicación a los pacientes o usuarios de salud, su representante legal, a los profesionales de la salud, a los establecimientos de salud y a los servicios médicos de apoyo públicos, privados o mixtos comprendidos en la Ley N° 26842, Ley General de Salud, que emplean historias clínicas electrónicas, así como todas las personas que laboren en los establecimientos de salud o servicios médicos de apoyo.

Artículo 3.- Definiciones operativas y acrónimos

Para los efectos del presente Reglamento entiéndase las siguientes definiciones y acrónimos conforme se señalan a continuación:

Definiciones operativas:

a) **Acreditación de sistemas de información de historias clínicas electrónicas.**- La acreditación es la verificación positiva que el sistema de información de historias clínicas electrónicas que usa un establecimiento de salud o conjunto de establecimientos de salud o servicios médicos de apoyo se sujeta a los criterios técnicos establecidos en el presente Reglamento y por la Autoridad Nacional de Salud en otras normas complementarias.

b) **Auditoría de sistemas de información de historias clínicas electrónicas.**- Es el proceso programado o inopinado mediante el cual la Autoridad Nacional de Salud recopila, verifica, analiza y evalúa evidencias para determinar si el establecimiento de salud o servicio médico de apoyo en el uso de su sistema de información de historias clínicas electrónicas, cumplen con lo establecido en la Ley, en el presente Reglamento y en las normas complementarias, así como con las medidas de seguridad y requisitos técnicos de interoperabilidad.

c) **Asistencia técnica.**- Es el proceso mediante el cual se brinda las orientaciones técnicas necesarias a los establecimientos de salud y servicios médicos de apoyo para la implementación de los sistemas de información de historias clínicas electrónicas a nivel nacional, regional y local.

d) **Autenticación de la identidad del usuario del RENHICE:** Es el proceso por el cual se verifica la identidad de una persona natural, para acceder al RENHICE.

e) **Autoridad Nacional de Salud:** Es el Ministerio de Salud, organismo rector del Sector Salud.

f) **Autoridad Regional de Salud:** Son las direcciones regionales de salud (DIRESAS), gerencias regionales de salud (GERESAS), o las que hagan sus veces en los gobiernos regionales. En el caso de Lima Metropolitana corresponde a las direcciones de redes integradas de salud (DIRIS).

g) **Autorización de acceso del paciente o usuario de salud o de su representante legal:** Es el consentimiento que brinda el paciente o usuario de salud o su representante legal al profesional de la salud para acceder a su información clínica, a través del RENHICE conforme a las condiciones y procedimientos previstos en la Ley N° 29733, Ley de Protección de Datos Personales, su norma reglamentaria aprobada mediante Decreto Supremo N° 003-2013-JUS y el presente Reglamento.

h) **Certificado digital:** El certificado digital es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad.

i) **Datos de filiación:** En el RENHICE los datos de filiación son la información personal del paciente o usuario en salud, contenida en la historia clínica electrónica, referida a los nombres, apellidos, tipo y número de documento de identificación, dirección, distrito, sexo, estado civil, fecha de nacimiento, nombre del padre y nombre de la madre. Además, incluyen los nombres, apellidos, el tipo y número de documento de identificación del representante legal cuando corresponda.

j) **Documento nacional de identidad electrónico (DNIe):** Es un documento nacional de identidad, emitido por el RENIEC, que acredita presencial y electrónicamente, la identidad personal de su titular, permitiendo la firma digital de documentos electrónicos.

k) **Historia clínica informatizada:** Es la historia clínica soportada en medios electrónicos que permiten su almacenamiento, actualización y recuperación, en una amplia gama de posibilidades para el uso de la información clínica, procesos y metodologías estandarizadas. Dicha historia clínica no utiliza la firma digital para refrendar su contenido.

l) **Implementación de los sistemas de información de historias clínicas electrónicas:** Es el proceso por el cual los establecimientos de salud o servicios médicos de apoyo realizan las gestiones necesarias con la finalidad de disponer de un sistema de información de historias clínicas electrónicas que les permitirá interoperar con el RENHICE.

m) **Información clínica:** Es toda información contenida en una historia clínica electrónica, que registra el profesional de la salud que atiende al paciente, concerniente a la salud pasada, presente o pronosticada, física o mental, de una persona, incluida la información complementaria (resultados de exámenes auxiliares y otros). No incluye los datos de filiación contenidos en la historia clínica electrónica.

De acuerdo a lo establecido en la Ley 29733, Ley de Protección de Datos Personales y su Reglamento aprobado mediante Decreto Supremo N° 003-2013-JUS, la información clínica constituye datos sensibles.

La información clínica a su vez contiene información clínica básica y también información clínica sensible.

n) **Información clínica básica:** Es la información clínica contenida en la historia clínica electrónica del paciente referida a los antecedentes generales, patológicos y familiares más importantes, como alergias, diagnósticos anteriores, medicación, cirugías previas, grupo sanguíneo, que proporcionen información básica para la atención de salud ante una situación de emergencia, la misma a la que el profesional de la

salud podrá acceder a través del RENHICE, desde un terminal en el establecimiento de salud o servicio médico de apoyo, sin la autorización de acceso del paciente o usuario de salud, únicamente en casos de grave riesgo para la vida o la salud de una persona cuyo estado no permita la capacidad de autorizar el acceso a sus historias clínicas electrónicas.

o) **Información clínica resumida:** Es el resumen de la estancia en el servicio de hospitalización del establecimiento de salud (Epicrisis), la misma que es elaborada por el médico tratante al egreso del paciente.

p) **Información clínica sensible:** Es la información clínica contenida en la historia clínica electrónica del paciente o usuario de salud y que este haya determinado como tal, la misma que puede estar referida a su genética, sexualidad, paridad, cirugías, enfermedades infecciosas como VIH, de transmisión sexual; y otras que por su naturaleza son temas sensibles para el paciente por las características físicas, morales o emocionales que pudieran presentar, así como los hechos o circunstancias que se pudieran generar en su vida afectiva, familiar o esfera íntima; y a la que solamente se debe acceder con su autorización expresa.

q) **Médico tratante:** Es el médico que tiene bajo su responsabilidad la atención de un paciente.

r) **Personas intervinientes en la gestión de la información accedida a través del RENHICE:** Son aquellas personas que por su labor u oficio acceden directa o indirectamente a la información clínica contenida en las historias clínicas electrónicas a través del RENHICE y que producto de ello se encuentran obligadas a guardar confidencialidad de dicha información, conforme a lo señalado por la Constitución Política del Perú, la Ley N° 29733, Ley de Protección de Datos Personales, su Reglamento aprobado mediante Decreto Supremo N° 003-2013-JUS y demás normas dadas en el ordenamiento jurídico. No están incluidos en esta definición los usuarios del RENHICE.

s) **Profesionales de la salud:** Son aquellos como el médico, enfermera, odontólogo, obstetra, psicólogo, nutricionista, entre otros, facultados para acceder a la historia clínica de un paciente o usuario de salud, y registrar en ella la atención que le brindan en el establecimiento de salud o servicio médico de apoyo.

t) **Sistema de Gestión de Seguridad de la Información:** Es la parte del sistema integral de gestión, basado en un enfoque de riesgo del negocio para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizacional, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos.

u) **Usuario del RENHICE:** Paciente o usuario de salud o su representante legal que autoriza que se pueda acceder a sus historias clínicas electrónicas a través del RENHICE y de los sistemas de información de los establecimientos de salud o servicios médicos de apoyo en los que se atendió, según lo establecido en el presente Reglamento. También es el profesional de salud que es autorizado por el paciente o usuario de salud o su representante legal, salvo en los supuestos contemplados en el presente Reglamento, para que acceda a la información clínica contenida en sus historias clínicas electrónicas correspondiente desde un establecimiento de salud o servicio médico de apoyo.

Acrónimos:

a) DIRESA: Dirección Regional de Salud

b) DIRIS: Direcciones de Redes Integradas de Salud

c) GERESA: Gerencia Regional de Salud

d) IPRESS: Instituciones Prestadoras de Servicios de Salud

e) ONGEI: Oficina Nacional de Gobierno Electrónico e Informática

f) PIDE: Plataforma de Interoperabilidad del Estado

g) RENHICE: Registro Nacional de Historias Clínicas Electrónicas

h) RENIEC: Registro Nacional de Identificación y Estado Civil

i) SUSALUD: Superintendencia Nacional de Salud

TÍTULO II

EL REGISTRO NACIONAL DE HISTORIAS CLÍNICAS ELECTRÓNICAS

CAPÍTULO I

DEL REGISTRO NACIONAL DE HISTORIAS CLÍNICAS ELECTRÓNICAS

Artículo 4.- Objetivos del RENHICE

Además de los objetivos señalados en la Ley, se establecen los siguientes:

- a) Establecer los mecanismos que garanticen la protección de datos personales en el proceso de atención de salud en los establecimientos de salud y servicios médicos de apoyo que implementan el uso de las historias clínicas electrónicas.
- b) Optimizar el uso de recursos y reducir la duplicidad de procedimientos de apoyo al diagnóstico que ya han sido aplicados al paciente o usuario de salud.

Artículo 5.- Principios del RENHICE

Son aplicables al RENHICE y su funcionamiento los siguientes principios:

a) Autonomía para la autorización de acceso

La autorización de acceso que brinda el paciente o usuario de salud o su representante legal al profesional de la salud que lo atiende, para la visualización o lectura de sus historias clínicas electrónicas a través del RENHICE, debe ser dado con la capacidad autónoma, libre y de manera informada, en concordancia con las exigencias de la normativa en materia de salud y con las obligaciones dispuestas en la Ley N° 29733, Ley de Protección de Datos Personales y su Reglamento aprobado mediante Decreto Supremo N° 003-2013-JUS.

b) Disponibilidad

La continuidad de la operatividad del sistema de información del RENHICE debe brindar y garantizar el acceso fácil, gratuito y seguro de los usuarios del RENHICE.

c) Veracidad

La información accedida a través del RENHICE debe corresponder con la consignada en la historia clínica electrónica del paciente o usuario de salud al momento de atenderse en cada establecimiento de salud o servicio médico de apoyo al que acude para recibir la atención.

d) Confidencialidad

Todas aquellas personas que acceden a la información clínica disponible a través del RENHICE, deben mantener la obligación de confidencialidad de dicha información según el mandato de Ley y del presente Reglamento, además de la obligación del secreto profesional correspondiente.

e) Accesibilidad

El paciente o usuario de salud como titular de su información clínica tendrá en todo momento derecho a acceder para visualizar sus datos de filiación registrados, así como a su información clínica contenida en sus historias clínicas electrónicas a través del RENHICE, sin necesidad de motivar el requerimiento.

f) Seguridad

El RENHICE y los sistemas de información de historias clínicas electrónicas se enmarcan dentro de un sistema de gestión de la seguridad de la información, que garantiza la confidencialidad y el derecho a la privacidad de los propietarios de la información clínica contenida en las historias clínicas electrónicas.

g) Finalidad de uso

Toda información disponible a través del acceso al RENHICE, en especial la referida a la información clínica de los pacientes o usuarios de salud, no puede ser utilizada o tratada para un uso distinto del autorizado por el paciente o usuario de salud o su representante legal, o autorización dada por ley. El uso debe ser para fines lícitos y en salvaguarda de los derechos constitucionales y legales que tiene el paciente o usuario de salud a la privacidad y a la protección de sus datos personales.

Artículo 6.- Autoridad competente

El Ministerio de Salud como Autoridad Nacional de Salud, es la autoridad competente para regular, organizar, implementar y supervisar el RENHICE, así como coordinar y supervisar el accionar de los diversos actores involucrados en su funcionamiento, implementación y uso, en cumplimiento de los objetivos y disposiciones establecidos por la Ley y el presente Reglamento.

Artículo 7.- Competencias del Ministerio de Salud en el RENHICE

Las competencias del Ministerio de Salud para la implementación y funcionamiento del RENHICE, son las siguientes:

- a) Ejercer la titularidad de la base de datos del RENHICE.
- b) Conducir, regular y administrar el RENHICE, y promover junto con los gobiernos regionales su implementación progresiva.
- c) Acreditar y supervisar los Sistemas de Información de Historias Clínicas Electrónicas implementados por los establecimientos de salud y servicios médicos de apoyo, en coordinación con la PCM, a través de ONGEI como ente rector del Sistema Nacional de Informática; de acuerdo a los lineamientos establecidos por el MINSA.
- d) Establecer la arquitectura, características, requisitos, estándares y buenas prácticas básicos de un sistema de información de historias clínicas electrónicas con los criterios técnicos establecidos en la Ley, el presente Reglamento y de acuerdo a la normatividad vigente en Gobierno Electrónico, para ser destinados a los establecimientos de salud y servicios médicos de apoyo públicos, bajo su ámbito.
- e) Suscribir convenios interinstitucionales o de cooperación técnica necesarios para la implementación y operación del RENHICE.
- f) Determinar e implementar el proceso de identificación y autenticación de la identidad del usuario para el acceso al RENHICE y a los sistemas de información de historias clínicas electrónicas.
- g) Supervisar que los establecimientos de salud y servicios médicos de apoyo aseguren la protección de los datos de filiación e información clínica involucrados en el funcionamiento e interoperabilidad de sus sistemas de información.
- h) Promover la implementación progresiva de los sistemas de información de historias clínicas electrónicas en los establecimientos de salud y servicios médicos de apoyo.
- i) Supervisar el cumplimiento de las obligaciones señaladas en la Ley, el presente Reglamento y demás normas complementarias que apruebe el Ministerio de Salud.
- j) Las demás competencias establecidas en la Ley.

Artículo 8.- Conducción del RENHICE

El Ministerio de Salud, a través de la Oficina General de Tecnologías de la Información, ejerce la responsabilidad de conducir el RENHICE, desde los aspectos técnicos y tecnológicos relacionados a su implementación. Dicha instancia coordina con la Dirección General de Intervenciones Estratégicas en Salud Pública, y demás órganos, unidades orgánicas y organismos públicos especializados adscritos al Ministerio de Salud y otras entidades e instituciones para el apoyo o la asistencia técnica del RENHICE que sean necesarios en coordinación con la PCM. .

Artículo 9.- Procesos del RENHICE

Los procesos principales que se desarrollan para el funcionamiento adecuado del RENHICE son los siguientes:

- a. Gestión del modelo de información y de la infraestructura tecnológica del RENHICE
- b. Gestión del desempeño del RENHICE
- c. Gestión de los servicios de autenticación del RENIEC
- d. Acreditación de los sistemas de información de historias clínicas electrónicas
- e. Supervisión y auditoría de los sistemas de información de historias clínicas electrónicas
- f. Administración del acceso a las historias clínicas electrónicas a través del RENHICE

g. Asistencia técnica y soporte a los Usuarios del RENHICE

Artículo 10.- Información contenida en el RENHICE

El RENHICE, respecto a la información del paciente, contiene lo siguiente:

- La identificación estándar de dato en salud N° 003, “Usuario de salud en el sector salud” correspondiente al número de documento nacional de identidad del paciente o usuario de salud;
- La identificación estándar de dato en salud N° 004, “Establecimiento de salud y de servicio médico de apoyo en el sector salud” correspondiente al código único del Registro Nacional de IPRESS, o el que haga sus veces, del establecimiento de salud o servicios médicos de apoyo que le ha generado una historia clínica electrónica; y
- Las Historias Clínicas Electrónicas de los establecimientos de salud y/o Servicios médicos de Apoyo, en los cuales el paciente haya recibido una atención, y haya autorizado expresamente que estas se sitúen en el RENHICE, las mismas que se encontrarán a modo de respaldo debidamente identificadas.

Esta información es por cada paciente o usuario de salud con historia clínica electrónica generada en cada establecimiento de salud o servicio médico de apoyo donde se haya atendido.

Artículo 11.- Características de la Información contenida en el RENHICE

La información contenida en el RENHICE debe estar disociada como implementación del sistema de gestión de seguridad de la información y protección de datos personales.

Artículo 12.- De la Información brindada por el RENHICE al Sistema Nacional de Salud

El Ministerio de Salud debe asegurar que el RENHICE cuente con la capacidad tecnológica necesaria principalmente para aplicar procedimientos de anonimización para brindar información al Sistema Nacional de Salud para el diseño y aplicación de políticas públicas que permitan el ejercicio efectivo del derecho a la salud de las personas, de conformidad con lo establecido en el literal “e” del artículo 4 de la Ley.

CAPÍTULO II

OBLIGACIÓN DE ACREDITAR LOS SISTEMAS DE INFORMACIÓN DE HISTORIAS CLÍNICAS ELECTRÓNICAS ANTE EL MINISTERIO DE SALUD

Artículo 13.- Obligatoriedad de los establecimientos de salud y servicios médicos de apoyo

Todo establecimiento de salud público, privado o mixto, que cuente con un sistema de información de historias clínicas electrónicas deberá acreditarlo, de manera obligatoria ante el Ministerio de Salud o la Autoridad Regional de Salud, conforme a lo establecido en la Ley, el presente Reglamento y demás normas complementarias.

Los servicios médicos de apoyo públicos, privados o mixtos, que brindan atención reiterada a los mismos usuarios de salud o pacientes, y que por la naturaleza del servicio que brindan, deben llevar el registro seriado de dichas atenciones en historias clínicas, y que para tal fin empleen historias clínicas electrónicas, están sujetos a lo dispuesto en el párrafo anterior. Lo dispuesto no aplica a los servicios médicos de apoyo que funcionan dentro de un establecimiento de salud.

CAPÍTULO III

ACCESO AL REGISTRO NACIONAL DE HISTORIAS CLÍNICAS ELECTRÓNICAS

Artículo 14.- De los medios de acceso al RENHICE

El acceso al RENHICE se podrá realizar únicamente a través del sistema de información de historias clínicas electrónicas de los establecimientos de salud o de los servicios médicos de apoyo, y a través del sistema de información propio del RENHICE, según las diferentes reglas de autorización de acceso establecidas en el artículo 60 del presente Reglamento.

El RENHICE utiliza la PIDE, la cual garantizará el intercambio automatizado de datos y acceso a la información clínica del paciente o usuario de salud contenida en los sistemas de información de historias clínicas electrónicas de los establecimientos de salud y servicios médicos de apoyo y el RENHICE,

mediante implementación de los estándares de interoperabilidad en salud, de seguridad y continuidad operativa, los cuales deberán ser acreditados y supervisados por el MINSA, como administrador del RENHICE y ente rector del Sistema Nacional de Salud.

Artículo 15.- Acceso de usuarios del RENHICE

Cada paciente o usuario de salud, según su necesidad, accede a su historia clínica electrónica usando el sistema de información del RENHICE. También puede brindar autorización de acceso a sus historias clínicas electrónicas, de otros establecimientos de salud o servicios médicos de apoyo durante la atención que le brinda el profesional de la salud en un establecimiento de salud y que necesita visualizar o leer dichas historias clínicas electrónicas. En todos los casos, el paciente o usuario de salud utiliza los mecanismos de autenticación establecidas en el Título VI, Capítulo I del presente Reglamento.

Los profesionales de la salud solamente acceden al RENHICE cuando brindan la atención, a través del sistema de información de historias clínicas electrónicas del establecimiento de salud o servicio médico de apoyo. Para dicho acceso es necesario que el paciente o usuario de salud le otorgue previa y expresamente su autorización de acceso. El profesional de la salud que lo atiende, accede al RENHICE cumpliendo con los mecanismos de autenticación de la identidad establecidos en el Título VI, Capítulo I del presente Reglamento.

Artículo 16.- De la infraestructura tecnológica del RENHICE

El Ministerio de Salud planifica, implementa, opera y mantiene la infraestructura tecnológica a través de la cual se realizará la recepción, almacenamiento, consulta, verificación, administración, transmisión y seguridad de la información contenida y accesible a través del RENHICE, ONGEI-PCM brindará la asistencia técnica correspondiente.

TÍTULO III

SISTEMA DE INFORMACIÓN PARA LAS HISTORIAS CLÍNICAS ELECTRÓNICAS

CAPÍTULO I

DE LOS SISTEMAS DE INFORMACIÓN DE HISTORIAS CLÍNICAS ELECTRÓNICAS

Artículo 17.- Sistema de información de historias clínicas electrónicas

Todo establecimiento de salud o servicio médico de apoyo que cuente con historias clínicas electrónicas debe acreditar obligatoriamente su sistema de información para acceder al RENHICE.

El sistema de información de historias clínicas electrónicas de cada establecimiento de salud o servicio médico de apoyo, permite que cada paciente o usuario de salud, nuevo o continuador, pueda ser atendido con su historia clínica electrónica, pero además si el paciente o usuario de salud lo autoriza permite que el médico tratante pueda acceder a través del RENHICE, a visualizar o leer sus otras historias clínicas electrónicas generadas en otros establecimientos de salud o servicios médicos de apoyo.

El sistema de información de historias clínicas electrónicas de cada establecimiento de salud o servicio médico de apoyo, debe estar diseñado para transmitir la actualización de información de las historias clínicas electrónicas, que el paciente haya autorizado expresamente, al repositorio de datos del RENHICE, mediante los mecanismos que establezca el Ministerio de Salud en la norma complementaria correspondiente.

El sistema de información de historias clínicas electrónicas de cada establecimiento de salud o servicio médico de apoyo, debe estar diseñado para presentar a requerimiento y por separado los datos de filiación, la información clínica, la información clínica básica, y la información clínica sensible de cada historia clínica electrónica.

Artículo 18.- De la implementación del RENHICE y de los sistemas de información de historias clínicas electrónicas en los establecimientos de salud públicos o servicios médicos de apoyo

Para la implementación del RENHICE y de los sistemas de información de historias clínicas electrónicas en los establecimientos de salud o servicios médicos de apoyo públicos del país, el gobierno nacional, gobiernos regionales, locales e instituciones públicas, deben realizar la planificación necesaria e incluirla en los presupuestos anuales correspondientes.

CAPÍTULO II

ACREDITACIÓN DE LOS SISTEMAS DE INFORMACIÓN DE LOS ESTABLECIMIENTOS DE SALUD Y SERVICIOS MÉDICOS DE APOYO

Artículo 19.- Responsabilidad de la Autoridad Nacional de Salud

El Ministerio de Salud es responsable de acreditar los sistemas de información de historias clínicas electrónicas de los establecimientos de salud y de los servicios médicos de apoyo públicos, privados y mixtos del país, que cuenten con dicho tipo de historia clínica; y de supervisar la implementación conforme a lo señalado en la Ley, el presente Reglamento y demás normas complementarias, cumpliendo con los criterios establecidos para acreditar, y garantizando que se resguarda la reserva, privacidad y confidencialidad de la información clínica contenida en estas.

Artículo 20.- Responsabilidad de la Autoridad Regional de Salud.

Las direcciones regionales de salud, gerencias regionales de salud, o las que hagan sus veces en los gobiernos regionales y las direcciones de redes integradas de salud, supervisan, promocionan e implementan progresivamente el uso de la historia clínica electrónica en cumplimiento de la Ley, el presente Reglamento y demás normas complementarias que emita el Ministerio de Salud. Asimismo, participan en la acreditación de los sistemas de información de historias clínicas electrónicas de los establecimientos de salud y servicios médicos de apoyo, públicos, privados y mixtos de su ámbito.

Artículo 21.- Acreditación de los sistemas de información de historias clínicas electrónicas para acceder al RENHICE

El Ministerio de Salud acredita los sistemas de información de historias clínicas electrónicas para acceder al RENHICE. La Autoridad Regional de Salud acredita los sistemas de información de historias clínicas electrónicas para acceder al RENHICE, de los establecimientos de salud y servicios médicos de apoyo, públicos, privados o mixtos, de su jurisdicción, bajo las disposiciones contenidas en la Ley, el presente Reglamento y las normas emitidas por la Autoridad Nacional de Salud.

Artículo 22.- Requisitos básicos para el proceso de acreditación del sistema de información de historias clínicas electrónicas

Como parte de los requisitos básicos para el proceso de acreditación de sus sistemas de información de historias clínicas electrónicas, los establecimientos de salud y servicios médicos de apoyo deben cumplir con:

- a. El establecimiento de salud o servicio médico de apoyo debe estar inscrito obligatoriamente en el Registro Nacional de IPRESS, o el que haga sus veces y deberá cumplir con lo señalado en la Norma Técnica de la Historia Clínica de los Establecimientos del Sector Salud vigente.
- b. El sistema de información de historias clínicas electrónicas debe cumplir con las identificaciones estándar de datos de salud aprobados con el Decreto Supremo N° 024-2005-SA y demás normas complementarias que el Ministerio de Salud apruebe.
- c. El sistema de información de historias clínicas electrónicas se contar con la capacidad tecnológica necesaria de brindar información al Sistema Nacional de Salud de acuerdo a lo establecido por el Ministerio de Salud. El sistema de información de historias clínicas electrónicas debe interoperar con los servicios de identificación de datos personales que brinda el RENIEC y el Ministerio del Interior para el presente Reglamento.
- d. Los requisitos mínimos de interoperabilidad establecidos en el artículo 34 del presente Reglamento.
- e. Los requisitos mínimos de la seguridad de la información referidos en el artículo 30 del presente Reglamento. Asimismo, la Base de Datos o el sistema de información de historias clínicas electrónicas de los establecimientos de salud o servicios médicos de apoyo deberán registrarse ante la Autoridad Nacional de Protección de Datos Personales del Ministerio de Justicia conforme a lo establecido en la Ley N° 29733, Ley de Protección de Datos Personales, su Reglamento aprobado por Decreto Supremo N° 003-2013-JUS y la Directiva de Seguridad de la Información aprobada por Resolución Directoral N° 019-2013-JUS-DGPDP.
- f. Incorporar la firma digital en los sistemas de información de historias clínicas electrónicas del establecimiento de salud y servicios médicos de apoyo, conforme a lo establecido en la Ley N° 27269,

Ley de Firmas y Certificados Digitales su Reglamento aprobado por Decreto Supremo N° 052-2008-PCM y sus modificatorias.

g. Una estructura de datos que separe los datos de filiación del paciente o usuario de salud de la información clínica correspondiente a sus atenciones, pudiendo asociarse ambas únicamente en el ámbito de la prestación de una atención asistencial al titular de la historia clínica electrónica, y que permita identificar la información clínica básica y la información clínica sensible.

h. El registro en la historia clínica electrónica se hará únicamente como consecuencia de la atención de salud al paciente o usuario de salud.

i. La implementación de mecanismos que permitan el acceso y disponibilidad para asegurar la continuidad de las atenciones de salud, así como la transmisión de la actualización de información de las historias clínicas electrónicas generadas en los establecimientos de salud y servicios médicos de apoyo y autorizadas expresamente por el paciente o usuario de salud para ser almacenadas en el RENHICE.

j. Los establecimientos de salud y servicios médicos de apoyo deben contar con equipos terminales de datos o dispositivos electrónicos para acceso, en cada consultorio de atención; en cada piso de hospitalización; en emergencia y en cada unidad productora de servicios de salud que generen información clínica del paciente.

k. Los demás criterios que el Ministerio de Salud establezca en las normas específicas y complementarias que sean necesarias en materia de gestión de la historia clínica electrónica, identificación, autenticación de las personas, seguridad de la información e interoperabilidad para acceder al RENHICE.

Artículo 23.- Acreditación de los sistemas de información de historias clínicas electrónicas por la Autoridad Regional de Salud

El Ministerio de Salud establecerá el procedimiento mediante el cual faculta a la Autoridad Regional de Salud a llevar a cabo la acreditación de los sistemas de información de su jurisdicción. Para ello verificará periódicamente que cuenten con las capacidades y competencias para cumplir con lo dispuesto en el presente Reglamento, y desarrollará previamente las acciones de capacitación y asistencia técnica necesaria, y de acompañamiento técnico, conforme a lo señalado en la norma complementaria que el Ministerio de Salud apruebe.

CAPÍTULO III

IMPLEMENTACIÓN DE LOS SISTEMAS DE INFORMACIÓN DE HISTORIAS CLÍNICAS ELECTRÓNICAS EN LOS ESTABLECIMIENTOS DE SALUD Y SERVICIOS MÉDICOS DE APOYO

Artículo 24.- Implementación de los sistemas de información de historias clínicas electrónicas de los establecimientos de salud

Los establecimientos de salud públicos, privados o mixtos, que usan historias clínicas informatizadas, deberán implementar un sistema de información de historias clínicas electrónicas para la acreditación establecida por la Ley, el presente Reglamento y demás normas complementarias.

Artículo 25.- Implementación de los sistemas de información de los servicios médicos de apoyo

Los servicios médicos de apoyo que no generen historias clínicas electrónicas no se encuentran obligados a acreditar su sistema de información.

Los servicios médicos de apoyo, públicos, privados o mixtos, que brindan atenciones continuas o repetidas y que por la naturaleza de su servicio generen historias clínicas electrónicas o informatizadas deberán implementar un sistema de información de historias clínicas electrónicas y acreditar obligatoriamente éste para acceder al RENHICE, según lo señalado por la Ley, el presente Reglamento y demás normas complementarias.

Artículo 26.- Obligatoriedad de adecuar el sistema de información de historias clínicas electrónicas al RENHICE

Todo establecimiento de salud y servicio médico de apoyo público, privado o mixto, que cuente con historias clínicas electrónicas o informatizadas están obligados a formar parte del RENHICE. Para ser parte del RENHICE deberán adecuar y acreditar su sistema de información de historias clínicas

electrónicas, en un plazo de doce (12) meses contados a partir de la aprobación del procedimiento que establecerá el Ministerio de Salud, conforme a lo previsto en el artículo 23 del presente Reglamento.

Artículo 27.- Implementación en los establecimientos de salud o servicios médicos de apoyo que cuenten con historias clínicas manuscritas

Los establecimientos de salud o servicios médicos de apoyo, públicos, privados o mixtos, que cuenten con historias clínicas manuscritas deberán de implementar en forma progresiva la historia clínica electrónica, de acuerdo a su disponibilidad presupuestal, y su implementación debe seguir los estándares para la acreditación de su sistema de información de historias clínicas electrónicas ante el RENHICE.

CAPÍTULO IV

CRITERIOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Artículo 28.- Del Ministerio de Salud

El Ministerio de Salud, a través de la Oficina General de Tecnologías de la Información establece los requisitos técnicos respecto a las medidas de seguridad necesarias para proteger y salvaguardar la información contenida en los sistemas de información de historias clínicas electrónicas, en cumplimiento del marco normativo de la seguridad de la información, en coordinación con ONGEI-PCM.

Artículo 29.- De los establecimientos de salud y servicios médicos de apoyo

Con el objeto de proteger la información clínica accedida a través del RENHICE, los establecimientos de salud y servicios médicos de apoyo establecerán en sus sistemas de información, las medidas necesarias que garanticen la seguridad de los mismos para evitar su alteración, pérdida, intercambio y acceso no autorizado, bajo responsabilidad señalada en el literal b) de la séptima disposición complementaria final de la Ley.

Asimismo, cumplirán con las medidas de seguridad exigidas en la Ley N° 29733, Ley de Protección de Datos Personales, su Reglamento aprobado mediante Decreto Supremo N° 003-2013-JUS, su directiva de seguridad de la información aprobada por Resolución Directoral N° 019-2013-JUS-DGPDP y demás normas complementarias que el Ministerio de Salud apruebe.

Artículo 30.- Registro y resguardo de la prestación de servicios de salud

Los sistemas de información de historias clínicas electrónicas deberán de registrar y resguardar la información derivada de la prestación de servicios de salud en forma de documentos electrónicos estructurados e inalterables de acuerdo a la directiva de acreditación de los sistemas de información de historias clínicas electrónicas que apruebe el Ministerio de Salud.

Artículo 31.- De la seguridad en el RENHICE

En relación a los aspectos de seguridad, el RENHICE administrado por el Ministerio de Salud debe implementar para el funcionamiento de los diversos sistemas de información de los establecimientos de salud y servicios médicos de apoyo como mínimo:

- a. Redes privadas virtuales y esquemas de autenticación de la identidad de los profesionales de la salud emitidos por una Entidad de Certificación conforme a lo establecido en la Ley de Firmas y Certificados Digitales, su Reglamento aprobado por el Decreto Supremo N°052-2008-PCM y sus modificatorias.
- b. Mecanismos físicos y tecnológicos necesarios para mitigar los riesgos de pérdida, modificación y/o alteración de la información durante todo el registro y/o acceso a los datos de filiación e información clínica, garantizando la confidencialidad, integridad y disponibilidad de la información.
- c. Guías y formatos técnicos para la implementación del Sistema de Gestión de Seguridad de la Información en los establecimientos de salud y servicios médicos de apoyo, quienes deberán basarse en estos documentos para su implementación.
- d. Otras señaladas en las normas complementarias que el Ministerio de Salud apruebe.

En relación a los establecimientos de salud y servicios médicos de apoyo se debe implementar como mínimo:

- a) Un Sistema de Gestión de Seguridad de la Información de acuerdo a la familia ISO/IEC 27000 adoptadas como Normas Técnicas Peruanas vigentes considerando además las normas en materia de

protección de datos personales conforme a lo señalado en la Ley N° 29733, Ley de Protección de Datos Personales, su Reglamento aprobado mediante Decreto Supremo N° 003-2013-JUS y su directiva de seguridad aprobada por Resolución Directoral N° 019-2013-JUS-DGPDP. Asimismo, deberán considerar los estándares en materia de seguridad de la información, que aseguren la confidencialidad, integridad, disponibilidad, trazabilidad, autenticidad y no repudio de la información clínica contenida en las historias clínicas electrónicas. Para el caso de los establecimientos de salud y servicios médicos de apoyo públicos, sin perjuicio de lo señalado, tienen la obligación de implementar la NTP-ISO/IEC 27001:2014, conforme a lo dispuesto mediante Resolución Ministerial N° 004-2016-PCM o en las normas que hagan sus veces.

b) Los procesos del ciclo de vida de software según lo establecido en la NTP ISO/IEC 12207, y su normatividad vigente.

c) Mecanismos de autenticación, de cifrado y de firma digital conforme a lo establecido en el presente Reglamento y en conformidad con la Ley N° 27269, Ley de Firmas y Certificados Digitales, su Reglamento aprobado mediante Decreto Supremo N° 052-2008-PCM y sus modificatorias.

d) Estrictos controles para proteger la información a la que acceden los profesionales de la salud a través de sus sistemas de información de historias clínicas electrónicas.

e) El acceso exclusivo para el uso de personas explícitamente autorizadas para ello, con el soporte de firmas y certificados digitales, según lo establecido en el presente Reglamento y en conformidad con la Ley N° 27269 — Ley de Firmas y Certificados Digitales, aprobado mediante Decreto Supremo N° 052-2008-PCM y sus modificatorias.

f) Un registro histórico informático de todas las transacciones ocurridas o bloqueadas, lo que posibilitará al Ministerio de Salud tener la trazabilidad de cada registro, pudiéndose evidenciar éstas de manera detallada e indubitable, a través de auditorías a todas las actividades realizadas y por todas las personas intervinientes en la gestión de la información accedida a través del RENHICE.

g) Otras señaladas en las normas complementarias que el Ministerio de Salud apruebe.

Artículo 32.- De la trazabilidad de las modificaciones o actualizaciones

El sistema de información de historias clínicas electrónicas del establecimiento de salud o servicio de apoyo debe permitir registrar y auditar de manera detallada e indubitable todas las modificaciones, actualizaciones, correcciones o tachados realizadas en la historia clínica electrónica, así como la información relativa a la fecha y hora en que se realizó el acceso, al establecimiento de salud o servicio médico de apoyo desde el que se realizó cada acceso, al profesional de salud que accedió a la información clínica, clínica sensible y clínica básica, según sea el caso y a las características de la información clínica accedida.

Artículo 33.- Condiciones específicas sobre la confidencialidad

Las personas autorizadas a acceder al RENHICE deben hacerlo respetando las medidas establecidas para la gestión de la seguridad y confidencialidad de la información, de conformidad con lo que se establezca en la Ley y el presente Reglamento y en otras normas complementarias que apruebe el Ministerio de Salud.

Todas las medidas de confidencialidad establecidas están dirigidas a prestar y garantizar la adecuada atención de salud a los pacientes o usuarios de salud, facilitar a los pacientes o usuarios de salud la información sobre cualquier actuación en el ámbito de su salud, respetar las decisiones adoptadas libre y voluntariamente por el paciente o usuario de salud dentro de los límites permitidos por la legislación peruana, y gestionar y custodiar la información clínica que guarden los sistemas de información de historias clínicas electrónicas.

Todo el personal que interviene directa o indirectamente en el funcionamiento del sistema de información del RENHICE, y en los sistemas de información de historias clínicas electrónicas de cada establecimiento de salud y servicio médico de apoyo, está obligado a guardar cumplimiento de lo dispuesto en la Ley, el presente Reglamento y demás normas complementarias, bajo responsabilidad señalada en el literal b) de la séptima disposición complementaria final de la Ley.

Artículo 34.- Documento de seguridad de la información

Los establecimientos de salud y servicios médicos de apoyo deberán establecer un documento maestro de seguridad de la información que incluya el sistema de información de historias clínicas electrónicas, así como desarrollar y mantener actualizado un documento de compromiso de confidencialidad en el

tratamiento de datos personales aplicable al personal relacionado con el tratamiento de dichos datos, conforme a lo señalado en la Ley N° 29733, Ley de protección de Datos Personales, su norma reglamentaria aprobado mediante Decreto Supremo N° 003-2013-JUS y su directiva de seguridad aprobada por Resolución Directoral N° 019-2013-JUS-DGPDP.

CAPÍTULO V

DE LA INTEROPERABILIDAD DE LOS SISTEMAS DE INFORMACIÓN

Artículo 35.- De los requerimientos para la interoperabilidad

El Ministerio de Salud aprueba la norma complementaria a la que deben sujetarse los sistemas de información de historias clínicas electrónicas de los establecimientos de salud y servicios médicos de apoyo, a fin de garantizar el intercambio, procesamiento, interpretación y seguridad de la información contenida en dichos sistemas.

Los establecimientos de salud y servicios médicos de apoyo deben implementar como mínimo:

- a. Las interfaces de intercambio y protocolos de información, las cuales deberán observar la compatibilidad para su interacción con el RENHICE de acuerdo a lo especificado en la norma del Ministerio de Salud y normatividad vigente.
- b. El equipamiento informático necesario para acceder al Sistema de información de historias clínicas electrónicas, cuando se realice la atención y se requiera consultar la información clínica autorizada por el paciente o usuario de salud en un establecimiento de salud o servicio médico de apoyo distinto al que le brinda dicha atención.
- c. La infraestructura tecnológica que permita conservar y mantener en condiciones adecuadas de operación su sistema de información de historias clínicas electrónicas, para asegurar la integridad, autenticidad y disponibilidad de los datos e información contenidos en el mismo a través del tiempo, así como para el acceso al RENHICE.
- d. Los protocolos de interoperabilidad que el Ministerio de Salud apruebe en las normas complementarias respectivas en coordinación con la ONGEI-PCM.
- e. La seguridad física y lógica para proteger todo componente que interviene en el tratamiento de los datos de filiación y la información clínica del paciente o usuario de salud contenidas en las historias clínicas electrónicas desde su registro.
- f. La interconexión a través de redes privadas virtuales u otros canales seguros para acceder al RENHICE y a la PIDE. Para el caso de Sistemas de Información de Historia Clínicas Electrónicas (SIHCE) compartidos por varios establecimientos de salud o servicios médicos de apoyo, bastará la interconexión vía red privada virtual u otros canales seguros desde el punto donde se centraliza la información.
- g. Otras señaladas en las normas complementarias que el Ministerio de Salud apruebe.

Artículo 36.- De la interoperabilidad en el RENHICE

El Ministerio de Salud en coordinación con la ONGEI determina los requisitos técnicos o tecnológicos que faciliten las disposiciones de intercambio de información, estándares técnicos probados, elaboración de guías, formatos que orientan a los establecimientos de salud y servicios médicos de apoyo para lograr la interoperabilidad semántica e interoperabilidad técnica en escenarios concretos de intercambio de información entre los sistemas de información de historias clínicas electrónicas, a efectos de procurar la compatibilización entre estos con los sistemas de gestión de la seguridad de la información en el ámbito del RENHICE, los cuales serán desarrolladas en una norma complementaria que el Ministerio de Salud apruebe.

CAPÍTULO VI

CARACTERÍSTICAS TÉCNICO INFORMÁTICAS

Artículo 37.- De la firma digital en la historia clínica electrónica

La historia clínica electrónica de un establecimiento de salud o servicio médico de apoyo debe estar soportada por un sistema de información que le permita firmar digitalmente al profesional de salud que brinda la atención.

Artículo 38.- Del sistema de información de historias clínicas electrónicas

El sistema de información de historias clínicas electrónicas de los establecimientos de salud o servicios médicos de apoyo debe estar acreditado para acceder al RENHICE y debe tener la posibilidad de identificar al paciente o usuario de salud y permitir la firma digital tanto del profesional de la salud como del paciente o usuario de salud.

TÍTULO IV

DE LA HISTORIA CLÍNICA ELECTRÓNICA

CAPÍTULO I

DE LA HISTORIA CLÍNICA ELECTRÓNICA

Artículo 39.- Información de la historia clínica electrónica

La historia clínica electrónica contiene los datos de filiación del paciente o usuario de salud, la información clínica y otras que señala la Norma Técnica de la Historia Clínica de los Establecimientos del Sector Salud vigente. El paciente o usuario de salud debe proporcionar sus datos de filiación al abrir o crear una historia clínica electrónica, sujetándose al principio de veracidad.

El paciente o usuario de salud podrá señalar en cada historia clínica electrónica de cada establecimiento de salud en el que reciba la atención el nombre de su representante legal, para los casos en que corresponda.

La información clínica que se encuentra contenida en las historias clínicas electrónicas es registrada por los profesionales de la salud, y refrendada con su firma digital.

Artículo 40.- De los datos de filiación

Los datos de filiación contenidos en la historia clínica electrónica son generados en cada establecimiento de salud al momento de abrir una historia clínica electrónica nueva, y el respectivo sistema informático se apoya en la base del RENIEC para verificar los datos referidos a nombres y apellidos del paciente o usuario de salud, y el número de su documento nacional de identidad - DNI. Los demás datos de filiación son obtenidos de la información directa que brinda el paciente o usuario de salud o su representante legal, según corresponda.

Los datos de filiación contenidos en las historias clínicas electrónicas únicamente se pueden modificar o actualizar en el establecimiento de salud o servicio médico de apoyo donde se generaron, y exclusivamente a solicitud del paciente o usuario de salud.

Artículo 41.- De la información clínica

La información clínica contenida en las historias clínicas electrónicas que registra el profesional de la salud que atiende al paciente se realiza a través del sistema de información de historias clínicas electrónicas del establecimiento de salud o servicio médico de apoyo y es refrendada con la firma digital de dicho profesional de la salud.

La información clínica tiene dentro de su contenido a la denominada información clínica sensible y la información clínica básica.

En caso que el profesional de la salud que atiende necesite acceder a la información clínica de su paciente o usuario de salud, contenida en las historias clínicas electrónicas de otros establecimientos de salud o servicios médicos de apoyo diferentes del que le brinda la atención, debe solicitar la autorización de acceso a dicho paciente o usuario de salud.

El paciente o usuario de salud, de estimarlo pertinente, puede autorizar el acceso del profesional de la salud a dichas historias clínicas electrónicas a través del mecanismo de autenticación señalado en el artículo 74 del presente Reglamento.

La autorización de acceso brindada por el paciente o usuario de salud, debe ser otorgada conforme a lo establecido en el artículo 62 del presente Reglamento.

El acceso del profesional de la salud a la información clínica de su paciente o usuario de salud, contenida en las historias clínicas electrónicas de otros establecimientos de salud o servicios médicos de apoyo diferentes al que le brinda la atención, es únicamente para visualización o lectura.

Artículo 42.- De la información clínica sensible

La información clínica sensible será determinada por el paciente o usuario de salud, para lo cual deberá indicarlo a través del sistema de información de las historias clínicas electrónicas del establecimiento de salud o servicio médico de apoyo donde recibió la atención.

El profesional de la salud que atiende accede a la información clínica sensible contenida en los sistemas de información de historias clínicas electrónicas del establecimiento de salud o servicio médico de apoyo donde se produce la atención. Para el caso en que éste necesite visualizar o leer la información clínica sensible contenida en las historias clínicas electrónicas de otros establecimientos de salud o servicios médicos de apoyo distintos del que brinda la atención, se requiere que el paciente o usuario de salud le brinde su autorización de acceso, según lo dispuesto por el artículo 63 del presente Reglamento.

Artículo 43.- De la información clínica básica

En situación de emergencia o cuando dada su condición, el paciente no pueda autorizar el acceso a sus historias clínicas electrónicas y no se cuente con representante legal autorizado, el profesional de la salud médico que lo atiende podrá acceder, únicamente, a la información clínica básica contenida en aquellas. El profesional de salud que atiende asume la responsabilidad de dicho acceso, por lo que debe valorar si es imprescindible para el tratamiento de la emergencia.

El sistema de información de historias clínicas electrónicas de cada establecimiento de salud o servicio médico de apoyo debe permitir identificar la información clínica básica, para que el RENHICE pueda visualizar o leer aquella que proviene de todas las historias clínicas electrónicas del mismo paciente o usuario de salud, y ponerla a disposición del profesional de salud autorizado que la solicita y que atiende la emergencia.

CAPÍTULO II

ACTUALIZACIÓN Y MODIFICACIÓN DEL CONTENIDO DE LA HISTORIA CLÍNICA ELECTRÓNICA

Artículo 44.- Obligatoriedad de atender la solicitud de los pacientes o usuarios de salud

Los establecimientos de salud o servicios médicos de apoyo son responsables de atender las solicitudes planteadas por los pacientes o usuarios de salud en referencia a sus historias clínicas electrónicas, para actualizar o corregir información errada, así como de la determinación de la procedencia o no de dicha solicitud; para lo cual deberán responder en la forma y plazo propuesto para cada derecho, según lo establecido en la Ley N° 29733, Ley de Protección de Datos Personales y su Reglamento aprobado por Decreto Supremo N° 003-2013-JUS. La actualización o corrección solicitada se realiza en el marco de lo dispuesto en el presente Reglamento y por el Ministerio de Salud en las normas complementarias que apruebe.

Artículo 45.- De la actualización de información susceptible de modificación o corrección

Los datos de filiación del paciente o usuario de salud, contenidos en las historias clínicas electrónicas que sean actualizables o susceptibles de actualización, o corrección, se procesarán únicamente en el establecimiento de salud o servicio médico de apoyo que la generó, solamente a solicitud del paciente o usuario de salud y bajo su responsabilidad.

El establecimiento de salud o servicio médico de apoyo atenderá lo solicitado, únicamente si el paciente o usuario de salud tiene fundamentada razón.

El sistema de información de historias clínicas electrónicas debe mantener registro de lo solicitado, y lo resuelto respecto a lo actualizado o corregido, los cambios realizados de ser el caso, y la persona que autorizó hacerlo. El sistema de información debe permitir la completa trazabilidad de lo actuado.

Artículo 46.- Prohibición de modificación de la información clínica de la historia clínica electrónica

Los establecimientos de salud y servicios médicos de apoyo, así como su personal profesional o técnico, administrativo o asistencial, están prohibidos de modificar el contenido de la información clínica de las historias clínicas electrónicas, a través de sus sistemas de información o de alguna otra forma, bajo responsabilidad.

Los establecimientos de salud y servicios médicos de apoyo son responsables de que los datos e información contenidos en sus sistemas de información de historias clínicas electrónicas para la prestación de servicios de salud permanezcan completos e inalterados.

No se puede modificar la información clínica de la historia clínica electrónica de un registro hecho anteriormente aduciendo que no refleja la realidad actual.

Artículo 47.- Actualización o modificación autorizada de la historia clínica electrónica

La información de las historias clínicas electrónicas solamente podrá ser modificada o actualizada en los establecimientos de salud y servicios médicos de apoyo donde fue generada, en las condiciones siguientes:

- a) Actualización de los datos de filiación, a solicitud del paciente o usuario de salud, quien tiene la carga de la prueba.
- b) Modificación de la información clínica, a solicitud del paciente o usuario de salud, cuando éste haya detectado alguna información errónea o ajena a la verdad, y requiere que el profesional de la salud que hizo el registro acepte hacer la modificación solicitada.
- c) Cuando el profesional de la salud que atiende detecta un error material en su registro de la atención procederá hacer la corrección como un registro nuevo, precisando la ubicación del error. Esto no aplica para los diagnósticos ni omisión de registro.

En caso que el profesional de la salud que hizo el registro no acepte hacer la modificación solicitada, o no sea ubicable, el paciente o usuario de salud puede solicitar que se deje constancia en la atención actual, su acotación respecto al dato que él considera errado y que solicita sea modificado.

En caso de ser información clínica debe mantenerse mandato de conservación del dato anterior con indicación de la nueva data introducida y la anterior modificada. No procede la actualización de la información que fue registrada como información clínica por el médico tratante en el momento de la atención.

TÍTULO V

USUARIOS DEL RENHICE

CAPÍTULO I

DE LOS USUARIOS DEL RENHICE

Artículo 48.- De los pacientes o usuarios de salud

Los pacientes o usuarios de salud tienen derecho a solicitar al establecimiento de salud o servicio médico de apoyo, responsable del sistema de información de historias clínicas electrónicas, que verifique su condición de registrado en éste o si contiene algún tipo de información concerniente a él.

Los pacientes o usuarios de salud pueden realizar, a través del sistema de información del RENHICE y de los sistemas de información de historias clínicas electrónicas del establecimiento de salud o servicio médico de apoyo donde se atiende, el seguimiento de los accesos realizados por los profesionales de la salud a la información clínica contenida en sus historias clínicas electrónicas a través de la fecha y hora del acceso, el establecimiento de salud o servicio médico de apoyo que realizó el acceso, el profesional de la salud que accedió y el tipo de información accedida, a fin de verificar la legitimidad de estos.

La consulta a todas sus historias clínicas electrónicas en los establecimientos de salud o servicios médicos de apoyo, en los que haya sido atendido, podrá ser hecha a través del portal que el Ministerio de Salud disponga para tal fin y con los mecanismos que permitan la confidencialidad, seguridad, integridad y disponibilidad de la información.

El paciente o usuario de salud podrá acceder a través del sistema de información del RENHICE, con su debida identificación y mediante los mecanismos de autenticación de la identidad establecidos en el Título VI Capítulo I del presente Reglamento.

Artículo 49.- Del representante Legal

La representación legal a la que se hace referencia en el presente artículo y en el presente Reglamento está relacionada únicamente al acceso a las historias clínicas electrónicas a través del sistema de información del establecimiento de salud o servicio médico de apoyo y del RENHICE, y para autorizar el acceso a los profesionales de la salud que atienden a su representado.

El representante legal del paciente o usuario de salud tendrá los mismos derechos y obligaciones que éste, siempre que cumpla con haber sido consignada su calidad de representante legal en el sistema de información de cada establecimiento de salud o servicio médico de apoyo donde se atienda el paciente o usuario de salud, y éste fuera menor de edad o tuviera impedimento legal para ejercer el derecho por sí mismo.

Para el caso de los menores de edad y los incapaces, la representación legal se ejerce según el mandato que señala el Código Civil en el artículo 45.

El paciente o usuario de salud con plena capacidad de ejercicio de sus derechos civiles podrá designar a su representante legal para este fin, de estimarlo pertinente, en cada establecimiento de salud o servicio médico de apoyo donde acuda para la atención, para que lo represente en caso que por razones de salud no pudiera ejercerlo por sí mismo.

En caso no lo indique, y se requiera dicha información por encontrarse en situación de emergencia, o inconsciente o en riesgo de morir, podrá ser representado en forma excluyente y en el siguiente orden por:

- a) Pareja, cónyuge o concubino
- b) Descendientes mayores de edad
- c) Ascendientes
- d) Hermanos

El representante legal del paciente o usuario de salud tiene acceso a la información clínica de este, de acuerdo a lo establecido en el presente artículo, y según lo que señale la ley, el presente Reglamento y demás normas complementarias, siempre que dicha información clínica esté disponible a través del RENHICE.

Artículo 50.- Profesionales de salud en atención directa y atención de soporte

Los profesionales de salud que laboran en una unidad productora de servicios de salud de atención directa acceden a la historia clínica electrónica de sus pacientes mediante el mecanismo de autenticación de la identidad señalado en el presente Reglamento y, deben firmar digitalmente mediante su certificado digital la información registrada en la historia clínica electrónica.

Para acceder a la historia clínica electrónica del establecimiento de salud o servicio médico de apoyo, los profesionales de salud que brindan atención de soporte lo realizan por el sistema de información de las historias clínicas electrónicas del mismo establecimiento de salud o servicio médico de apoyo, al que acceden mediante un mecanismo de autenticación de la identidad y únicamente a la información clínica correspondiente a su profesión, salvo que el paciente o usuario de salud no desee restringirlo en estos términos.

Los profesionales de salud son responsables de los registros que hacen en la historia clínica electrónica de los pacientes a los que atienden.

Para acceder a las historias clínicas electrónicas del paciente o usuario de salud, a través del RENHICE en otros establecimientos de salud o servicios médicos de apoyo, diferente a aquel en el que se atiende, los profesionales de salud que brindan atención directa como el médico, obstetra u odontólogo, podrán hacerlo a través del sistema de información de historias clínicas electrónicas del establecimiento de salud o servicio médico de apoyo, con su debida identificación y mediante los mecanismos de autenticación de la identidad establecidos en el Título VI Capítulo I del presente Reglamento, previa autorización expresa del paciente o usuario de salud, o su representante legal, según corresponda. Este acceso será únicamente para visualización o lectura.

Artículo 51.- Registro del acceso de los profesionales de la salud

Todos los accesos realizados por los profesionales de la salud al RENHICE y a la información disponible a través de éste, serán registrados y estarán disponibles para los procedimientos de verificación y trazabilidad, debiendo permitir identificar de manera indubitable a la persona que lo realiza, el sistema de información utilizado, la ubicación desde donde se accede, la fecha y la hora de acceso, y las acciones realizadas.

Los procedimientos pertinentes para tal fin los establece el Ministerio de Salud en la norma complementaria correspondiente.

Artículo 52.- De los alcances de la autorización de acceso otorgada para acceder al RENHICE

Cuando el médico tratante haya obtenido la autorización de acceso explícito y expreso del paciente o usuario de salud o de su representante legal a través de un formulario refrendado con firma digital o cualquier otro mecanismo de autenticación que garantice la voluntad inequívoca de éste, podrá acceder a través del RENHICE a las historias clínicas electrónicas de dicho paciente, debiendo mantener la reserva y el secreto profesional respecto a la información a la que accede.

El acceso autorizado a las historias clínicas electrónicas a través del RENHICE debe respetar el tiempo establecido en el artículo 67 del presente Reglamento.

CAPÍTULO II

DERECHOS DEL PACIENTE O USUARIO DE SALUD

Artículo 53.- Titularidad y propiedad de las historias clínicas electrónicas

El paciente o usuario de salud es el titular de su historia clínica electrónica en tanto es el propietario de su información clínica allí contenida.

El establecimiento de salud o servicio médico de apoyo es el propietario de las historias clínicas electrónicas y del sistema de información de historias clínicas electrónicas acreditado ante el RENHICE; y por tanto tiene la responsabilidad de conservar, custodiar y garantizar la seguridad de estas y de la información allí contenida.

Artículo 54.- Responsabilidad del establecimiento de salud o servicio médico de apoyo de informar al paciente o usuario de salud

Cada establecimiento de salud o servicio médico de apoyo que cuente con un sistema de información acreditado de historias clínicas electrónicas es responsable de informar al paciente o usuario de salud que el establecimiento se encuentra incorporado al RENHICE, por lo que su documento nacional de identidad, los códigos del Registro Nacional de IPRESS, o el que haga sus veces, de los establecimientos en que se atendió y su historia clínica electrónica si es que lo autoriza expresamente, estarán en dicho registro; pero además que el acceso a sus historias clínicas electrónicas y su información clínica únicamente podrá ser visible siempre y cuando el paciente o usuario de salud lo autorice expresamente, usando los mecanismos de autenticación de la identidad establecidos en el Título VI, Capítulo I del presente Reglamento.

Dicha información debe incluir también a las excepciones de reserva de la información que establece la Ley N° 26842, Ley General de Salud, y la responsabilidad que asume el paciente o usuario de salud en los resultados de la asistencia médica recibida, cuando este decide limitar el acceso a todo o parte de su información clínica sensible contenida en sus historias clínicas electrónicas a su médico tratante.

Artículo 55.- Derecho de información

Los pacientes o usuarios de salud tienen el derecho a solicitar a cualquier establecimiento de salud o servicio médico de apoyo que le informen si su historia clínica electrónica ha sido incluida por el establecimiento de salud o servicio médico de apoyo en el RENHICE. Este derecho incluye a toda persona que considere que necesita ser informado sobre este aspecto independiente de que sea o no paciente o usuario de salud del establecimiento de salud o servicio médico de apoyo. El acceso a la información solicitada está referido únicamente a la misma persona solicitante.

Artículo 56.- Derecho de acceso

Los pacientes o usuarios de salud tienen el derecho de acceder a la información clínica contenida en sus historias clínicas electrónicas a través del sistema de información del RENHICE aplicando los mecanismos establecidos en la Ley, el presente Reglamento y las normas complementarias que el Ministerio de Salud apruebe. Asimismo, es parte del ejercicio de ese derecho el poder imprimir, copiar, descargar a un dispositivo de almacenamiento local, entre otras, la información clínica contenida en sus historias clínicas electrónicas o parte de ellas, para lo cual el sistema de información del RENHICE le permitirá hacerlo en formato que asegure que no se podrá modificar ni alterar el contenido.

Tales acciones deberán quedar registradas en el sistema de información del RENHICE conforme a los criterios de seguridad y trazabilidad señalados en el Título III, Capítulo IV del presente Reglamento.

Artículo 57.- Acceso a la información clínica a través del sistema de información de historias clínicas electrónicas

Para que los médicos tratantes accedan a la información clínica a través del RENHICE, esta se podrá realizar únicamente a través del sistema de información de historias clínicas electrónicas de los establecimientos de salud o servicios médicos de apoyo donde se produce la atención y siempre que el paciente o usuario de salud brinde su autorización de acceso a éste, conforme a lo establecido en el artículo 62 del presente Reglamento.

El profesional de la salud no está facultado a que la información clínica visualizada sea impresa, copiada, capturada o descargada a cualquier dispositivo de almacenamiento local, entre otros.

Artículo 58.- Derecho de oposición

El paciente o usuario de salud puede negarse a que una o todas sus historias clínicas electrónicas en diferentes establecimientos de salud o servicios médicos de apoyo sean accedidas a través del RENHICE, en alguna circunstancia, sin necesidad de expresar motivación alguna, bajo su responsabilidad.

Artículo 59.- Derecho a limitar el acceso a parte de su información clínica sensible a través del RENHICE

El paciente o usuario de salud tiene derecho a que la información clínica sensible contenida en las historias clínicas electrónicas a las que se accede a través del RENHICE, no sea visualizada o leída por el profesional de la salud, bajo ningún mecanismo. Tal decisión de ocultar o limitar el acceso podrá ser ejercida a iniciativa expresa del paciente o usuario de salud, y revertida o revocada por el propio paciente o usuario de salud en el momento que este así lo disponga.

El sistema de información de historias clínicas electrónicas deberá advertir al paciente o usuario de salud de las consecuencias negativas que dicha acción puede ocasionarle por condicionar la toma de decisiones del profesional de la salud, que debe realizar el proceso diagnóstico y terapéutico sin contar con toda la información existente.

Este derecho no implica que dicha información sea eliminada de la historia clínica electrónica, sino que queda oculta.

La información clínica sensible ocultada deberá ser advertida a través del sistema de información de historias clínicas electrónicas al profesional de la salud en la atención que le brinde al paciente o usuario de salud. Dicha advertencia no implica la especificación del tipo de información clínica sensible ocultada.

El profesional de la salud, durante la atención, podrá informar al paciente o usuario de salud la trascendencia que tiene conocer dicha información sensible ocultada, para que este la desproteja, si así lo decide.

CAPÍTULO III

AUTORIZACIÓN DE ACCESO DEL

PACIENTE O USUARIO DE SALUD A

LA HISTORIA CLÍNICA ELECTRÓNICA

Artículo 60.- Reglas de autorización de acceso

En el establecimiento de salud se realiza la primera autorización de acceso dado por el paciente o usuario de salud, conforme a lo señalado en la Ley N° 29733, Ley de Protección de Datos Personales, y su Reglamento aprobado mediante Decreto Supremo N° 003-2013-JUS, cuando se crea o apertura una historia clínica electrónica en el sistema de información de historias clínicas electrónicas del establecimiento de salud o servicio médico de apoyo al que acude para la atención. Dicha autorización de acceso debe ser entendida tanto para acceder a los datos de filiación e información clínica como para la información clínica sensible, por los profesionales de la salud que lo atienden directamente en dicho establecimiento de salud.

En el RENHICE se realiza la segunda y tercera autorización de acceso. La segunda regla es para que el profesional de la salud que lo atiende, acceda a la lectura de la información clínica contenida en las historias clínicas electrónicas del mismo paciente o usuario de salud a través del RENHICE, y que fueron generadas en otro establecimiento de salud o servicio médico de apoyo distinto al que le brinda la atención en ese momento. Esta autorización de acceso no incluye a la información clínica sensible en ningún caso.

La tercera autorización de acceso es para la lectura de la información clínica sensible contenida en las historias clínicas electrónicas del mismo paciente o usuario de salud a través del RENHICE, y que fueron generadas en otro establecimiento de salud o servicio médico de apoyo distinto al que le brinda la atención en ese momento; para lo cual éste o su representante legal deben brindar la autorización de acceso de manera expresa, si lo estima necesario conforme a lo señalado en el artículo 62 del presente Reglamento. La autorización de acceso podrá ser para todas las historias clínicas electrónicas o seleccionar alguna de ellas, según lo que el paciente o usuario de salud decida.

Es facultad del Ministerio de Salud normar las demás consideraciones relacionadas a las reglas de autorización de acceso que el paciente o usuario de salud debe brindar al profesional de la salud.

Artículo 61.- Acceso a través del RENHICE

Para visualizar o leer la historia clínica electrónica del paciente o usuario de salud, de otros establecimientos de salud o servicios médicos de apoyo, el profesional de la salud deberá acceder a través del sistema de información de historias clínicas electrónicas del establecimiento de salud o servicio médico de apoyo al RENHICE, cumpliendo con lo señalado en el artículo 60 del presente Reglamento.

El paciente o usuario de salud tiene acceso a su información clínica a través del sistema de información del RENHICE según lo establecido en la Ley, el presente Reglamento y demás normas complementarias. Para tal fin el paciente o usuario de salud debe autenticar debidamente su identidad mediante los mecanismos señalados en el Título VI Capítulo I del presente Reglamento.

Artículo 62.- La autorización de acceso a la información clínica contenida en las historias clínicas electrónicas

El acceso a la información clínica contenida en una o todas las historias clínicas electrónicas a través del RENHICE por el profesional de la salud debe ser autorizado por el paciente o usuario de salud o su representante legal de manera expresa. La voluntad del paciente debe quedar consignada en un formulario de autorización de acceso que deberá estar refrendado mediante su firma digital o cualquier otro mecanismo de autenticación que garantice dicha voluntad.

El contenido del formulario de la autorización de acceso que brinda el paciente o usuario de salud debe incluir la información establecida para cumplir con el requisito de consentimiento conforme a lo señalado en la Ley N° 29733, Ley de Protección de Datos Personales y su Reglamento aprobado mediante Decreto Supremo N° 003-2013-JUS.

Artículo 63.- Condiciones para acceder a la información clínica sensible

En caso de ser necesario para el profesional de salud acceder a través del RENHICE a la lectura de la información clínica sensible del paciente o usuario de salud, contenida en las historias clínicas electrónicas de otros establecimientos de salud o servicios médicos de apoyo, éste debe brindar la autorización de acceso señalada en el artículo 62 y de acuerdo a las reglas de autorización de acceso dispuesta en el artículo 60 del presente Reglamento.

Artículo 64.- Acceso y estado de inconciencia

En situación de grave riesgo para la vida o la salud de un paciente o usuario de salud, cuyo estado no permita la capacidad de autorizar el acceso a sus historias clínicas electrónicas, y no estuviera su representante legal, el profesional de la salud podrá acceder, a través del sistema de información de las

historias clínicas electrónicas del establecimiento de salud o servicio médico de apoyo al RENHICE, a la información clínica básica contenida en las historias clínicas electrónicas del paciente, con fines de diagnóstico y tratamiento médico o quirúrgico. El profesional de la salud asume la responsabilidad de dicho acceso, por lo que debe valorar si es imprescindible para el tratamiento de la emergencia.

Artículo 65.- Casos excepcionales de menores de edad

En casos de urgencia o emergencia de un paciente o usuario de salud menor de edad, ante la ausencia de los titulares de la patria potestad o tutores, según corresponda, el profesional de la salud podrá acceder a la información clínica básica a través del sistema de información de las historias clínicas electrónicas del establecimiento de salud o servicio médico de apoyo al RENHICE, en función del interés superior del niño. El profesional de la salud asume la responsabilidad de dicho acceso, por lo que debe valorar si es imprescindible para el tratamiento de la emergencia.

Artículo 66.- Personas intervinientes en la gestión de la información accedida a través del RENHICE

Las personas responsables de la gestión de la información contenida y accesible a través del RENHICE y quienes intervengan en cualquiera de las actividades de gestión de la misma, están sometidas al secreto profesional y a mantener confidencialidad, el cual persistirá, aunque finalice su contrato laboral en estas dependencias o cualquier otra relación jurídica o de hecho que haya amparado su participación.

El cumplimiento de este deber no debe limitar el acatamiento de los protocolos, registros, informes, estadísticas y demás documentación que guarde relación con los procesos clínicos en que intervienen los autorizados a acceder al RENHICE.

Artículo 67.- Temporalidad de la autorización a través del RENHICE

El acceso autorizado al profesional de la salud que atiende para visualizar o leer las historias clínicas electrónicas del paciente o usuario de salud a través del RENHICE, caduca obligatoriamente al terminar la atención o cumplido un periodo de tiempo máximo que no debe exceder de los cuarenta (40) minutos, lo que ocurra primero. La necesidad de un nuevo acceso requiere de una nueva autorización del paciente o usuario de salud.

Artículo 68.- Revocatoria de autorización de acceso

La autorización de acceso dado al profesional de la salud podrá ser revocada por el paciente o usuario de salud o su representante legal, en el momento que lo estime pertinente, en el sistema de información de historias clínicas electrónicas del establecimiento de salud o servicio médico de apoyo donde se atiende, sin que deba expresar la motivación, y mediante los mecanismos informáticos que apruebe el Ministerio de Salud en una norma complementaria.

CAPÍTULO IV

RESTRICCIÓN DE ACCESO AL RENHICE

Artículo 69.- Suspensión de acceso al RENHICE del profesional de la salud

El Ministerio de Salud, en su calidad de administrador del RENHICE está facultado a suspender el acceso a determinados profesionales de la salud cuando se compruebe el incumplimiento de la Ley, el presente Reglamento y demás normas complementarias.

La suspensión de acceso al RENHICE del profesional de la salud podrá ser temporal o definitiva según corresponda. Esta suspensión no implica la inhabilitación del ejercicio profesional.

Además, procederá a suspender el acceso temporal o permanente a aquellos profesionales de la salud cuyos respectivos colegios profesionales los hayan suspendido en el ejercicio de su profesión, por lo que dichas entidades están obligadas a comunicarlo a la Autoridad Nacional de Salud de manera inmediata bajo responsabilidad establecida en el literal b) de la séptima disposición complementaria final de la Ley.

Artículo 70.- Suspensión de acceso al RENHICE del paciente o usuario salud

El Ministerio de Salud suspenderá el acceso dado a un paciente o usuario de salud en los siguientes casos:

a. Muerte del paciente o usuario de salud,

b. Declaración de incapacidad legal del paciente o usuario de salud y que no cuente con su representante legal conforme a los criterios señalados en el artículo 49 del presente Reglamento.

Artículo 71.- Denegación de acceso de forma temporal de un usuario del RENHICE

El Ministerio de Salud puede denegar el acceso al RENHICE de forma temporal a un paciente o usuario de salud o a su representante legal, y a un profesional de la salud, si comprueba o tiene indicios razonables de un acceso no autorizado o no consentido, o cuando exista un acceso autorizado y consentido pero con fines distintos a los señalados en la Ley, el presente Reglamento y demás normas complementarias o existen indicios de la comisión de delitos contra la intimidad de los pacientes o usuarios de salud, conforme a lo establecido en los artículos 154A y 157 del Código Penal. Estas personas podrán estar sujetas al inicio de acciones administrativas, civiles y/o penales que correspondan conforme al marco jurídico vigente.

La denegación será por el plazo necesario para subsanar o aclarar los acontecimientos que originaron la misma.

La denegación de acceso al RENHICE no implica que el paciente o usuario de salud no pueda acceder a sus historias clínicas electrónicas directamente en cada uno de los establecimientos de salud o servicio médico de apoyo donde se haya atendido.

Artículo 72.- Denegación de acceso de forma permanente de un usuario del RENHICE

El Ministerio de Salud puede denegar de manera permanente el acceso a un usuario del RENHICE, si comprueba que, de manera dolosa, ha cometido acciones que ponen o podrían haber puesto en grave riesgo o peligro la seguridad, disponibilidad del servicio, integridad y la confidencialidad de la información contenida o accesible a través del RENHICE. Estas personas podrán estar sujetas al inicio de acciones administrativas, civiles y/o penales que correspondan conforme al marco jurídico vigente.

La denegación de acceso al RENHICE no implica que el paciente o usuario de salud no pueda acceder a sus historias clínicas electrónicas directamente en cada uno de los establecimientos de salud o servicio médico de apoyo donde se haya atendido.

TÍTULO VI

MECANISMOS DE AUTENTICACIÓN DE LA IDENTIDAD Y FIRMA DIGITAL

CAPÍTULO I

DE LA AUTENTICACIÓN DE LA IDENTIDAD Y FIRMA DIGITAL

Artículo 73.- Mecanismos de autenticación de la identidad del paciente o usuario de salud

La autenticación de la identidad del paciente o usuario de salud o su representante legal es para que reciba la atención de salud correspondiente, para que el paciente o su representante legal otorguen la autorización de acceso al profesional de la salud o para el acceso del paciente o su representante legal al RENHICE.

Corresponderá a los establecimientos de salud y los servicios médicos de apoyo públicos, privados o mixtos integrar el presente procedimiento de autenticación de la identidad del paciente o usuario de salud o su representante legal con el sistema de información de historias clínicas electrónicas, conforme a lo que señala el presente Reglamento y las normas complementarias que apruebe el Ministerio de Salud.

Artículo 74.- Autenticación de la identidad del paciente o usuario de salud para la atención de salud

Para la atención de salud, el paciente o usuario de salud deberá autenticar su identidad, considerando los siguientes mecanismos:

Nacionales

- a. Autenticación biométrica mediante el uso del aplicativo Match OnCard del documento nacional de identidad electrónico - DNIe.
- b. Autenticación digital mediante el correspondiente certificado digital para persona natural contenido en el documento nacional de identidad electrónico - DNIe.
- c. Y otro que se establezca conforme a lo señalado en el artículo 8 de la Ley.

Extranjeros residentes o en tránsito:

Autenticación a través de Carné de Extranjería que emite el Ministerio del Interior para extranjeros residentes, o del Pasaporte o Documento de Identidad Extranjero para los extranjeros en tránsito; y de una clave generada por el Ministerio de Salud.

Artículo 75.- Autenticación de la identidad y firma digital para que el paciente o usuario de salud autorice el acceso desde el establecimiento de salud o servicio médico de apoyo donde se atiende

Para que el paciente o usuario de salud o su representante legal otorgue la autorización de acceso a sus historias clínicas electrónicas a través del RENHICE desde el establecimiento de salud donde se atiende, deberá autenticar su identidad mediante el documento nacional de identidad electrónico - DNIE a través del correspondiente certificado digital para persona natural contenido en este.

Luego especificará, en el formulario de autorización de acceso, a qué historias clínicas electrónicas le autoriza a acceder, debiendo firmar digitalmente dicha autorización, o usar cualquier otro mecanismo de autenticación que garantice la voluntad inequívoca de éste con su DNIE.

Artículo 76.- Autenticación de la identidad para que el paciente o usuario de salud acceda a sus historias clínicas electrónicas a través del RENHICE

Para que el paciente o usuario de salud o su representante legal acceda a sus historias clínicas electrónicas directamente a través del RENHICE, utilizará la autenticación digital mediante el correspondiente certificado digital para persona natural contenido en el documento nacional de identidad electrónico – DNIE u otros que se determinen de acuerdo a la normatividad vigente.

Artículo 77.- Mecanismos de autenticación de la identidad del profesional de la salud

La autenticación de la identidad de los profesionales de salud para acceder al sistema de información de historias clínicas electrónicas del establecimiento de salud o servicio médico de apoyo, se realizará mediante su certificado digital, el cual debe ser emitido de conformidad con la Ley N° 27269, Ley de Firmas y Certificados Digitales, su Reglamento aprobado mediante Decreto Supremo N° 052-2008-PCM y sus modificatorias.

El certificado digital respectivo debe tener las funciones de autenticación y de firma.

La autenticación del profesional de la salud se realizará por medio del certificado digital contenido en su DNIE o el certificado digital entregado por el establecimiento de salud o servicio médico de apoyo donde preste servicios.

Artículo 78.- Firma digital del profesional de la salud en la historia clínica electrónica

Para firmar digitalmente la historia clínica electrónica, el profesional de la salud adscrito a su establecimiento de salud utilizará el certificado digital contenido en el DNIE o el entregado por el establecimiento de salud y/o servicio médico de apoyo.

CAPÍTULO II

DE LA PARTICIPACIÓN DEL RENIEC

Artículo 79.- Financiamiento de los servicios que preste el Registro Nacional de Identificación y Estado Civil – RENIEC

El Registro Nacional de Identificación y Estado Civil – RENIEC incluirá en su presupuesto anual los costos operativos de la autenticación de la identidad de los pacientes o usuarios de salud, así como del personal de la salud involucrados en el funcionamiento del RENHICE, de manera que se asegure su implementación.

Para la determinación del presupuesto anual a ser financiado por el Estado a través del marco normativo correspondiente, el RENIEC, sobre la base de la información proporcionada por el Ministerio de Salud, determinará la cantidad de consultas de autenticación proyectadas de los establecimientos de salud y servicios médicos de apoyo de acuerdo a las modalidades previstas de autenticación, autenticación digital, biométrica o consultas en línea. Lo cuantificado por el RENIEC deberá incluirlo en la programación y formulación de su presupuesto anual.

**TÍTULO VII
DECLARACIÓN DE INTERÉS NACIONAL**

CAPÍTULO I

DE LA DECLARACIÓN DE INTERÉS NACIONAL

Artículo 80.- De la Declaración de interés nacional

En tanto la implementación de RENHICE ha sido declarada de interés nacional, el Ministerio de Salud y las entidades públicas relacionadas dispondrán en su presupuesto anual del financiamiento necesario para el cumplimiento de lo establecido por la Ley y el presente Reglamento.

CAPÍTULO II

DE LA IMPLEMENTACIÓN

Artículo 81.- Normas complementarias para la implementación del RENHICE y de los sistemas de información de historias clínicas electrónicas

El Ministerio de Salud establecerá las normas complementarias para la implementación del RENHICE, de los sistemas de información de historias clínicas electrónicas de los establecimientos de salud o servicios médicos de apoyo, y para la temporalidad de los plazos para lo que estime pertinente.

Artículo 82.- Disponibilidad de recursos necesarios para la implementación

El Director médico o el responsable de la atención de salud de los establecimientos de salud o servicios médicos de apoyo asegurarán la disponibilidad de recursos necesarios para la implementación de lo dispuesto en el presente Reglamento.

Artículo 83.- Implementación del identificador de la Historia Clínica

La implementación del identificador de la Historia Clínica será gradual y progresiva en el establecimiento de salud o servicio médico de apoyo, la misma que debe realizarse Cuando se apertura una historia clínica electrónica por primera vez.

El identificador que se usa para los pacientes o usuarios nacionales es el número del Documento Nacional de Identidad – DNI emitido por el Registro Nacional de Identificación y Estado Civil – RENIEC; en el caso de los extranjeros residentes, el carnet de extranjería que emite la Superintendencia Nacional de Migraciones; y, para los extranjeros en tránsito, el pasaporte o el documento de identidad extranjero.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera.- Del grupo de trabajo responsable del Ministerio de Salud

El Ministerio de Salud conforma en un plazo máximo de 15 días hábiles después de la publicación del presente Reglamento, un grupo de trabajo responsable de elaborar el plan de implementación del RENHICE, donde se definan las condiciones, los requerimientos, entre otros que demande su implementación.

Segunda.- Normas complementarias para la implementación del RENHICE

El Ministerio de Salud emitirá los documentos normativos correspondientes a la acreditación de los sistemas de información de historias clínicas electrónicas, la autenticación de la identidad del usuario del RENHICE, las medidas de seguridad referida a los aspectos técnicos y organizacionales del RENHICE, y demás que se consideren pertinentes, las cuales deberán observar los mandatos relativos a seguridad establecidos en el presente Reglamento, lo establecido en la Ley N° 29733, Ley de Protección de Datos Personales, su Reglamento aprobado mediante Decreto Supremo N° 003-2013-JUS y su Directiva de Seguridad de la Información aprobada por Resolución Directoral N° 019-2013-JUS-DGPDP, o la que haga sus veces, así como la Ley N° 27269, Ley de Firmas y Certificados Digitales, su Reglamento aprobado mediante Decreto Supremo N° 052-2008-PCM y sus modificatorias, NTP ISO/IEC N° 12207 Procesos del ciclo de vida de software, NTP ISO/IEC N° 27001:2014 Sistema de gestión de seguridad de la información, entre otras normas.

Tercera.- Participación de SUSALUD

SUSALUD, en el marco de sus competencias, supervisará el cumplimiento de las obligaciones contenidas en el presente Reglamento en los establecimientos de salud o servicios médicos de apoyo referidas a la atención de salud.

DISPOSICIONES COMPLEMENTARIAS TRANSITORIAS

Primera.- Autenticación de la identidad del paciente o usuario de salud para la atención de salud

En tanto no se implemente en su totalidad el documento nacional de identidad electrónico –DNIE o no se cuente con los mecanismos o dispositivos necesarios para la autenticación de la identidad a través del DNIE, la autenticación de la identidad del paciente o usuario de salud para la atención de salud en los establecimientos de salud o servicios médicos de apoyo que cuenten con un sistema de información de historias clínicas electrónicas será mediante uno de los siguientes mecanismos:

- a) Documento nacional de identidad vigente y una contraseña que el Ministerio de Salud le proporcione, o
- b) Documento nacional de identidad vigente y servicio de autenticación biométrica de RENIEC.

Segunda.- Autenticación de la identidad para que el paciente o usuario de salud autorice el acceso a sus historias clínicas electrónicas a través del RENHICE desde el establecimiento de salud o servicio médico de apoyo

En tanto no se implemente en su totalidad el documento nacional de identidad electrónico – DNIE o no se cuente con los mecanismos o dispositivos necesarios para la autenticación de la identidad a través del DNIE, el paciente o usuario de salud, para otorgar su autorización de acceso a sus historias clínicas electrónicas deberá autenticar su identidad ante el profesional de la salud que lo atiende y a través del sistema de información de historias clínicas electrónicas del establecimiento de salud o servicio médico de apoyo, mediante uno de los siguientes mecanismos:

- a) Documento nacional de identidad vigente, una contraseña que el Ministerio de Salud le proporcione y firma manuscrita, o
- b) Documento nacional de identidad vigente y servicio de autenticación biométrica de RENIEC.

Tercera.- Autenticación de la identidad para que el paciente o usuario de salud acceda a sus historias clínicas electrónicas a través del RENHICE

En tanto no se implemente en su totalidad el documento nacional de identidad electrónico –DNIE o no se cuente con los mecanismos o dispositivos necesarios para la autenticación de la identidad a través del DNIE, el paciente o usuario de salud o su representante legal para que acceda a sus historias clínicas electrónicas a través del RENHICE, autenticará su identidad con su documento nacional de identidad vigente más la contraseña que el Ministerio de Salud le proporcione.

Cuarta.- Proceso de autenticación de la identidad y firma digital para los profesionales de la salud.

El Ministerio de Salud podrá determinar mediante una norma complementaria las disposiciones y los mecanismos para asegurar el proceso de certificación digital de los profesionales de salud, en los sistemas de información de historias clínicas electrónicas.

Quinta.- Validez legal a las historias clínicas electrónicas implementadas antes de la entrada en vigencia del presente reglamento

Las historias clínicas electrónicas implementadas con firma digital antes de la entrada en vigencia del presente reglamento, dentro del marco de la Ley N° 27269, Ley de Firmas y Certificados Digitales, su reglamento aprobado mediante Decreto Supremo N° 052-2008-PCM y sus modificatorias, continuarán con la validez legal correspondiente, hasta que el Ministerio de Salud establezca la implementación del RENHICE.

Sexta.- Temporalidad del RENHICE de asumir las funciones de acceso e intercambio de información clínica atribuidas a la PIDE

El MINSA desarrollará la plataforma correspondiente para que se implemente el RENHICE, en tanto la PIDE concluya con la implementación de los estándares de interoperabilidad en salud, de seguridad y continuidad operativa para el intercambio de información clínica contenida en los sistemas de información de historias clínicas electrónicas (sistema de misión crítica) de los establecimientos de salud

o servicios médicos de apoyo, lo cual deberá ser acreditado por el MINSA, como administrador del RENHICE y ente rector del Sistema Nacional de Salud.

Anexo 11: Ley N° 26842 - Ley General de Salud

DECRETO SUPREMO

N° 033-2015-SA

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, el artículo 7 de la Constitución Política del Perú, establece que todas las personas tienen derecho a la protección de su salud, la del medio familiar y la de la comunidad, así como el deber de contribuir a su promoción y defensa. La persona incapacitada para velar por sí misma a causa de una deficiencia física o mental tiene derecho al respeto de su dignidad y a un régimen legal de protección, atención, readaptación y seguridad;

Que, los numerales I y II del Título Preliminar de la Ley N° 26842, Ley General de Salud disponen que la salud es condición indispensable del desarrollo humano y medio fundamental para alcanzar el bienestar individual y colectivo, y que es responsabilidad del Estado regularla, vigilarla y promoverla;

Que, la Ley N° 29889, Ley que modifica el artículo 11 de la Ley 26842, Ley General de Salud, y garantiza los derechos de las personas con problemas de salud mental, tiene por objeto garantizar que las personas con problemas de salud mental tengan acceso universal y equitativo a las intervenciones de promoción y protección de la salud, prevención, tratamiento, recuperación y rehabilitación psicosocial, con visión integral y enfoque comunitario, de derechos humanos, género e interculturalidad, en los diferentes niveles de atención;

Que, la precitada Ley, establece en su Segunda Disposición Complementaria Final que el Poder Ejecutivo la reglamentará;

Que, el Reglamento de la precitada Ley permitirá garantizar que las personas con problemas de salud mental tengan acceso universal y equitativo a las intervenciones de promoción y protección de la salud, prevención, tratamiento, recuperación y rehabilitación psicosocial, con visión integral y enfoque comunitario, de derechos humanos, género e interculturalidad, en los diferentes niveles de atención;

Que, en ese sentido, resulta necesario aprobar el Reglamento de la Ley N° 29889, Ley que modifica el artículo 11 de la Ley 26842, Ley General de Salud, y garantiza los derechos de las personas con problemas de salud mental;

De conformidad con lo dispuesto en el numeral 8 del artículo 118 de la Constitución Política del Perú y el numeral 3 del artículo 11 de la Ley N° 29158, Ley Orgánica del Poder Ejecutivo;

DECRETA:

Artículo 1.- Aprobación

Apruébese el Reglamento de la Ley N° 29889, Ley que modifica el artículo 11 de la Ley 26842, Ley General de Salud, y garantiza los derechos de las personas con problemas de salud mental, que consta de cinco (5) títulos, veintisiete (27) artículos, dos (2) disposiciones complementarias transitorias y una (1) disposición complementaria final, que forma parte integrante del presente Decreto Supremo.

Artículo 2.- Publicación

El presente Decreto Supremo y el Reglamento que aprueba, serán publicados en el Portal del Estado Peruano (www.peru.gob.pe) y en el portal institucional del Ministerio de Salud (www.minsa.gob.pe), el mismo día de su publicación en el Diario Oficial El Peruano.

Artículo 3.- Refrendo

El presente Decreto Supremo será refrendado por el Ministro de Salud.

Dado en la Casa de Gobierno, en Lima, a los cinco días del mes de octubre del año dos mil quince.

OLLANTA HUMALA TASSO

Presidente de la República

ANÍBAL VELÁSQUEZ VALDIVIA

Ministro de Salud

REGLAMENTO DE LA LEY N° 29889, LEY QUE MODIFICA EL ARTÍCULO 11 DE LA LEY N° 26842, LEY GENERAL DE SALUD, Y GARANTIZA

LOS DERECHOS DE LAS PERSONAS

CON PROBLEMAS DE SALUD MENTAL

TÍTULO PRIMERO

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1.- Objeto

El presente Reglamento regula las disposiciones establecidas en la Ley 29889; Ley que modifica el artículo 11 de la Ley N° 26842, Ley General de Salud y garantiza los derechos de las personas con problemas de salud mental, tiene como objeto garantizar que las personas con problemas de salud mental tengan acceso universal y equitativo a las intervenciones de promoción y protección de la salud, prevención, tratamiento, recuperación y rehabilitación psicosocial, con visión integral y enfoque comunitario, de derechos humanos, género e interculturalidad, en los diferentes niveles de atención.

Artículo 2.- Ámbito de aplicación

Las disposiciones contenidas en el presente Reglamento son de aplicación general para los establecimientos de salud y servicios médicos de apoyo públicos a cargo del Instituto de Gestión de Servicios de Salud-IGSS, de los Gobiernos Regionales, de los Gobiernos Locales, del Seguro Social de Salud - EsSalud, de las Sanidades de las Fuerzas Armadas y de la Policía Nacional del Perú, así como para los establecimientos de salud privados y otros prestadores que brinden atención de salud en todo el país.

Artículo 3.- Definiciones y acrónimos

Para los efectos del presente Reglamento se entenderá por:

1. Adicción.- Trastorno mental y del comportamiento que consiste fundamentalmente en alteraciones de la voluntad e implica incapacidad para abstenerse de consumir una sustancia, o la necesidad incontrolada y reiterada de realizar una conducta nociva. La adicción es un trastorno tratable y la recuperación es posible.
2. Discapacidad mental.- En concordancia con la Ley N° 29973, Ley General de la Persona con Discapacidad, la persona con discapacidad mental es aquella que tiene una o más deficiencias mentales o intelectuales de carácter permanente que al interactuar con diversas barreras actitudinales y del entorno, no ejerce o pueda verse impedida en el ejercicio de sus derechos; y de su inclusión plena y efectiva en la sociedad, en igualdad de condiciones que las demás. Incluye cualquier restricción o falta de capacidad para llevar a cabo o completar una actividad determinada, aparecida como consecuencia de un trastorno mental.
3. Capacidad de juicio afectado.- Alteración cuantitativa y/o cualitativa del pensamiento consistente en percibir cognitivamente la realidad de manera distorsionada.
4. Crisis.- Episodio de pérdida total o parcial de la capacidad de control sobre sí mismo y/o sobre su situación vital, que una persona experimenta por primera vez o en forma intermitente, de duración variable, a raíz de un trastorno mental conocido o probable, según criterio médico.
5. Emergencia psiquiátrica.- Alteración mental que pone en riesgo la integridad del paciente y/o de terceros, determinada por el médico evaluador.
6. Equipo interdisciplinario de salud mental.- Equipo interdisciplinario conformado por profesionales de la salud y técnicos capacitados y dedicados a la salud mental, que toman decisiones conjuntas y realizan acciones articuladas en este campo.

7. Internamiento u Hospitalización.- Proceso por el cual el usuario es ingresado a un establecimiento de salud para recibir cuidados necesarios, con fines diagnósticos, terapéuticos o de rehabilitación, así como procedimientos médico-quirúrgicos, y que requieran permanencia y necesidad de soporte asistencial por más de doce (12) horas, por su grado de dependencia o riesgo, según corresponda al nivel de atención. En establecimientos de salud del Primer Nivel de Atención, categoría I-4, se desarrolla la actividad de internamiento, y en los establecimientos de salud de segundo y tercer nivel de atención se desarrolla la actividad de hospitalización.

8. Intervención en salud mental.- Toda acción, incluidas las propias de la medicina y de otras profesiones relacionadas, tales como psicología, enfermería, terapia ocupacional, trabajo social y otras según sea procedente, que tengan por objeto potenciar los recursos propios de la persona para su autocuidado y favorecer factores protectores para mejorar la calidad de vida de la persona, la familia y la comunidad.

9. Intervenciones de salud mental en la comunidad.- Actividades o acciones de carácter promocional, preventivo, terapéutico, de rehabilitación y reinserción social que se realizan con la participación activa de la población organizada en beneficio de las personas con trastornos mentales o la promoción y protección de la salud mental individual y colectiva.

10. Junta Médica.- Se denomina así a la reunión de dos o más médicos psiquiatras, convocados para intercambiar opiniones respecto al diagnóstico, pronóstico y tratamiento de una persona. Es convocada por el médico tratante, a iniciativa propia, a solicitud del paciente o de sus familiares, u ordenada para aspectos legales por la autoridad competente, o de acuerdo al requerimiento de la ley, en el caso de personas con adicciones, para la determinación de su capacidad de juicio para tratamiento o internamiento involuntario.

11. Médico tratante.- Profesional médico que siendo competente para manejar el problema del paciente, conduce el diagnóstico y tratamiento. Cuando el paciente es trasladado a otro servicio o unidad, el médico tratante es aquel que asume su tratamiento médico o quirúrgico.

12. Modelo de atención comunitario de salud mental.- Es un modelo de atención de la salud mental centrado en la comunidad, que promueve la promoción y protección de la salud mental, así como la continuidad de cuidados de la salud de las personas, familias y colectividades con problemas psicosociales y/o trastornos mentales, en cada territorio, con la participación protagónica de la propia comunidad.

13. Problema psicosocial.- Es una dificultad generada por la alteración de la estructura y dinámica de las relaciones entre las personas y/o entre estas y su ambiente, por ejemplo: la violencia, la desintegración familiar, la desintegración comunitaria y social, la discriminación, entre otros.

14. Salud mental.- La salud mental es un proceso dinámico, producto de la interrelación entre el entorno y el despliegue de las diversas capacidades humanas tanto de los individuos como de los grupos y colectivos que forman la sociedad. Lo dinámico también incluye la presencia de conflictos en la vida de las personas, así como la posibilidad de afrontarlos de manera constructiva. Implica un proceso de búsqueda de sentido y armonía, que se encuentra íntimamente ligado a la capacidad de auto-cuidado, empatía y confianza que se pone en juego en la relación con las demás personas, así como con el reconocimiento de la condición -propia y ajena- de ser sujetos de derecho.

15. Servicios médicos de apoyo.- Son establecimientos que brindan servicios complementarios o auxiliares de la atención médica, que tienen por finalidad coadyuvar en el diagnóstico y tratamiento de los problemas clínicos. Pueden funcionar independientemente o dentro de un establecimiento de internamiento.

16. Trastorno mental y del comportamiento.- Condición mórbida que sobreviene en una determinada persona, afectando en intensidades variables el funcionamiento de la mente y del comportamiento, el organismo, la personalidad y la interacción social, en forma transitoria o permanente. Los trastornos mentales a que se refiere el presente Reglamento, se encuentran contemplados en la Clasificación Internacional de Enfermedades de la Organización Mundial de la Salud.

17. Tratamiento del trastorno mental y del comportamiento.- Acciones propias de la medicina, psicología, enfermería, terapia ocupacional, trabajo social y de otras profesiones relacionadas según sea procedente, dirigidas por un médico tratante y que tengan por objeto producir la recuperación o mejoría, adaptación y/o habilitación de una persona con trastorno mental y del comportamiento.

Listado de Acrónimos.-

- CIE: Clasificación Internacional de Enfermedades.

- OMS: Organización Mundial de la Salud.

- OPS: Organización Panamericana de la Salud.

TÍTULO SEGUNDO

CAPÍTULO I

DE LOS DERECHOS DE LAS PERSONAS

A LA SALUD MENTAL

Artículo 4.- Derecho a acceder a los servicios de salud mental

Se rige por los derechos establecidos en el artículo 15 de Ley N° 26842, Ley General de Salud, y la Ley N° 29414, Ley que establece los derechos de las personas usuarias de los servicios de salud; y adicionalmente asisten a las personas con problemas de salud mental los siguientes derechos específicos:

a. A ser atendido por su problema de salud mental en el establecimiento de salud más cercano a su domicilio, protegiéndose la vinculación con su entorno familiar, comunitario y social.

b. A recibir información necesaria sobre los servicios de salud a los que puede acceder y los requisitos necesarios para su uso, previo al sometimiento a procedimientos diagnósticos o terapéuticos, con excepción de las situaciones de emergencia en que se requiera aplicar dichos procedimientos.

c. A recibir en términos comprensibles información completa, oportuna y continuada sobre su estado de salud mental, incluyendo el diagnóstico, pronóstico y alternativas de tratamiento; así como sobre los riesgos, contraindicaciones, precauciones y advertencias de las intervenciones, tratamientos y medicamentos que se prescriban y administren.

- d. A obtener servicios, medicamentos y productos sanitarios adecuados y necesarios para prevenir, promover, conservar o recuperar su salud, según lo requiera, garantizando su acceso en forma oportuna, continua, integral y digna.
- e. A servicios de internamiento u hospitalización como recurso terapéutico de carácter excepcional.
- f. A servicios de internamiento u hospitalización en ambientes lo menos restrictivos posibles que corresponda a su necesidad de salud a fin de garantizar su dignidad y su integridad física.
- g. A otorgar su consentimiento informado, libre y voluntario, sin que medie ningún mecanismo que vicie su voluntad, para el procedimiento o tratamiento indicado.
- h. A ser informado sobre su derecho a negarse a recibir o continuar el tratamiento y a que se le expliquen las consecuencias de esa negativa.
- i. A la protección contra el abandono por parte de la familia, así como de los servicios del Estado, mediante la implementación de servicios de fortalecimiento de la vinculación familiar y comunitaria y de protección residencial transitoria.
- j. A contar con acceso al tratamiento de mayor eficacia y en forma oportuna, a través del uso pleno de sus respectivos seguros, incluida la protección financiera en salud del Estado.
- k. A recibir tratamientos cuya eficacia o mecanismos de acción hayan sido científicamente comprobados o cuyas reacciones adversas y efectos colaterales le hayan sido advertidos.
- l. A recibir tratamiento lo menos restrictivo posible, acorde al diagnóstico que le corresponda.
- m. A no ser privado de visitas durante el internamiento u hospitalización cuando éstas no estén contraindicadas por razones terapéuticas, y nunca por razones de sanción o castigo.
- n. A recibir la medicación correspondiente con fines terapéuticos o de diagnóstico, y nunca como castigo o para conveniencia de terceros.
- o. A la libertad de movimiento y comunicación con el interior y exterior del establecimiento, siempre y cuando sea compatible con el tratamiento programado.
- p. A autorizar, o no, la presencia de personas que no están directamente relacionados a la atención médica, en el momento de las evaluaciones.
- q. A ser escuchado y recibir respuesta por la instancia correspondiente cuando se encuentre disconforme con la atención recibida. Para estos efectos el servicio de salud debe contar con mecanismos claros para la recepción, tratamiento y resolución de quejas.
- r. A que su consentimiento conste por escrito cuando sea sujeto de investigación para la aplicación de medicamentos o tratamientos.

s. A no ser objeto de aplicación de algún método de anticoncepción sin previo consentimiento informado, emitido por la persona cuando no se encuentre en situación de crisis por el trastorno mental diagnosticado.

t. A tener acceso a servicios de anticoncepción independientemente de su diagnóstico clínico, incluido el retardo mental, con el apoyo pertinente del servicio para el ejercicio de su capacidad para obrar y la defensa de sus derechos.

u. A no ser discriminado o estigmatizado por tener o padecer, de manera permanente o transitoria, un trastorno mental o del comportamiento.

v. A recibir efectiva rehabilitación, inserción y reinserción familiar, laboral y comunitaria, en los servicios comunitarios de salud mental y de rehabilitación psicosocial y/o laboral.

w. Otros derechos que determine la Ley.

TÍTULO TERCERO

CAPÍTULO I

DE LA REFORMA DE LA ATENCIÓN

EN SALUD MENTAL

Artículo 5.- De la conformación de redes de atención para la atención de personas con problemas de salud mental

a. A la clasificación de establecimientos de salud de la red de servicios de salud existentes en el país establecidos en los artículos 45, 52 y 85 del Reglamento de Establecimientos de Salud y Servicios Médicos de Apoyo, aprobado por Decreto Supremo N° 013-2006-SA, se incorporan las siguientes estructuras:

1) Establecimientos de salud sin internamiento:

- Establecimientos de salud del primer nivel de atención, no especializado con servicios de atención de salud mental.

- Centros de salud mental comunitarios.

2) Establecimientos de salud con internamiento:

- Unidades de hospitalización de salud mental y adicciones de los Hospitales Generales.

- Unidades de hospital de día de salud mental y adicciones de los Hospitales Generales.

3) Servicios médicos de apoyo:

- Hogares protegidos
- Residencias protegidas
- Centros de rehabilitación psicosocial
- Centros de rehabilitación laboral

b. Las estructuras mencionadas en el literal precedente, constituyen en conjunto la red de atención comunitaria de salud mental, como parte integrante de la red de atención de salud.

c. El gobierno nacional, los gobiernos regionales y locales impulsan, implementan y sostienen la red de atención comunitaria de salud mental dentro de las redes de atención integral, incluyendo servicios médicos de apoyo para la atención de la salud mental.

d. Los servicios médicos de apoyo para la atención de salud mental cumplen sus funciones asegurando la continuidad de cuidados de la salud que se requiera para cada caso, incluida la rehabilitación psicosocial.

e. Las instituciones descritas en el ámbito de aplicación del presente Reglamento, realizan gestiones necesarias con los Gobiernos regionales y/o locales para la implementación, seguimiento y evaluación de las acciones de reforma de la atención en salud mental, fundamentalmente en lo relacionado a la implementación de hogares o residencias protegidas u otros servicios de protección residencial.

Artículo 6.- De los establecimientos de salud del primer nivel de atención con servicios de atención de salud mental.

a. Todas las redes de salud garantizan que los centros de salud nivel I-3 y I-4 tengan profesionales psicólogos.

b. Todas las redes de salud garantizan que los equipos básicos de salud de los establecimientos de salud bajo su responsabilidad se encuentren en capacitación continua, en servicio, para afrontar los problemas de salud mental de su población asignada.

Artículo 7.- De los centros de salud mental comunitarios

a. Los centros de salud mental comunitarios son establecimientos de salud categoría I-3 o I-4 especializados, que cuentan con psiquiatra y servicios especializados para niños/as y adolescentes, adultos y adultos mayores, adicciones y participación social y comunitaria.

b. Realizan actividades para la atención ambulatoria especializada de usuarios con trastornos mentales y/o problemas psicosociales, el fortalecimiento técnico de los establecimientos del primer nivel de atención y la activación de la red social y comunitaria de su jurisdicción.

Artículo 8.- De las Unidades de Hospitalización de Salud Mental y Adicciones

a. La Unidad de Hospitalización de Salud Mental y Adicciones es un servicio de hospitalización de estancia breve (hasta 60 días), dependiente del hospital general, desde el nivel II -2, con capacidad según la demanda proyectada.

b. Tiene como finalidad la estabilización clínica de personas en situación de emergencia psiquiátrica, agudización o reagudización del trastorno mental diagnosticado.

Artículo 9.- De las Unidades de Hospital de Día de Salud Mental y Adicciones

a. La Unidad de Hospital de Día de Salud Mental y Adicciones es un servicio ambulatorio especializado, de estancia parcial (6-8 horas por día), dependiente del hospital general o psiquiátrico, desde el nivel II-2, con capacidad según la demanda proyectada.

b. Brinda servicios complementarios a la hospitalización psiquiátrica, durante el lapso necesario para lograr la estabilización clínica total y su derivación al servicio de salud mental ambulatorio correspondiente, más cercano al domicilio del usuario.

Artículo 10.- De los Centros de Rehabilitación Psicosocial

a. Los Centros de Rehabilitación Psicosocial, son servicios médicos de apoyo, de atención especializada en rehabilitación psicosocial, destinados a personas con trastornos mentales con discapacidades, para recuperar el máximo grado de autonomía personal y social, y promover su mantenimiento e integración en la comunidad, así como apoyar y asesorar a sus familias; cuentan con psicólogos.

b. Los Centros de Rehabilitación Psicosocial dependen de la red de salud y coordinan con el Centro de Salud Mental Comunitario, los Centros de Rehabilitación Laboral y los Hogares o Residencia Protegidas y las organizaciones sociales y comunitarias de su ámbito territorial.

Artículo 11.- De los Centros de Rehabilitación Laboral

a. Los Centros de Rehabilitación Laboral, son servicios médicos de apoyo, especializados en rehabilitación laboral, destinados a personas con discapacidad laboral de diversa severidad producida por algún trastorno mental, para ayudarles a recuperar o adquirir los hábitos y capacidades laborales necesarias para acceder a la inserción o reinserción laboral, y apoyar su integración y mantenimiento en la misma; cuentan con psicólogos y terapeutas ocupacionales.

b. Los Centros de Rehabilitación Psicosocial dependen de la red de salud y coordinan con el Centro de Salud Mental Comunitario, los Centros de Rehabilitación Psicosocial y los Hogares o Residencia Protegidas y las organizaciones sociales y comunitarias de su ámbito territorial.

Artículo 12.- De los Hogares y Residencias Protegidas

- a. Los Hogares y Residencias Protegidas, son servicios médicos de apoyo que brindan servicios residenciales transitorios, alternativos a la familia, para personas con algún grado de discapacidad de causa mental que no tienen las habilidades para vivir en forma independiente y no cuentan con el apoyo de su familia.
- b. Los hogares protegidos se orientan a pacientes en condiciones de alta hospitalaria, que requieren cuidados mínimos y no cuentan con soporte familiar suficiente.
- c. Las residencias protegidas, se orientan a pacientes clínicamente estables, en condiciones de alta hospitalaria, pero con secuelas discapacitantes, pero que aún requieren cuidados por las secuelas discapacitantes.
- d. Los hogares y residencias protegidas dependen de la red de salud correspondiente y coordinan, según el estado del paciente con problemas de salud mental en tratamiento, con la Unidad de Hospitalización de Salud Mental y Adicciones, la Unidad de Hospital de Día de Salud Mental y Adicciones del hospital general local, con el Centro de Salud Mental Comunitario y con los Centros de Rehabilitación Psicosocial y Laboral.

CAPÍTULO II

DE LA ATENCIÓN A LAS PERSONAS

CON PROBLEMAS DE SALUD MENTAL

Artículo 13. De la atención de la salud mental

- a. La atención de la salud mental se realiza obligatoriamente desde el primer nivel de atención y en el marco de la política de redes integradas de servicios de salud y de acuerdo al nivel de complejidad.
- b. Las autoridades que dirigen las instancia comprendidas en el ámbito de aplicación del presente Reglamento son responsables de:
 - Garantizar la continuidad de cuidados de salud que cada persona con problemas de salud mental requiere, sean problemas psicosociales o trastornos mentales y del comportamiento, protegiendo su vinculación familiar y comunitaria.
 - La implementación de la atención ambulatoria especializada en salud mental a través de los centros de salud mental comunitarios, siendo éstos prioridades para cada red de servicios de salud.
 - Garantizar el funcionamiento de unidades de hospitalización de salud mental y adicciones, y unidades de hospital de día en sus establecimientos de salud de segundo nivel de atención.

- Priorizar la implementación de centros de salud mental comunitarios y servicios médicos de apoyo (hogares y residencias protegidas, centros de rehabilitación psicosocial y laboral) en el primer nivel de atención, que aseguren la continuidad de cuidados de la salud mental individual y colectiva de la población bajo su responsabilidad.

c. Todos los establecimientos de salud públicos realizan la vigilancia activa o tamizaje de problemas psicosociales y/o trastornos mentales y del comportamiento más comunes, entre sus usuarios y/o poblaciones asignadas.

d. Todos los establecimientos de salud públicos deben programar sus actividades preventivas a partir de una meta anual, correspondiente a la magnitud de la prevalencia del problema o el trastorno en la población usuaria o asignada.

e. Todos los servicios de salud públicos incorporan la atención de la salud mental de sus usuarios o su población asignada. Los médicos, principalmente los médicos generales, internistas, pediatras, gineco-obstetras y geriatras, deben evaluar y atender los aspectos mentales básicos que presenten sus usuarios, en todas las etapas de vida.

f. Es de responsabilidad del médico tratante, principalmente de los médicos generales, internistas, pediatras, gineco-obstetras y geriatras, formular el plan de tratamiento básico relacionado a la salud mental orientado por las guías de práctica clínica del Ministerio de Salud y/o su formación universitaria básica, incluyendo, de ser necesaria, la referencia o interconsulta del paciente a un servicio especializado.

g. En la historia clínica se incluye la sección de evaluación básica del estado mental del paciente, de llenado, supervisión y auditoría obligatoria, según nivel de atención y capacidad resolutoria.

Artículo 14.- De la reestructuración de los hospitales generales para garantizar la atención de la salud mental, y el establecimiento de camas para los usuarios.

Todos los hospitales generales, desde la categoría II-2, y especializados no psiquiátricos, o sus equivalentes públicos y privados, deben:

a. Contar con unidades de hospitalización y de hospital de día de salud mental y adicciones, y atención de emergencias psiquiátricas en el servicio de emergencias.

b. Brindar atención de salud mental de emergencia, hospitalización breve (hasta 60 días) y hospital de día, a usuarios provenientes de sus ámbitos de influencia, inclusive de ámbitos colindantes, en caso que éstos no contasen con estos servicios, independientemente de que el paciente cuente o no con seguro, y de la condición y tipo de seguro, en el marco de los convenios de intercambio prestacional.

c. Contar con médicos psiquiatras en su equipo.

d. Brindar la atención de las emergencias psiquiátricas en su servicio de emergencia, por el equipo de emergencia o de guardia, y/o el médico psiquiatra del hospital.

e. Contar con unidades asistenciales que integren los recursos de psiquiatría, psicología, enfermería, trabajo social y disciplinas afines, para garantizar la calidad de las intervenciones basadas en equipos interdisciplinarios especializados, en coordinación con los departamentos o servicios respectivos.

f. Coordinar con el sistema de referencia y contrarreferencia la atención del paciente, a través de sus departamentos o servicios de salud mental, de ser necesario.

g. Brindar, a través de sus departamentos o servicios de salud mental o sus equivalentes, el apoyo técnico, monitoreo y supervisión de las atenciones de salud mental en los Centros de Salud de su área de influencia, en los territorios donde no se hayan instalado Centros de Salud Mental Comunitarios.

Artículo 15.- Del internamiento u hospitalización

La persona con problemas de salud mental, que requiera internamiento u hospitalización para su tratamiento, lo recibe considerando las siguientes premisas:

- a. El internamiento u hospitalización forma parte del proceso de cuidado continuo de la salud.
- b. Requiere el consentimiento informado libre y voluntario del paciente, o de su representante legal, cuando corresponda.
- c. Se realiza cuando brinda mayores beneficios terapéuticos que la atención ambulatoria.
- d. Se prolonga el tiempo estrictamente necesario para la estabilización clínica.
- e. Se lleva a cabo en el establecimiento de salud más cercano al domicilio del paciente.
- f. Al momento del alta médica, debe asegurarse la continuidad de cuidados de la salud ambulatorios que requiere cada caso.

Artículo 16.- Del consentimiento informado

La atención de la persona con problemas de salud mental, requiere del consentimiento informado para su estudio y tratamiento, teniendo en cuenta lo siguiente:

- a. Es previo a cualquier procedimiento médico.
- b. El documento en el que se refrenda el consentimiento informado del paciente, debe hacer evidente por escrito el proceso de información y decisión que ha recibido. Constituye un documento oficial.
- c. En caso de emergencia psiquiátrica, en que por su condición clínica el paciente no se encuentre en capacidad de discernir, su familiar directo firma los documentos de autorización correspondiente; en caso contrario, se procede a comunicar a la Fiscalía de turno correspondiente la necesidad del internamiento u

hospitalización o del procedimiento, para que la autoridad expida los documentos de autorización pertinentes.

d. En caso que el paciente o su familiar directo no supiera firmar, imprimirá su huella digital.

e. En caso de personas con adicciones que presentan capacidad de juicio afectada, su tratamiento o internamiento involuntario indicado por el médico tratante, procederá previa evaluación de la capacidad de juicio por una junta médica.

Artículo 17.- Del acceso universal y gratuito al tratamiento de problemas de salud mental

a. Las personas con trastornos mentales y del comportamiento o con discapacidades mentales que cuentan con seguros públicos o privados tienen acceso a través de su seguro al tratamiento de mayor eficacia y en forma oportuna, incluyendo el diagnóstico, tratamiento ambulatorio y/o de hospitalización, recuperación y rehabilitación.

b. Los seguros públicos y privados incluyen en sus coberturas los trastornos mentales y del comportamiento reconocidos en el Plan Esencial de Aseguramiento en Salud y sus planes complementarios.

Artículo 18.- De la disponibilidad de psicofármacos desde el primer nivel de atención

a. La provisión de psicofármacos deberá basarse fundamentalmente en las Guías de Práctica Clínica vigentes y en el Petitorio Nacional Único de Medicamentos. El Ministerio de Salud promueve el uso racional de los mismos.

b. Los establecimientos de salud disponen permanentemente de psicofármacos desde el primer nivel de atención, en forma sostenida, y preferentemente de aquellos psicofármacos de mayor demanda entre sus usuarios y/o poblaciones asignadas bajo su responsabilidad.

c. Los médicos cirujanos pueden prescribir medicamentos psicofármacos orientados por las Guías de Práctica Clínica del Ministerio de Salud y su formación universitaria básica.

CAPÍTULO III

DE LA DEINSTITUCIONALIZACIÓN

Artículo 19.- De las personas con discapacidad mental con estancia prolongada en el establecimiento de salud

Son aquellas personas que pese a tener un diagnóstico de alta médica, por diferentes circunstancias ajenas a su voluntad, permanecen innecesariamente internadas en los hospitales donde fueron llevados para tratar un episodio propio de su discapacidad mental.

Artículo 20.- De la desinstitucionalización de la persona con discapacidad mental

a. Es el proceso por el cual un establecimiento de salud debe implementar para sus pacientes hospitalizados por discapacidad mental, que tienen un periodo de internamiento mayor a los cuarenta y cinco días (45) días, y que se encuentran en condición de alta médica, y que ya no requieren internamiento para su tratamiento, o puede continuarlo de manera ambulatoria, pero que por razones no médicas no pueden dejar el hospital.

Esta situación debe evitarse en los establecimientos de salud, para lo cual se deberá hacer uso de la red de atención comunitaria de salud mental.

b. Todo establecimiento de salud con internamiento y que atienda a personas con problemas de salud mental, debe constituir el Comité Permanente Encargado de Evaluar la Desinstitucionalización de Personas con Discapacidad Mental, ante el cual se presentará la situación del paciente con un informe médico emitido por el médico tratante.

c. Es el Servicio Social del establecimiento de salud, quien hace conocer los casos al Comité Permanente Encargado de Evaluar la Desinstitucionalización de Personas con Discapacidad Mental, de aquellos pacientes que reúnan la condición descrita en el artículo 19 del presente Reglamento y es además quien gestiona el informe médico del paciente con su médico tratante.

Artículo 21.- Del Comité Permanente Encargado de Evaluar la Desinstitucionalización de Personas con Discapacidad Mental

a. Es el órgano adscrito a la Dirección del establecimiento de salud con internamiento, y que está integrado por un médico psiquiatra, un abogado, una trabajadora social, así como por un representante de la Defensoría del Pueblo.

b. El referido Comité es responsable de realizar las siguientes funciones:

- Evaluar el informe médico y social del paciente que se encuentra en condición de estancia prologada.
- Realiza las indagaciones para determinar el lugar más apropiado de reinserción del paciente, determinando si tiene familiares u otras personas o instituciones que puedan hacerse cargo del paciente, en tanto no requieran atención médica.
- Coordina con las instituciones públicas y privadas, así como con los servicios médicos de apoyo correspondientes, la incorporación y acogida para aquellos pacientes que no tienen familiares que se hagan cargo de ellos.
- Elabora en base a los antecedentes clínicos e informe social del paciente un Informe Final dirigido al director del establecimiento de la salud.
- Realiza el seguimiento periódico y supervisión continua de los pacientes que fueron desinstitucionalizados, dando cuenta de sus acciones al Director del establecimiento de salud.

Artículo 22.- De la reinserción del paciente luego de su desinstitucionalización

a. Las personas con discapacidad mental que permanecen en establecimientos de salud y que clínicamente no requieren hospitalización, son reinsertadas con su familia o derivadas a las instituciones públicas o privadas conformadas para tal fin, como hogares o residencias protegidas, procurando una recuperación gradual del ejercicio de su autonomía, dependiendo de su grado de discapacidad, respetando su dignidad personal y derechos humanos.

b. Las personas con discapacidad mental que presenten periodos de recidiva o recurrencia, que requiera cuidados especializados de hospitalización total, son derivados a la unidad de hospitalización de salud mental y adicciones del establecimiento de salud correspondiente, hasta lograr su recuperación; una vez que reciban el alta médica son derivados al lugar donde fueron acogidos. De presentarse nuevas circunstancias son nuevamente reevaluados por el Comité Permanente Encargado de Evaluar la Desinstitucionalización de Personas con Discapacidad Mental, para decidir la continuidad de su tratamiento.

CAPÍTULO IV

DE LA ATENCIÓN DE LA SALUD MENTAL

EN LA COMUNIDAD

Artículo 23. Del modelo de atención comunitario

a. El modelo de atención comunitario para la salud mental tiene las siguientes características:

1) Prioriza la promoción y protección de la salud mental y la continuidad de los cuidados de la salud de las personas, familias y comunidad.

2) Promueve la participación de la comunidad organizada, a través de las asociaciones de personas afectadas por problemas de salud mental y sus familiares, así como de organizaciones sociales de base comprometidas en el proceso de identificación de necesidades, planificación, gestión y evaluación de planes y programas de intervención local.

3) Cubre necesidades de atención en salud mental de una población jurisdiccionalmente determinada, en una red de servicios de salud.

4) Funciona en red, logrando la coordinación y articulación de los servicios, y programas de la red asistencial, asegurando la continuidad de cuidados de salud.

5) Promueve un entorno familiar saludable para las personas usuarias, a través de la propia familia y su comunidad, o de su incorporación en hogares o residencias protegidas, en caso de no contar con familia.

6) Se basa en la identificación y respuesta a las necesidades de salud mental de una población determinada en general y de los usuarios y usuarias en particular.

7) Promueve la atención integral: Bio-psico-social, con equipos multidisciplinarios y abordajes interdisciplinarios.

8) Impulsa la reinserción socio-laboral en función a la articulación de los recursos intersectoriales y de la propia comunidad.

9) Asegura la atención especializada e integrada en el primer nivel de atención dentro del Sistema Nacional Coordinado y Descentralizado de Salud, mediante los centros de salud mental comunitarios.

10) Promueve la capacitación continua en salud mental de los equipos de salud, respetando las especificidades de formación y labor de los profesionales de la salud y agentes comunitarios.

Artículo 24.- De la participación social y comunitaria

a. Las agrupaciones de familiares y de usuarios, así como las organizaciones sociales de base se incorporan en redes locales, regionales y/o nacionales que les permita participar organizadamente en la formulación e implementación de políticas y planes y la vigilancia comunitaria en sus ámbitos correspondientes.

b. Las agrupaciones de familiares y de personas usuarias de servicios de salud mental o de organizaciones aliadas facilitan el apoyo emocional entre sus participantes, la educación respecto a la enfermedad y su tratamiento, así como la resolución conjunta y solidaria de aquellos problemas que les son comunes. Estas agrupaciones se orientan a ser una instancia de autoayuda y reciben el apoyo del Gobierno Regional y de la Dirección Regional de Salud, o quien haga sus veces, de acuerdo a su lugar de residencia.

Artículo 25.- De la Coordinación intersectorial

a. El Ministerio de la Mujer y Poblaciones Vulnerables, el Ministerio de Desarrollo e Inclusión Social, el Ministerio de Educación y el Ministerio de Trabajo y Promoción del Empleo participan en forma coordinada con el Ministerio de Salud para las intervenciones en salud mental, en correspondencia a sus competencias y funciones.

b. Los gobiernos regionales y locales participan activamente en las acciones del Ministerio de Salud en materia de salud mental, conforme a sus competencias y funciones en beneficio de la población.

c. El Instituto Nacional de Salud Mental tiene la responsabilidad de gestionar y realizar programas y proyectos de investigación para el fortalecimiento de las políticas y normas públicas en salud mental.

TÍTULO CUARTO

CAPÍTULO I

DE LA SUPERVISIÓN

Artículo 26.- Ente Supervisor

a. La autoridad sanitaria en los niveles nacional y regional, según corresponda, realiza la verificación sanitaria de los establecimientos de salud y servicios médicos de apoyo destinados a la atención de personas que sufren trastornos mentales, con el fin de brindar asistencia técnica en el cumplimiento de las condiciones relativas al internamiento u hospitalización, tratamiento y alta de los pacientes.

b. La verificación sanitaria se realiza a través de inspecciones ordinarias y extraordinarias y con el personal calificado multidisciplinario.

c. Las inspecciones ordinarias se realizan periódicamente y son programadas de acuerdo a un plan debidamente aprobado.

d. Las inspecciones extraordinarias se realizan en cualquier momento, con la finalidad de prever o corregir cualquier circunstancia que ponga en peligro la salud de los pacientes. Estas inspecciones se realizan en aquellos supuestos en los que existan indicios razonables de irregularidad o de comisión de alguna infracción.

e. La Superintendencia Nacional de Salud (SUSALUD) ejerce la supervisión de las atenciones de la persona con problemas de salud mental a las instituciones prestadoras de servicios de salud, en el ámbito de su competencia.

f. Para realizar la visita de verificación sanitaria, la autoridad de salud podrá solicitar, de ser pertinente, la participación del Ministerio Público, Policía Nacional del Perú y la Municipalidad Distrital correspondiente.

TÍTULO QUINTO

CAPÍTULO I

DE LA FORMACIÓN, ESPECIALIZACIÓN

Y CAPACITACIÓN

Artículo 27.- De la incorporación del componente de salud mental en la formación de profesionales y técnicos de la salud

a. Las instituciones formadoras de profesionales y técnicos de la salud, son responsables de implementar un curso, de no menos de tres (3) créditos en la formación de los profesionales y técnicos de la salud que se oriente a los diversos aspectos de la salud mental y con enfoque comunitario.

b. Los programas de segunda especialización médica (Residentado Médico), incluyen un curso, de no menos de tres (3) créditos, que se oriente a los diversos aspectos de la salud mental, en el último año de la currícula de los médicos residentes de todas las especialidades.

c. Los programas de segunda especialización médica (Residentado Médico), incluyen no menos del 10% de plazas para la especialidad de Psiquiatría, para lo cual las Universidades y las instituciones prestadoras

de servicios de salud generan campos clínicos, bajo responsabilidad de la autoridad del Comité Nacional del Residentado Médico (CONAREME).

d. La Dirección General de Gestión de Desarrollo de Recursos Humanos del Ministerio de Salud, es responsable de formular e implementar el Plan Nacional de Capacitación en Salud Mental, en coordinación con la Dirección de Salud Mental, con la finalidad de fomentar la capacitación continua en servicio, para el personal asistencial de todas las redes de servicios de salud.

e. Las instituciones de los diversos sub sectores de salud designan no menos del 10% de su presupuesto de capacitación y desarrollo de recursos humanos al fortalecimiento y mantenimiento de competencias de sus equipos para la atención de salud mental.

DISPOSICIONES COMPLEMENTARIAS TRANSITORIAS

Primera.- En un plazo que no excederá de treinta (30) días calendario a partir de la publicación del presente Reglamento, en cumplimiento de la Sentencia del Tribunal Constitucional recaída en el Expediente N° 03426-2008-PHC/TC, mediante Resolución Suprema se conformará la Comisión Multisectorial de naturaleza temporal, adscrita al Ministerio de Salud, encargada de proponer una política de tratamiento y rehabilitación de salud mental de las personas a quienes se les ha impuesto judicialmente una medida de seguridad de internación, por padecer de una enfermedad mental.

Segunda.- En un plazo que no excederá de ciento veinte (120) días a partir de la publicación del presente Reglamento el Ministerio de Salud, mediante Resolución Ministerial, aprobará los documentos técnicos que correspondan al Modelo de atención Comunitario de Salud Mental, Centro de Salud Mental Comunitario, Unidades de Hospitalización de Salud Mental y Adicciones de Hospitales Generales, Unidades de Hospital de Día de Salud Mental y Adicciones de Hospitales Generales, Hogares y Residencias Protegidas, Centros de Rehabilitación Psicosocial y Centros de Rehabilitación Laboral.

DISPOSICIÓN COMPLEMENTARIA FINAL

Única.- Los internamientos u hospitalizaciones indicados por la autoridad judicial competente consideran los criterios de internamiento establecidos en el presente reglamento, los mismos que se ciñen a las Convenciones y tratados sobre Derechos Humanos vigentes de los cuales el Estado Peruano es parte.

Anexo 12: Decreto de Urgencia_Sistema Nacional de Transformación Digital

DECRETO DE URGENCIA

N° 006-2020

DECRETO DE URGENCIA QUE CREA EL SISTEMA NACIONAL DE TRANSFORMACIÓN DIGITAL

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, de conformidad con el artículo 135 de la Constitución Política del Perú, durante el interregno parlamentario, el Poder Ejecutivo legisla mediante decretos de urgencia de los que da cuenta a la Comisión Permanente para que los examine y los eleve al nuevo Congreso, una vez que éste se instale;

Que, mediante Decreto Supremo N° 165-2019-PCM, Decreto Supremo que disuelve el Congreso de la República y convoca a elecciones para un nuevo Congreso, se revocó el mandato parlamentario de los congresistas, manteniéndose en funciones la Comisión Permanente;

Que, el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado mediante Decreto Supremo N° 022-2017-PCM, establece en el artículo 47, que la Secretaría de Gobierno Digital es el órgano de línea, con autoridad técnico normativa a nivel nacional, responsable de formular y proponer políticas nacionales y sectoriales, planes nacionales, normas, lineamientos y estrategias en materia de Informática y de Gobierno Electrónico, y ejerce la rectoría del Sistema Nacional de Informática;

Que, el Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital, establece el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno;

Que, en el marco de la Política Nacional de Competitividad y Productividad, aprobada mediante el Decreto Supremo N° 345-2018-EF, mediante Decreto Supremo N° 237-2019-EF, se aprueba el Plan de Competitividad y Productividad 2019-2030, el cual presenta un conjunto de medidas consensuadas entre el sector público y privado con miras a establecer un entorno favorable y competitivo que permita generar bienestar para todos los peruanos sobre la base de un crecimiento económico sostenible con enfoque territorial;

Que, la Organización para la Cooperación y Desarrollo Económicos (OCDE) señala en el documento Políticas de Banda Ancha para América Latina y el Caribe - Un manual para la Economía Digital que las tecnologías digitales podrían contribuir a cada uno de los Objetivos de Desarrollo Sostenible (ODS);

Que, el Foro Económico Mundial señala que la transformación digital tiene impacto directo en la competitividad de los países y en la generación de bienestar social y económico para los ciudadanos a través del impulso en la educación, en el acceso a la tecnología, en las pequeñas y medianas empresas, en los sectores de mayor demanda de la población, en los emprendimientos e innovación y en la cobertura de las necesidades de los ciudadanos;

Que, el Programa de las Naciones Unidas para el Desarrollo (PNUD), reconoce el avance del Perú en el Índice de Desarrollo Humano, pero a su vez señala que se presentan brechas que deben ser reducidas y analiza las desigualdades actuales y cómo pueden cambiar en el futuro, observando particularmente dos cambios relevantes que darán forma a la vida hasta el siglo 22, entre ellos la transformación digital; indicando que las tecnologías digitales, las finanzas digitales y las soluciones de salud digital, ofrecen una idea de cómo el futuro de la desigualdad puede romper con el pasado, si las oportunidades pueden aprovecharse rápidamente y compartirse ampliamente;

Que, la transformación digital es un proceso crítico para el bienestar de la población, siendo urgente desarrollar el ecosistema que regule las actividades digitales del país, así como establecer los mecanismos de colaboración y articulación con actores públicos, privados y sociedad civil en el entorno digital, a través de un enfoque sistémico e integral, que asegure la generación de valor público y promueva la generación de valor económico y social para los ciudadanos, entidades y sociedad en general, y contribuya al fortalecimiento de las funciones sustantivas del Estado;

En uso de las facultades conferidas por el artículo 135 de la Constitución Política del Perú;

Con el voto aprobatorio del Consejo de Ministros; y

Con cargo a dar cuenta a la Comisión Permanente para que lo examine y lo eleve al nuevo Congreso, una vez que éste se instale:

DECRETA:

Artículo 1.- Objeto

El presente Decreto de Urgencia tiene por objeto crear el Sistema Nacional de Transformación Digital.

Artículo 2.- Principios

Son principios que rigen el Sistema Nacional de Transformación Digital:

- a) Apertura, transparencia e inclusión.- El uso de tecnologías digitales brinda la oportunidad de fortalecer la apertura, transparencia e inclusión.
- b) Compromiso y participación.- La toma de decisiones, diseño de políticas y entrega de servicios digitales se realiza utilizando enfoques, métodos o técnicas colaborativas que atiendan las necesidades y demandas de las personas.
- c) Datos como activo estratégico.- Los datos son reconocidos como un activo estratégico para diseñar políticas, tomar decisiones, así como crear y entregar servicios digitales. Asimismo, la gestión transparente y ética de los datos se soporta en procesos, roles y estructuras de gobernanza.
- d) Protección de datos personales y preservación de la seguridad.- Se asegura la estructura de gobernanza, regulación y liderazgo que facilite el equilibrio entre la apertura de datos y los niveles adecuados de privacidad y seguridad digital.
- e) Liderazgo y compromiso político.- El liderazgo y compromiso se asegura desde la alta dirección para dirigir, orientar y supervisar la transformación digital, haciendo uso de los mecanismos de coordinación existentes.
- f) Cooperación y colaboración.- La cooperación con otros países y organizaciones, así como la colaboración entre entidades, facilita el intercambio de experiencias, buenas prácticas, información y conocimiento, y desarrollo de servicios en materia de gobierno y transformación digital.
- g) Servicios digitales centrados en las personas.- La creación, diseño y desarrollo de servicios digitales responde a las demandas y necesidades de la ciudadanía, buscando asegurar la generación de valor público.

h) Competencias digitales.- La transformación digital requiere fortalecer las competencias digitales, habilidades y destrezas, en especial aquellas competencias relacionadas a las prácticas de gestión de proyectos digitales, el cambio cultural, los servicios digitales, seguridad digital y la arquitectura digital.

i) Adquisiciones y contrataciones inteligentes.- La adquisición de tecnologías digitales se adapta a enfoques que prioricen el uso compartido y la reutilización de infraestructura, plataformas y recursos digitales.

Artículo 3.- Transformación Digital

La transformación digital es el proceso continuo, disruptivo, estratégico y de cambio cultural que se sustenta en el uso intensivo de las tecnologías digitales, sistematización y análisis de datos para generar efectos económicos, sociales y de valor para las personas.

Artículo 4.- Sistema Nacional de Transformación Digital

4.1 El Sistema Nacional de Transformación Digital es un Sistema Funcional del Poder Ejecutivo, conformado por un conjunto de principios, normas, procedimientos, técnicas e instrumentos mediante los cuales se organizan las actividades de la administración pública y se promueven las actividades de las empresas, la sociedad civil y la academia orientadas a alcanzar los objetivos del país en materia de transformación digital.

4.2 El Sistema Nacional de Transformación Digital se sustenta en la articulación de los diversos actores públicos y privados de la sociedad y abarca, de manera no limitativa, las materias de gobierno digital, economía digital, conectividad digital, educación digital, tecnologías digitales, innovación digital, servicios digitales, sociedad digital, ciudadanía e inclusión digital y confianza digital; sin afectar las autonomías y atribuciones propias de cada sector, y en coordinación con estos en lo que corresponda en el marco de sus competencias.

Artículo 5.- Finalidad del Sistema Nacional de Transformación Digital

El Sistema Nacional de Transformación Digital tiene por finalidad:

1. Fomentar e impulsar la transformación digital de las entidades públicas, las empresas privadas y la sociedad en su conjunto, fortalecer el uso efectivo de las tecnologías digitales, las redes y los servicios digitales por parte de los ciudadanos y personas en general.
2. Impulsar la innovación digital, el fortalecimiento de una sociedad digital inclusiva y el ejercicio de una ciudadanía digital con deberes y derechos digitales de los ciudadanos.
3. Promover la economía digital, la competitividad, productividad e inclusión financiera en una sociedad digital.
4. Fortalecer el acceso y la inclusión a las tecnologías digitales en el país y la confianza digital fomentando la seguridad, transparencia, protección de datos personales y gestión ética de las tecnologías en el entorno digital para la sostenibilidad, prosperidad y bienestar social y económico del país.

Artículo 6.- Ámbito de aplicación

Los principios, normas y procedimientos que rigen la materia de Transformación Digital son aplicables a las entidades establecidas en el artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo N° 004-2019-JUS, y, a las organizaciones de la sociedad civil, ciudadanos, empresas y academia en lo que corresponda.

Artículo 7.- Ente rector del Sistema Nacional de Transformación Digital

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector del Sistema Nacional Transformación Digital, constituyéndose en la autoridad técnico-normativa a nivel nacional sobre la materia.

Artículo 8.- Funciones del ente rector

8.1 Son funciones del ente rector:

- a) Formular y proponer la política y estrategia nacional de transformación digital.
- b) Promover, dirigir, coordinar, supervisar y evaluar la transformación digital del país.
- c) Elaborar y proponer normas reglamentarias y complementarias que regulen la transformación digital del país.
- d) Elaborar y aprobar lineamientos, procedimientos, metodologías, instrumentos, técnicas, modelos, directivas u otros para la transformación digital del país.
- e) Elaborar y proponer estándares técnicos en coordinación con los sectores competentes.
- f) Supervisar y fiscalizar, cuando corresponda, el cumplimiento del marco normativo en materia del Sistema Nacional de Transformación Digital.
- g) Emitir opinión vinculante sobre el alcance, interpretación e integración de normas que regulan la materia de transformación digital; así como sobre el despliegue de plataformas transversales administradas por el Estado en materia de transformación digital.
- h) Promover, coordinar y gestionar el intercambio de conocimientos a nivel nacional e internacional en materia de transformación digital en el país.
- i) Articular acciones con representantes del sector privado, la sociedad civil, la academia, las personas u otros interesados para promover la transformación digital del país.

8.2 Dichas funciones se ejercen sin afectar las autonomías y atribuciones de cada sector en el marco de sus competencias.

Artículo 9.- Integrantes del Sistema Nacional Transformación Digital

Forman parte del Sistema Nacional de Transformación Digital:

- a) La Presidencia del Consejo de Ministros
- b) El Ministerio de Economía y Finanzas
- c) El Ministerio de Educación
- d) El Ministerio de Transportes y Comunicaciones
- e) El Ministerio de Justicia y Derechos Humanos
- f) El Ministerio de la Producción
- g) El Ministerio de Relaciones Exteriores
- h) El Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica
- i) Los Comités de Gobierno Digital de las entidades públicas a nivel nacional
- j) Organizaciones del sector privado, la sociedad civil, la academia u otros actores relevantes para una sociedad digital

Artículo 10.- Del Comité de Alto Nivel por un Perú Digital, Innovador y Competitivo

El Comité de Alto Nivel por un Perú Digital, Innovador y Competitivo constituye el espacio de coordinación y articulación entre el sector público, privado, sociedad civil, academia y ciudadanos para las acciones relacionadas al desarrollo y consolidación de la transformación digital en el país, a fin de fortalecer la competitividad, productividad, el cierre de brechas en materia digital, el bienestar social y económico de las personas y asegurar su sostenibilidad en todas las regiones del Perú.

Artículo 11.- Organizaciones del sector privado, la sociedad civil, la academia y otros actores relevantes para la construcción de una sociedad digital

Las organizaciones del sector privado, la sociedad civil, la academia, entre otros actores relevantes para la construcción de una sociedad digital y el desarrollo de una economía digital, consideran en sus acciones los objetivos de la política y estrategia nacional de transformación digital orientadas a fortalecer la confianza digital en el diseño e implementación de servicios digitales.

Artículo 12.- Política y Estrategia Nacional de Transformación Digital

La Política y Estrategia Nacional de Transformación Digital se constituyen en los instrumentos estratégicos y orientadores para la transformación digital en el país.

Artículo 13.- Articulación con el Sistema Administrativo de Modernización de la Gestión Pública

La Secretaría de Gobierno Digital coordina con la Secretaría de Gestión Pública las acciones vinculadas con el Sistema Administrativo de Modernización de la Gestión Pública.

Artículo 14.- Financiamiento

La implementación de lo establecido en el presente Decreto de Urgencia se financia con cargo al presupuesto institucional de las entidades correspondientes.

Artículo 15.- Refrendo

El presente Decreto de Urgencia es refrendado por el Presidente del Consejo de Ministros, la Ministra de Economía y Finanzas, la Ministra de Educación, el Ministro de Transportes y Comunicaciones, la Ministra de Justicia y Derechos Humanos, la Ministra de la Producción y el Ministro de Relaciones Exteriores.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera.- Modificación del artículo 8 del Decreto Legislativo 1310 que aprueba medidas adicionales de simplificación administrativa

Modifícase el artículo 8 del Decreto Legislativo N° 1310 que aprueba medidas adicionales de simplificación administrativa, en los siguientes términos:

“Artículo 8. Sistemas de Trámite Documentario de las Entidades de la Administración Pública

Las entidades de la Administración Pública deben interconectar sus sistemas de trámite documentario o equivalentes para el envío automático de documentos electrónicos entre dichas entidades a través de la Plataforma de Interoperabilidad del Estado administrada por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital.

Las entidades del Poder Ejecutivo deben adecuar sus sistemas de trámite documentario o equivalentes para el envío automático de documentos electrónicos con otras entidades, así como dentro de sus áreas, órganos y unidades, hasta el 31 de diciembre de 2021.

Mediante Decreto Supremo refrendado por el Presidente del Consejo de Ministros se establecen los plazos aplicables a las demás entidades de la Administración Pública, y cualquier otra disposición que resulte necesaria para la digitalización e integración de sus sistemas de trámite documentario o equivalentes.”

Segunda.- Reglamento del Sistema Nacional de Transformación Digital

El Reglamento del Sistema Nacional de Transformación Digital se aprueba a propuesta de la Presidencia del Consejo de Ministros con el refrendo del Ministerio de Economía y Finanzas en un plazo máximo de noventa (90) días hábiles posterior a la publicación del presente Decreto de Urgencia.

Tercera.- Política y Estrategia Nacional de Transformación Digital

En un plazo no mayor a noventa (90) días hábiles, posterior a la publicación del presente Decreto de Urgencia, la Presidencia del Consejo de Ministros, en su calidad de ente rector del Sistema Nacional de Transformación Digital formula y propone la Política y la Estrategia Nacional de Transformación Digital.

Cuarta.- Aplicación de la Norma

Los proyectos de inversión privada que, a la fecha, cuenten con contratos suscritos o que hayan sido incorporados al proceso de promoción de la inversión privada, seguirán sujetos a la normativa vigente hasta antes de la entrada en vigencia del presente Decreto de Urgencia.

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

Única.- Norma derogatoria

Deróganse las disposiciones contenidas en el Decreto Legislativo 604 relativas al Sistema Nacional de Informática que se opongan al presente Decreto de Urgencia. Entiéndase, para todos sus efectos, que el Sistema Nacional de Transformación Digital sustituye al Sistema Nacional de Informática.

Dado en la Casa de Gobierno, en Lima, a los ocho días del mes de enero del año dos mil veinte.

MARTÍN ALBERTO VIZCARRA CORNEJO

Presidente de la República
VICENTE ANTONIO ZEBALLOS SALINAS
Presidente del Consejo de Ministros
MARÍA ANTONIETA ALVA LUPERDI
Ministra de Economía y Finanzas y
Encargada del Despacho del Ministerio de
Relaciones Exteriores
FLOR AIDEÉ PABLO MEDINA
Ministra de Educación
ANA TERESA REVILLA VERGARA
Ministra de Justicia y Derechos Humanos
ROCÍO INGRED BARRIOS ALVARADO
Ministra de la Producción
EDMER TRUJILLO MORI
Ministro de Transportes y Comunicaciones
1844001-1

Anexo 13: Propuesta de pantallas PMV

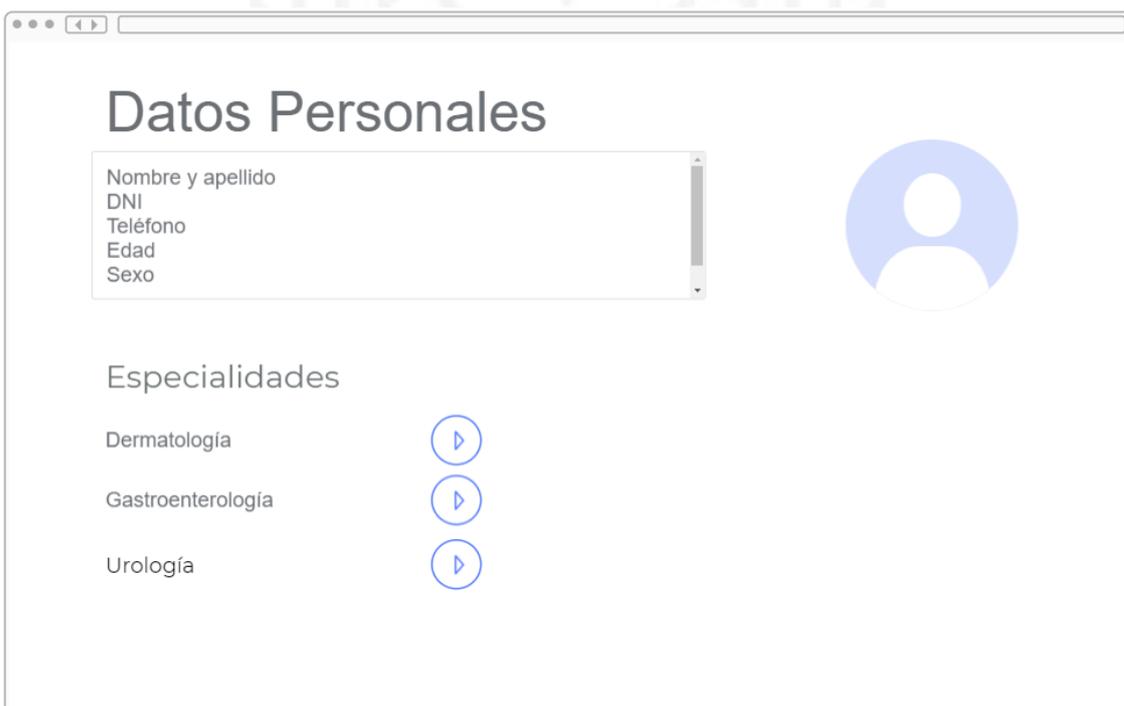
Se muestra la pantalla de Login para el paciente



The screenshot shows a web browser window with the title "Historia Clínica en línea". On the left, there is a placeholder icon for a profile picture. The main content area contains a login form with the following elements:

- A label "Usuari" followed by a text input field containing "Ingrese DNI".
- A label "Contraseña" followed by a password input field containing "*****".
- Two blue buttons: "Ingresar" and "Cancelar".
- Two links: "Registrar Usuario" and "Olvido de contraseña".

La siguiente pantalla posterior al login satisfactorio se muestra las especialidades en las que el paciente se ha atendido.



The screenshot shows a web browser window with the title "Datos Personales". The page is divided into two main sections:

- Datos Personales:** A list of personal data fields: "Nombre y apellido", "DNI", "Teléfono", "Edad", and "Sexo". To the right of this list is a circular profile picture placeholder.
- Especialidades:** A list of medical specialties with corresponding play button icons: "Dermatología", "Gastroenterología", and "Urología".

Al hacer clic Dermatología, se observará el detalle de todas las citas que haya tenido el paciente así como las clínicas donde se atendió en esa especialidad.

The screenshot shows a web browser window with the title "Datos Personales". On the left, there is a scrollable list of personal data fields: "Nombre y apellido", "DNI", "Teléfono", "Edad", and "Sexo". To the right of this list is a blue circular profile icon. Below the personal data is a table with four columns: "Médico", "Clínica", "Descripción", and "Fecha y hora". The table contains four rows, each starting with a radio button. The second radio button is selected. At the bottom right of the table area, there is a blue button with a right-pointing arrow.

Al seleccionar alguna de las citas se mostrará la receta y tratamiento brindado en aquella oportunidad.

The screenshot shows the same "Datos Personales" page, but with additional information displayed below the personal data. There are two text input fields. The first is labeled "Receta" and contains the text "Placeholder". The second is labeled "Tratamiento" and also contains the text "Placeholder". The rest of the page, including the personal data list and the profile icon, remains the same as in the previous screenshot.

Anexo 14: Ficha Técnica de Entrevista Abierta

DIRECCIÓN: Las entrevistas de este proyecto fueron realizadas por Michael Olaya, Bachiller de la Universidad de Lima

TÉCNICA: El tipo de entrevista utilizada fue la entrevista abierta no estructurada sin un orden preestablecido pero con el objetivo de identificar los problemas más relevantes para los pacientes y médicos, asimismo en una segunda iteración para determinar si el problema seleccionado es relevante para el segmento de clientes escogido. Se optó por este tipo de entrevistas con la finalidad de conducir la comunicación activa parecida a una conversación permitiendo la espontaneidad.

FECHA DE REALIZACIÓN: Las entrevistas fueron realizadas entre 15 de Abril y 12 de Mayo de 2019.

LISTADO DE ENTREVISTADOS:

Pacientes:

Lidia Aranda

Santiago Cornejo

Renán Guzmán

RosseMarie Espinoza

Jahan Silva

Ángelo Danielli

Claudia Díaz

Christian Burgos

Gerardo Florindez

Elisa Escudero

Lisset Juárez

José Atoche

José Araujo

Maritza

Yesenia Flores

David Pauta

Ricardo Pachas

Lily Muro

Iveth Ramírez

Paul Palacios

Aseneth Uriona

Médicos:

Claudia Fuentes
Javier Vásquez
Miguel Díaz
Carlos Villanueva
Fiorella Aguilar
Kelly Moscoso
Fiorella Núñez



Anexo 15: Guía de entrevista – Paciente y Médico

Pacientes:

1. Indique su rango de edad
2. ¿Alguna vez se ha atendido en una clínica?
3. ¿Cuenta con algún tipo de seguro privado o se atendió de forma particular?
4. ¿Cuál fue el motivo por el cual se atendió en la clínica y no en el seguro?
5. Cuénteme ¿cuál fue su experiencia en su visita al centro de salud? ¿Por qué?
6. ¿Alguna vez se ha hospitalizado? ¿Cómo describirías la atención? ¿Por qué?
7. ¿Se hospitalizó en el mismo centro donde tenían su historia clínica? ¿Siente que la atención era mejor por tener su historia allí? (Si la respuesta fue NO ir a la pregunta 9)
8. ¿Qué retos tecnológicos encuentra para que la atención mejore? Por ejemplo contar con citas por internet, pagos en línea, un Sistema que controle su historial médico, entre otras.
9. Si la respuesta fue NO: ¿Que trámites administrativos tuvo que realizar para ser atendido en el nuevo centro de salud? ¿cuánto tiempo demoró?
 - ¿Cómo describiría el proceso?
 - ¿Cómo se sintió en ese momento? ¿Qué retos encuentra para mejorar? ¿Por qué?
 - ¿Cuándo se atendió en la nueva clínica y como parte del tratamiento de su enfermedad tenía análisis, exámenes médicos (resonancias, rayos x, endoscopia, entre otros) tuvo que hacerlos nuevamente?
 - ¿Qué sintió en ese momento?
 - ¿Cuándo cambia de centro de salud se acuerda de los medicamentos y dosis que tomó?
 - ¿Cree que es conveniente que cuando usted pase en atenderse a otro centro de salud, el nuevo centro pueda tener en la base de datos su información llamase historial médico, el cual le permita al médico saber los exámenes, resultados de los mismos, tratamientos recibidos, medicación y dosis: para que puedan continuar con el tratamiento?

Emergencia

10. ¿Alguna vez fue atendido de emergencia en un centro donde antes no lo hacía?
11. Cuénteme ¿cómo se sentía cuando le hacían las preguntas que se suelen hacer para llenar antecedentes antes de iniciar con la atención de la emergencia?
12. ¿Cree que es importante contar con el historial médico en línea? ¿Por qué?,
13. ¿Cómo cree que pueda ayudar el hecho de tener el historial médico en línea? Por ejemplo continuar con algún tratamiento, revisar exámenes médicos, entre otros

Respecto al proyecto

14. Si tuviera su historia clínica en línea, ¿qué tipo de información le gustaría visualizar?
15. ¿Quiénes podrían tener acceso a su historia Clínica? ¿Quién debería poder brindar o quitar acceso a esta información? Por ejemplo usted, el estado, la institución donde se atiende
16. ¿Qué le preocuparía respecto al hecho de que su historia clínica este en internet? ¿Por qué?
17. ¿Estaría dispuesto a pagar para contar con dicho servicio? ¿Por qué?
18. ¿Cuánto estaría dispuesto a pagar? ¿Por qué?

Médicos:

- ¿Cuándo llega un enfermo a emergencias, por su estado crítico de salud y si nunca se atendió en el centro de salud, cómo sabe si es alérgico a un medicamento o qué antecedentes de salud tiene para evitar una negligencia médica?
- ¿ha utilizado algún sistema de información hospitalaria? ¿Cómo se ha sentido al utilizar dicho sistema? ¿Podría ayudarme describiendo el por qué?
- ¿Siente que es de ayuda el sistema? ¿Por qué?
- ¿Cómo cree que se pueda mejorar el procedimiento para la utilización de dicho sistema?
- ¿Qué opina de la posibilidad de contar con historias clínicas en línea, que le sirva como apoyo en la toma de decisiones en los casos de hospitalización o emergencia, independientemente si el paciente se atiende o no en la clínica? ¿Por qué?
- ¿Qué retos encuentra para la utilización de la información de las historias clínicas en línea en los casos de hospitalización y emergencias? ¿Por qué?
- ¿Cuándo le ha tocado tratar a pacientes referidos de otros centros de salud, A pesar que trajo sus análisis y resultados tuvo que iniciar nuevamente los exámenes para tener la corroboración de los datos? ¿Me podría ayudar a entender por qué se debe actuar de esa forma? Los pacientes o familiares ¿muestran algún tipo de resistencia a este procedimiento?
- De su experiencia, le ha pasado que algunos pacientes o familiares, han extraviado algunos documentos de su historial clínico ¿Que sugiere usted en esa situación? Por ejemplo que se vuelva a realizar el examen, que solicite una copia al centro de salud de donde proviene, entre otras
- ¿De los pacientes que atiende, suelen recordar los tratamientos, medicamentos recetados por otro médico? ¿Le ayudaría tener esta información? ¿de qué manera le serviría esta información?
- ¿Cree que es importante contar con un sistema que centralice las historias clínicas de los pacientes? ¿Por qué?
- ¿Cómo se siente con el uso de del sistema hospitalario que tiene la clínica?

Anexo 16: Estado de Ganancias y Pérdidas

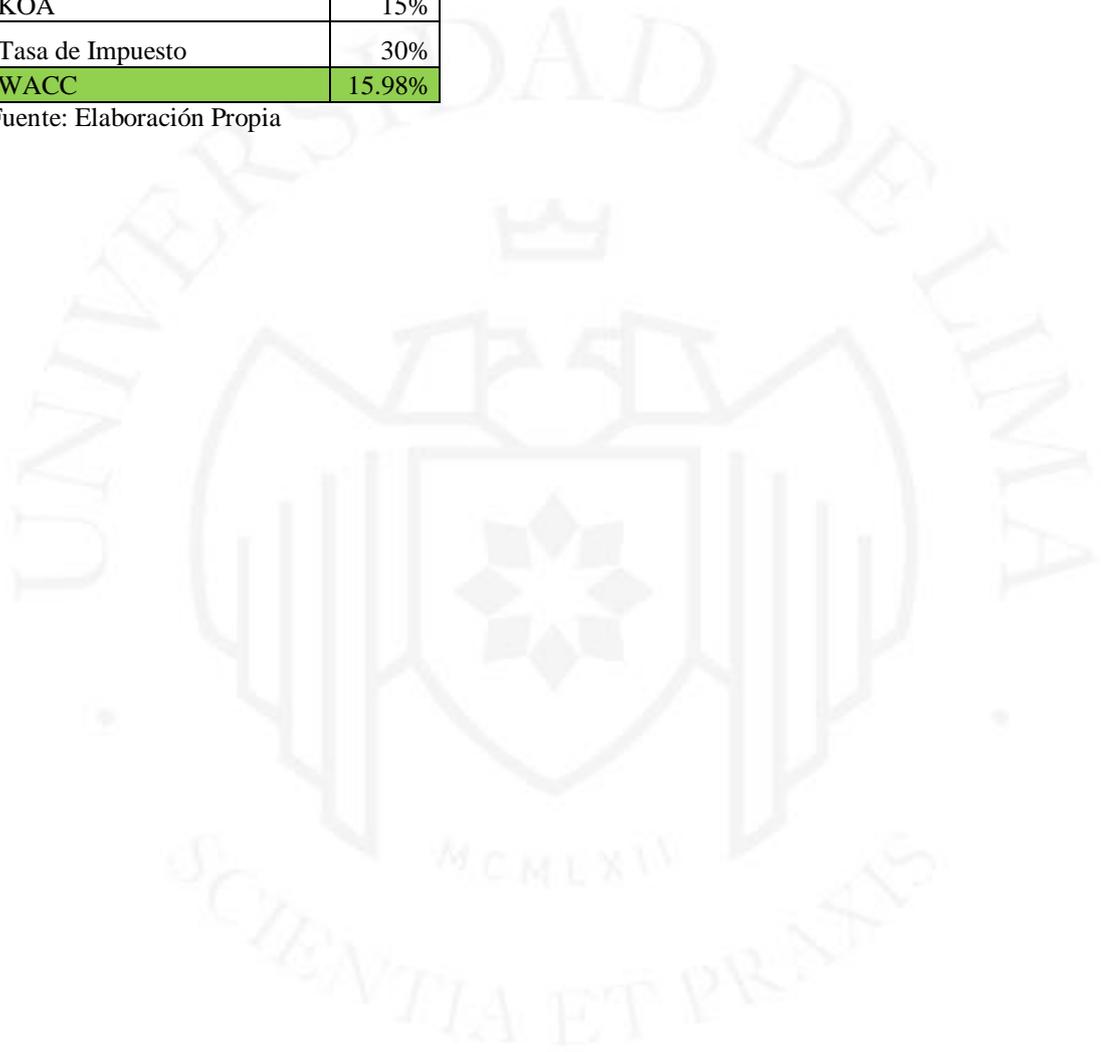
RUBRO	AÑOS				
	AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5
Ventas	29663.13	87506.23	197408.13	345775.69	513925.59
Costo de mantenimiento	56040	59292	62751.6	66433.68	70354.31
Utilidad Bruta	-26376.87	28214.23	134656.53	279342.01	443571.28
Gastos Generales	1941.18	2038.24	2140.15	2247.15	2359.51
Gastos Administrativos	18943.77	19890.95	20885.50	21929.78	23026.27
Gastos de Ventas	1200	1260	1323	1389.15	1458.61
Utilidad de Operación	-48461.81	5025.04	110307.88	253775.93	416726.89
Gastos Financieros	5013.33	2003.04	0	0	0
Utilidad Antes de Impuestos	-53475.14	3022.00	110307.88	253775.93	416726.89
Impuestos (30%)	0.00	906.60	33092.36	76132.78	125018.07
Utilidad Neta (Dólares)	-53,475.14	2,115.40	77,215.52	177,643.15	291,708.83

Fuente: Elaboración Propia

Anexo 17: Determinación del WACC

% Deuda	10%
% Capital	90%
TCEA	35.39%
KOA	15%
Tasa de Impuesto	30%
WACC	15.98%

Fuente: Elaboración Propia



Anexo 18: Periodo de recuperación de la Inversión – Económico

	0	1	2	3	4	5
Flujos Netos	-190,512.94	-48,461.81	4,118.44	77,215.52	177,643.15	464,981.77
Flujos Netos Descontados	(190,512.94)	(41,784.63)	3,061.73	49,494.31	98,178.42	221,574.82
Flujo Neto Acumulado	(190,512.94)	(232,297.57)	(229,235.84)	(179,741.53)	(81,563.11)	140,011.71

Periodo de Recuperación de la Inversión	4 AÑOS 5 MESES	4.37
--	-----------------------	------

Fuente: Elaboración Propia



Anexo 19: Periodo de recuperación de la Inversión – Financiero

	0	1	2	3	4	5
Flujos Netos	(170,512.94)	(61,970.00)	(9,389.74)	77,215.52	177643.15	464981.766
Flujos Netos Descontados	(170,512.94)	(53,886.95)	(7,099.99)	50,770.46	101,568.05	231,178.12
Flujo Neto Acumulado	(170,512.94)	(224,399.90)	(231,499.89)	(180,729.43)	(79,161.39)	152,016.73

Periodo de Recuperación de la Inversión	4 AÑOS 5 MESES	4.34
--	-----------------------	------

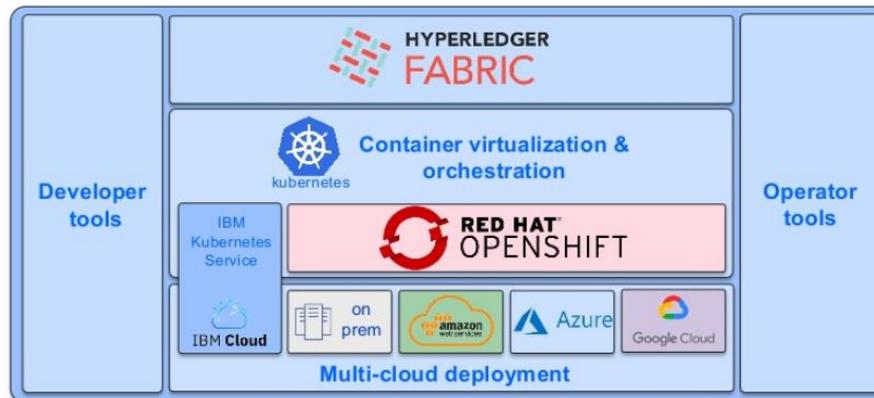
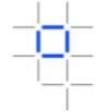
Fuente: Elaboración Propia



Anexo 20: Componentes de la plataforma Blockchain de IBM

Introducing IBM Blockchain Platform

Build, operate and grow Hyperledger Fabric networks



Advanced tooling

Create & manage smart contracts, applications & networks

Open technology

Hyperledger Fabric, Containers, Kubernetes

Deploy anywhere

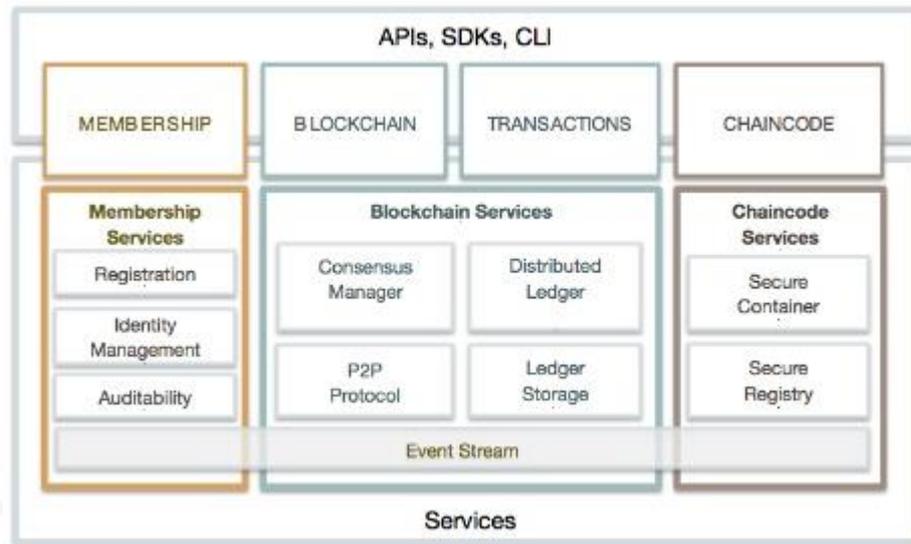
Comprehensive cloud & on-premises options

IBM Blockchain

IBM



Anexo 21: Arquitectura de Hyperledger Fabric



Anexo 22: Codificación

```
1 Model .cto
2 namespace org.blocknitive.hc
3 //Estados por los que pasa la HC de un paciente
4
5 enum Estado {
6   o Nuevo
7   o Modificando
8   o Actualizado
9 }
10
11 concept DatosGenerales {
12   o String email
13   o String telefono
14   o String ciudad
15   o String direccion1
16   o String direccion2 optional
17 }
18
19 //Creamos Hospital y agregamos el concepto Datos generales
20 participant Institucion identified by ruc {
21   o String ruc
22   o String razonsocial
23   o String nombrecomercial
24   o String director
25   o String rlegal
26   o DatosGenerales datosgenerales optional
27   //o DateTime dob optional
28   //o String[] authorized optional
29 }
30
```



```

31 //Creamos paciente y agregamos el concepto Datos generales
32 participant Paciente identified by dni {
33   o String dni
34   o String nombre
35   o String apellido1
36   o String apellido2
37   //o HistCli nhc
38   o String profesion
39   o String gruposanguineo
40   o String estcivil
41   o DateTime fechaNacimiento
42   o DatosGenerales datosgenerales optional
43   o String[] authorized optional
44 }
45
46 abstract transaction MemberTransaction {
47   o String memberId
48 }
49
50 //Declaramos el asset HC
51 asset HistCli identified by nhc {
52   o String nhc
53   o String diagnostico
54   o String receta
55   o String alergias
56   o Estado estado
57   o String observaciones optional
58   --> Institucion institucion
59   --> Paciente paciente
60 }
61
62 transaction AuthorizeAccess extends MemberTransaction {
63 }
64
65 transaction RevokeAccess extends MemberTransaction {
66 }
67
68 //Declaramos la transaccion que despues definiremos
69 transaction ActualizaHistoria {
70   o Estado estadoHistoria
71   --> HistCli historia
72 }
73
74 event MemberEvent {
75   o MemberTransaction memberTransaction
76 }
77
78 //Creamos un evento cuando actualicemos la historia
79 event EventoActualizaHistoria {
80   o Estado estadoHistoria
81   o HistCli historia
82 }

```

```

84 Script file .js
85
86 /* global getCurrentParticipant getParticipantRegistry getFactory emit */
87
88 /**
89  * A Member grants access to their record to another Member.
90  * @param {org.blocknitive.hc.AuthorizeAccess} authorize - the authorize to be processed
91  * @transaction
92  */
93 async function AuthorizeAccess(authorize) { // eslint-disable-line no-unused-vars
94
95     const me = getCurrentParticipant();
96     console.log('**** AUTH: ' + me.getIdentifier() + ' granting access to ' + authorize.memberId );
97
98     if(!me) {
99         throw new Error('A participant/certificate mapping does not exist.');
```

```

100     }
101
102     // if the member is not already authorized, we authorize them
103     let index = -1;
104
105     if(!me.authorized) {
106         me.authorized = [];
107     }
108     else {
109         index = me.authorized.indexOf(authorize.memberId);
110     }
111
112     if(index < 0) {
113         me.authorized.push(authorize.memberId);
114
115         // emit an event
116         const event = getFactory().newEvent('org.blocknitive.hc', 'MemberEvent');
117         event.memberTransaction = authorize;
118         emit(event);
119
120         // persist the state of the member
121         const memberRegistry = await getParticipantRegistry('org.blocknitive.hc.Institucion');
122         //await memberRegistry.update(authorize.memberId);
123         await memberRegistry.update(me);
124     }
125 }
126
127 /**
128  * A Member revokes access to their record from another Member.
129  * @param {org.blocknitive.hc.RevokeAccess} revoke - the RevokeAccess to be processed
130  * @transaction
131  */
132 async function revokeAccess(revoke) { // eslint-disable-line no-unused-vars
133
134     const me = getCurrentParticipant();
135     console.log('**** REVOKE: ' + me.getIdentifier() + ' revoking access to ' + revoke.memberId );
136
137     if(!me) {
138         throw new Error('A participant/certificate mapping does not exist.');
```

```

139     }
140
141     // if the member is authorized, we remove them
142     const index = me.authorized ? me.authorized.indexOf(revoke.memberId) : -1;
143
144     if(index>-1) {
145         me.authorized.splice(index, 1);
146
147         // emit an event
148         const event = getFactory().newEvent('org.blocknitive.hc', 'MemberEvent');
149         event.memberTransaction = revoke;
150         emit(event);
151
152         // persist the state of the member
153         const memberRegistry = await getParticipantRegistry('org.blocknitive.hc.Institucion');
154         await memberRegistry.update(me);
155     }
156 }

```

```

157
158 /**
159  * Actualizar el estado de la historia clinica del paciente.
160  * @param {org.blocknitive.hc.ActualizaHistoria} historiaActualiza - ActualizaHistoria a ser procesada
161  * @transaction
162  */
163
164 async function actualizaHistoria(historiaActualiza) {
165
166     var logAntiguoEstado = historiaActualiza.historia.estado;
167     historiaActualiza.historia.estado = historiaActualiza.estadoHistoria;
168     console.log('Actualizando estado historia');
169     return getAssetRegistry('org.blocknitive.hc.historia')
170     .then (function (assetRegistry){
171         return assetRegistry.update(historiaActualiza.historia);
172     })
173     .then (function(){
174         var event = getFactory().newEvent('org.blocknitive.hc','EventoActualizaHistoria');
175         event.Historia = historiaActualiza.historia;
176         event.estadoHistoria = logAntiguoEstado;
177         exit(event);
178     });
179 }
180
181 Access Control .acl
182 rule AuthorizeAccessTransaction {
183     description: "Allow all participants to submit AuthorizeAccess transactions"
184     participant: "ANY"
185     operation: CREATE
186     resource: "org.blocknitive.hc.AuthorizeAccess"
187     action: ALLOW
188 }
189
190 rule RevokeAccessTransaction {
191     description: "Allow all participants to submit RevokeAccess transactions"
192     participant: "ANY"
193     operation: CREATE
194     resource: "org.blocknitive.hc.RevokeAccess"
195     action: ALLOW
196 }
197
198 rule PacienteVeSuHistoria {
199     description: "Los Pacientes pueden ver solo su historia clinica"
200     participant(p): "org.blocknitive.hc.Paciente"
201     operation: READ
202     resource(h): "org.blocknitive.hc.HistCli"
203     condition: (p.getIdentifier() == h.paciente.getIdentifier())
204     action: ALLOW
205 }
206
207 rule InstitucionesdeSaludPuedenCrearHistorias {
208     description: "Las Instituciones de salud pueden crear Historias clinicas"
209     participant(p): "org.blocknitive.hc.Institucion"
210     operation: CREATE, UPDATE
211     resource(h): "org.blocknitive.hc.HistCli"
212     condition: (p.getIdentifier() == h.institucion.getIdentifier())
213     action: ALLOW
214 }
215
216 rule InstitucionesdeSaludPuedenLeerHistorias {
217     description: "Las Instituciones de salud pueden leer Historias clinicas de pacientes"
218     participant: "org.blocknitive.hc.Institucion"
219     operation: READ
220     resource: "org.blocknitive.hc.*"
221     action: ALLOW
222 }

```

```

223 rule OwnRecordFullAccess {
224     description: "Allow all participants full access to their own record"
225     participant(p): "org.blocknitive.hc.Paciente"
226     operation: ALL
227     resource(r): "org.blocknitive.hc.HistCli"
228     condition: (r.getIdentifier() == p.getIdentifier())
229     action: ALLOW
230 }
231
232 rule ForeignRecordConditionalAccess {
233     description: "Allow participants access to other people's records if granted"
234     participant(p): "org.blocknitive.hc.Institucion"
235     operation: ALL
236     resource(r): "org.blocknitive.hc.HistCli"
237     condition: (r.authorized && r.authorized.indexOf(p.getIdentifier()) > -1)
238     action: ALLOW
239 }
240
241 rule SystemACL {
242     description: "System ACL to permit all access"
243     participant: "org.hyperledger.composer.system.Participant"
244     operation: ALL
245     resource: "org.hyperledger.composer.system.*"
246     action: ALLOW
247 }
248
249 rule NetworkAdminUser {
250     description: "Grant business network administrators full access to user resources"
251     participant: "org.hyperledger.composer.system.NetworkAdmin"
252     operation: ALL
253     resource: "*"
254     action: ALLOW
255 }
256
257 rule NetworkAdminSystem {
258     description: "Grant business network administrators full access to system resources"
259     participant: "org.hyperledger.composer.system.NetworkAdmin"
260     operation: ALL
261     resource: "org.hyperledger.composer.system.*"
262     action: ALLOW
263 }

```