ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

SOLUCIONES TECNOLÓGICAS PARA DAR CUMPLIMIENTO CON LO ESTABLECIDO CON LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN CIENCIAS DE LA COMPUTACIÓN

MILAN LEONARDO CONTRERAS ANDRADE
milan.contreras@epn.edu.ec

DIRECTORA: PhD. GABRIELA LORENA SUNTAXI OÑA
gabriela.suntaxi@epn.edu.ec

Quito, abril 2023

CERTIFICACIONES

Yo, MILAN LEONARDO CONTRERAS ANDRADE declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

MILAN LEONARDO CONTRERAS ANDRADE

Certifico que el presente trabajo de integración curricular fue desarrollado por MILAN LEONARDO CONTRERAS ANDRADE, bajo mi supervisión.

PhD. Gabriela Lorena Suntaxi Oña
DIRECTORA DE PROYECTO

Certificamos que revisamos el presente trabajo de integración curricular.

Nombre1 Nombre2 Apellido1 Apellido2
REVISOR1 DEL TRABAJO
DE INTEGRACIÓN CURRICULAR

Nombre1 Nombre2 Apellido1 Apellido2
REVISOR2 DEL TRABAJO
DE INTEGRACIÓN CURRICULAR

DECLARACIÓN

Yo, MILAN LEONARDO CONTRERAS ANDRADE , declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

MILAN LEONARDO CONTRERAS ANDRADE

DEDICATORIA

A mi mamá quien me ha dado todo su amor sin esperar nada a cambio y siempre ha sabido darme los mejores consejos.

A mi papá, quien ha sabido transmitirme todos sus conocimientos y darme todo el amor siendo mi mejor amigo.

A mi hermana, quien me enseña que alguien tan chiquita puede sentir tanto amor.

Y a mi compañera, quien a sabido estar a mi lado sin condiciones y me ha enseñado lo lindo de ser amado todos los días.

AGRADECIMIENTOS

Agradezco a todas la personas que formaron parte de esta etapa en mi vida. A mis amigos, compañeros, colegas y profesores. Quiero que sepan que es gracias a ustedes el profesional que soy el día de hoy.

De igual forma quiero agradecer a mi Directora de Proyecto Grabriela Suntaxi quien me apoyó durante todo el proceso y fue vital para el proyecto.

Finalmente, quiero agradecer especialmente a la docente Jenny Torres, quien demostró ser una docente que enseña con el corazón. Es la primera persona que confió en mi y es algo que lo llevo en el corazón.

CONTENIDO

RESUMEN

Este documento presenta como resultado, un prototipo a modo de aplicación web el cual cumpla con los requerimientos de la Ley Orgánica Contra La Protección de Datos Personales en Ecuador. El prototipo se centra en la gestión del consentimiento por parte del titular de los datos, el control de acceso y la portabilidad de los datos.

Para llegar a la solución propuesta, se realizó una investigación sobre la Ley Orgánica de Protección de Datos Personales, para tener una mejor visión sobre los requerimientos. De igual forma, se investigó sobre los controles internacionales presentes en la protección de datos. Para saber si existían documentos o aplicaciones con respecto a cumplir con las leyes establecidas en la Ley Orgánica contra la Protección de Datos Personales en Ecuador, se llevó a cabo una revisión sistemática de la literatura de la cual se realiza un análisis para obtener los mejores resultados y en base a ellos diseñar y realizar el desarrollo del prototipo.

El documento presenta las tecnologías usadas para el prototipo, así como el funcionamiento del mismo. Finalmente, se muestran los resultados y de igual forma se proponen mejoras las cuales pueden ser añadidas al prototipo para tener nuevas funcionalidades.

Palabras Claves: Consentimiento, Acceso, Portabilidad, Ecuador, LOPDP, GDPR.

ABSTRACT

This document presents a prototype as a web application to comply with the requirements of the Organic Law on Personal Data Protection. The prototype focuses on the management of consent by the data owner, access control and data portability.

In order to arrive at the proposed solution, an investigation was carried out on the Organic Law on Personal Data Protection, to have a better vision of the requirements. In the same way, international controls present in data protection were investigated. In order to find out if there were documents or applications with respect to complying with the laws established in the Organic Law on Personal Data Protection in Ecuador, a systematic review of the literature was carried out. Based on the results of the systematic literature review, we design and carry out the development of a prototype.

The document presents the technologies used for the development of the prototype, as well as its operation. Finally, the results are shown and in the same way improvements are proposed which can be added to the prototype to have new functionalities.

Keywords: Consent, Access, Portability, Ecuador, LOPDP, GDPR.

1 INTRODUCCIÓN

La tecnología con el paso de los años sigue evolucionando y conforme la tecnología evoluciona, los datos se vuelven cada vez más importantes. Como dijo Clive Humby “Los datos son el nuevo petróleo” [1] y a lo que se refiere es que, así como al petróleo se le debe dar tratamientos para obtener gasolina u otros combustibles o materiales, a los datos de igual forma se los deben tratar para que puedan tener valor. Clive Humby estuvo tan en lo cierto que actualmente, en el 2022, los datos representan poder; quien tenga más datos y los trate de la mejor forma tendrá más poder que aquellos que no los tengan.

Un ejemplo claro es la venta de productos, pues quienes puedan seccionar mejor su mercado serán quienes obtengan mejores resultados y por consecuencia más ganancias. O inclinándonos un poco más hacia el lado político quienes conozcan mejor a la gente podrán llegar a ellos de una mejor manera, pudiendo así ganar una campaña o manejar mejor a quienes gobierna. Posiblemente para muchos no sea un problema que las empresas tengan nuestra información, pero puede llegar un punto en que se suba información que no deseamos que esté en internet y una vez en internet perdemos control total sobre esa información.

Por lo tanto, las personas suben sus datos a internet sin el conocimiento de que alguien está almacenado esos datos y está lucrando de los mismos y más importante aún es que posiblemente se esté violando su privacidad. Debido a esto en Europa, nace en el 2012 el GDPR que es el Reglamento General de Protección de Datos, el cual tiene como objetivo principal que los propios usuarios sean quienes tengan el control sobre sus datos. En vista del gran impacto de este reglamento en Ecuador se buscó aplicar un reglamento similar. Para lo cual se creó la LOPDP que es la Ley Orgánica de protección de Datos Personales de Ecuador. De igual forma que la GDPR presenta reglas que aseguren la privacidad, el consentimiento y el acceso de los datos personales de los usuarios. Estas reglas deben ser

usadas por las empresas que manejan datos.

Las empresas ecuatorianas tienen un periodo de dos años para adaptarse a estas leyes; es decir, deben buscar herramientas para cumplir con la LOPDP. Con este trabajo se encontrarán soluciones para el cumplimiento de estas leyes. Estas soluciones serán métodos o herramientas las cuales nos ayuden a gestionar el consentimiento al igual que el acceso a los datos, y garantizar el derecho a la portabilidad. Las soluciones serán encontradas mediante la realización de una revisión sistemática de la literatura. Posteriormente se realizará un prototipo basado en una solución para la gestión del consentimiento y acceso a la información como lo establece la LOPDP.

1.1 OBJETIVO GENERAL

Generar un prototipo de una solución de privacidad basado en herramientas centradas en el usuario para la gestión del consentimiento y acceso a su información personal con el fin de garantizar el derecho a la portabilidad establecido en la LOPDP.

1.2 OBJETIVOS ESPECÍFICOS

- ❒ Realizar una revisión sistemática para identificar las soluciones a la gestión de consentimiento, control de acceso y portabilidad de datos personales.
- ❒ Realizar el análisis de una solución para la gestión de consentimiento y control de acceso y portabilidad de datos personales.
- ❒ Desarrollar un prototipo de software que garantice la gestión de consentimiento y control de acceso y portabilidad de datos personales.

1.3 ALCANCE

Para el desarrollo del proyecto se tomará como marco de referencia la metodología propuesta por J. vom Brocke, A. Hevner y A. Maedche en [2] . La metodología contempla las siguientes fases: Identificación del problema y motivación, definición de objetivos para una

solución, diseño y desarrollo, demostración, evaluación y comunicación.

En la fase de identificación del problema y motivación, se definirá el problema de investigación el cual está orientado con buscar soluciones que ayuden al cumplimiento de la LOPDP, específicamente sobre el control de acceso, gestión del consentimiento y a la portabilidad; y se justificará la necesidad de una solución.

Se definirán los objetivos para el problema de investigación planteado. Se realizará la revisión sistemática de la literatura para la gestión de consentimiento y control de acceso con la metodología propuesta por B. Kitchenham y S. Charters.[3] la cual está compuesta de 6 pasos: preguntas de investigación, proceso de búsqueda, Criterios de inclusión y exclusión, selección de artículos, evaluación de calidad y extracción de datos.

Las fases de diseño y desarrollo, demostración y evaluación se las ejecutó en base a la metodología Scrum que se plantea en [4], estas fases contemplan el desarrollo del prototipo de software.

Finalmente, en la fase de comunicación, se realiza una publicación formal con los hallazgos del proyecto.

2 MARCO TEÓRICO

Los datos personales de las personas circulan por todo el internet, y no existe un control sobre estos. Es ahí donde nace la necesidad de controlar el manejo de estos datos, garantizando la privacidad y seguridad de los mismos. Y es esta la razón por la cual países han decidido crear regulaciones.
Ecuador, en mayo del 2021 presentó la Ley Orgánica de Protección de Datos Personales, la cual busca que los titulares de la información sean quienes puedan tener el control sobre la misma. Ecuador dio plazo a las empresas a cumplir con esta ley hasta el 26 de mayo de 2023. En este documento se verán soluciones para cumplir puntos específicos de esta ley. Centrados en la gestión de acceso, la gestión de consentimiento y la portabilidad de los datos por lo que abarcaremos mas sobre estos temas y términos relacionados con estos.
Actualmente existen estándares internacionales para la seguridad por lo que se estarán usando los estándares ISO-27001 Y NIST sp 800-53 los cuales están asociados a la seguridad informática y realizarán una gran aportación a este trabajo.

2.1 SEGURIDAD Y PRIVACIDAD DE LOS DATOS

Si bien los datos personales pertenecen al usuario estos están siendo almacenados en una empresa y esto quiere decir que estos datos pueden ser comprometidos. Para asegurase de que esto no suceda, las empresas deben garantizar la seguridad y la privacidad de los datos.

2.1.1 Seguridad de los datos

Es un área de la protección de datos que se refiere a como son protegidos los datos para evitar que los mismos sean comprometidos. Por ejemplo con el cifrado de los datos, el

respaldo de la información, autenticación, entre otros. Es un enfoque mas hacia el lado de proteger los datos contra amenazas maliciosas. Es muy común escuchar sobre la triada CIA cuando se habla sobre la seguridad de los datos, ya que es un acrónimo sobre los principios de la seguridad de los datos, confidencialidad, integridad y disponibilidad.

2.1.2 Privacidad de los datos

Es un área de la protección de datos que se refiere a el manejo adecuado de los datos. Es decir como estos serán manejados, recopilados o entregados. Por lo que principalmente en este punto podemos encontrar la gestión de acceso, donde se determina quien puede y quien no acceder a los datos. De la mista forma en este punto se incluye la gestión del consentimiento donde estaríamos abarcando como el usuario autoriza que sus datos sean utilizados y de igual forma si autoriza a que estos sean compartidos con terceros o no. Más adelante veremos de forma más específica la gestión de acceso y consentimiento. Para el correcto manejo de los datos se proporcionan documentos o leyes, y un claro ejemplar es la Ley Orgánica de Protección de Datos Personales que será descrita en la sección 2.3. De igual forma, existen otros ejemplares equivalentes a la ley de Ecuador pero para otros países o regiones, como es la GDPR (Reglamento General de Protección de Datos) para la unión Europea y CCPA (Ley de privacidad del consumidor de California) para California en E.E.U.U.

2.2 CONTROLES INTERNACIONALES PARA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

2.2.1 ISO-27001

En primer lugar ISO es la Organización Internacional de Normalización, la cual realiza normas técnicas internacionales. La ISO-27001 se refiere específicamente a normas relacionadas con sistemas de gestión de la seguridad de la información. Esta norma aborda tres puntos importantes, la confidencialidad, integridad y seguridad de los datos y de la información. [5].

2.2.2 NIST sp 800-53

NIST es el instituto de nacional de estándares y tecnología. Lo que buscan es promover la innovación y la competencia industrial. La NIST sp 800-53 es una publicación en la cual se abordan los temas de controles para la seguridad y privacidad para los sistemas de información y las organizaciones[6].

2.3 LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (LOPDP)

En el Registro Oficial Suplemento No. 459 de 26 de mayo de 2021 se publicó la Ley Orgánica de Protección de Datos Personales. Dentro de este se estipula que las empresas dentro del territorio ecuatoriano tendrán un periodo de dos años, es decir hasta el 26 de mayo del 2023 para cumplir las leyes de este documento[7].

Esta ley tiene como objetivo principal garantizar el ejercicio al derecho a la protección de datos personales. Es decir, el propietario de los datos tendrá el derecho a decidir quien puede tener sus datos, saber como están siendo manejados sus datos, saber que datos poseen las empresas y con quienes se están compartiendo los datos. Los datos deben ser tratados como lo imponen la ley para que estos sean legítimos, caso contrario serán sancionados con lo especificado en el mismo documento. A continuación, se muestran los principales derechos de la ley:

- A la información: el titular de los datos tiene derecho a saber los fines del tratamiento, la base legal para el tratamiento, los tiempos de conservación, la existencia de una base de datos donde estén sus datos, el origen de sus datos personales si no fueron obtenidos por parte del titular, identidad y datos de contacto de quien esté encargado del tratamiento, entre otras. Es decir, el usuario tiene el derecho a saber todo lo que ocurre con sus datos [7].
- Al acceso: El titular de los datos tiene el derecho a recibir toda la información sobre sus datos de forma gratuita por parte del responsable del tratamiento [7].
- A la rectificación y actualización: El titular tiene el derecho a rectificar o actualizar sus datos personales inexactos o incompletos [7].

- ❒ A la eliminación: En ciertos casos el titular tiene el derecho a que el tratador elimine sus datos personales [7].
- ❒ A la oposición: El titular tiene el derecho a oponerse a que sus datos sean tratados [7].
- ❒ A la portabilidad: El titular tiene el derecho a obtener sus datos en un formato compatible, actualizado, estructurado, común, ínteroperable y de lectura mecánica, preservando sus características por parte del responsable del tratamiento [7].
- ❒ A no ser objeto de de una decisión basada única o parcialmente en valoraciones automatizadas [7].
- ❒ A la consulta pública y gratuita ante el Registro Nacional de Protección de Datos Personales [7].

Como ya se había mencionado en este documento no centraremos específicamente en la gestión de acceso y consentimiento de los datos así como de su portabilidad. Por lo que a continuación, se mostrará que nos dice la LOPDP sobre estos temas en específico.

2.3.1 Actores

1. **Titular:** Persona quien es dueña de los datos que están siendo tratados por un tercero.
2. **Responsable del tratamiento:** Persona natural o jurídica que es encargada de tratar los datos.
3. **Encargado del tratamiento:** Persona, empresa u organismo que este haciendo uso, es decir tratando datos personales por orden del responsable del tratamiento.
4. **Destinatario:** Persona, empresa u organización que ha recibido datos personales.
5. **Autoridad de Protección de Datos Personales:** Autoridad pública independiente quien será la encargada de que la ley sea cumplida, con respecto s lis datos personales de los titulares.
6. **Delegado de protección de datos personales:** Es el punto intermedio entre el Responsable del Tratamiento y la Autoridad de Protección de Datos Personales. De tal forma que este le recuerda al Responsable del Tratamiento sus obligaciones sobre la ley al igual que vela por el cumplimiento de las mismas.

2.3.2 Gestión de Consentimiento

La gestión del consentimiento hace referencia a la licitud del tratamiento de los datos, es decir si el dueño de los datos está de acuerdo en la forma que serán tratados sus datos y como estos serán compartidos con otros. De igual forma, así como el dueño de los datos da el consentimiento, este puedo retirarlos dándole así el control total sobre los mismos.
A continuación, en la Tabla 2.1 se verán requerimientos asociados a los artículos presentes en la LOPDP.

Tabla 2.1: Requerimientos Control de Acceso

Código	Requerimientos	Artículo
A1	El sistema permitirá al titular de los datos, conocer y obtener todos sus datos que estén siendo usados por un responsable del tratamiento.	13
A2	El sistema permitirá crear un contrato donde se establezca de forma clara y precisa por parte del encargado de los datos como serán usados y tratados los datos del titular.	34
A3	El sistema permitirá al responsable del tratamiento tener acceso a los datos únicamente de cuyos titulares tenga el consentimiento	34

2.3.3 Gestión de Control de Acceso

El control de acceso hace referencia a que un usuario pueda comprobar su identidad. El control de acceso lo podemos encontrar en múltiples lugares, por ejemplo, cuando ingresamos a una discoteca y nos solicitan la cédula o cuando vamos a retirar dinero del banco y nos solicitan nuestra cédula. Como vemos, se necesita de un documento o de un método el cual nos pueda garantizar que es la persona que dice ser para si darle acceso a lo que necesite. Es de la misma forma como funciona en el área de la computación, en este caso los usuarios siempre necesitan tener acceso a datos los cuales están protegidos para que nadie pueda acceder a ellos, y es mediante en control de acceso que verificamos su identidad y se les otorga el acceso a los datos.
A continuación, en la Tabla 2.2 se verán requerimientos asociados a los artículos presentes en la LOPDP.

Tabla 2.2: Requerimientos Control de Consentimiento

Código	Requerimiento	Artículo

C01	El sistema le permitirá al titular de los datos dar el consentimiento en como serán tratados sus datos.	7
C02	El sistema le permitirá al titular revocar el consentimiento de tratamiento por parte del responsable de tratamientos, en cualquier momento.	8
C03	El sistema deberá permitir al titular actualizar en cualquier momento sus datos personales.	12
C04	El sistema deberá permitir al responsable del tratamiento tener acceso siempre a los datos actualizados del titular, siempre y cuando exista el consentimiento.	12
C05	El sistema le permitirá al titular eliminar sus datos personales para que no puedan ser tratados por los responsables del tratamiento	15
C06	El sistema deberá destruir los datos por el lado del responsable de tratamientos, una vez se haya terminado el tiempo establecido en el contrato.	34

2.3.4 Portabilidad

En este contexto la portabilidad de los datos hacen referencia a que estos tengan un formato compatible, actualizado, estructurado, común, interoperable y de lectura mecánica [7]. Con esto nos referimos a que en el momento en que el dueño de los datos los solicite estos deben ser entregado con las característica indicadas anteriormente. Y de igual forma, si un usuario solicita que sus datos sean transferidos a otra empresa estos datos deben tener el mismo formato. El objetivo de esto es que el usuario tenga un mayor control sobre sus datos, pudiendo el mismo entender que datos están siendo usados y de igual forma transportarlos de tal forma que si desea entregarlos a una nueva empresa sea fácil comenzar con el tratamiento de los mismos. Cabe recalcar que la portabilidad funciona a partir de que existe una gestión de consentimiento y un control de acceso para que se pueda acceder a los datos, la portabilidad se basa más en como sera almacenada la información así como su formato. A continuación, en la Tabla 2.3 se verán requerimientos asociados a los artículos presentes en la LOPDP.

Tabla 2.3: Requerimientos de Portabilidad

Código	Requerimiento	Artículo
P01	El sistema le permitirá al titular recibir sus datos personales tratados por un responsable en formato compatible	17
P02	El sistema le permitirá al titular recibir sus datos personales tratados por un responsable con información actualizada	17

P03	El sistema le permitirá al titular recibir sus datos personales tratados por un responsable en formato interoperable	17
P04	El sistema le permitirá al titular recibir sus datos personales tratados por un responsable en formato de lectura mecánica	17

2.4 BLOCKCHAIN

Blockchain se traduce al español como cadena de bloques. El término fue popularizado en el artículo de Nakamoto[8] en el cual se explica que este era el protocolo usado por la criptomoneda Bitcoin. Este protocolo se encarga de realizar transacciones electrónicas, a forma de un libro de contabilidad digital en el cual se registran todas las transacciones, y son guardadas en una red descentralizada de computadoras.

Para entenderlo de una forma más gráfica podemos entender como bloques, a un conjunto de información. Tomando el ejemplo de Bitcoin cuando se realizan transacciones, estas son verificadas por la red descentralizada, y almacenadas en un bloque. Este nuevo bloque se une a los anteriores mediante una cadena la cual digitalmente es creada mediante el hash de un bloque. El hash es una firma digital del bloque. El hash del bloque anterior es escrito en el bloque actual de tal forma que se puedan relaciona siempre con el bloque anterior y se crea una cadena. Es por eso por lo que el blockchain toma su característica principal, que es la inmutabilidad de los datos que se obtiene gracias a la red descentralizada y a la firma digital. En la Figura 6.6 se puede observar de gráfica el funcionamiento de un blockchain.[9]

Antes de continuar con el blockchain, la firma digital tiene el mismo objetivo que una firma

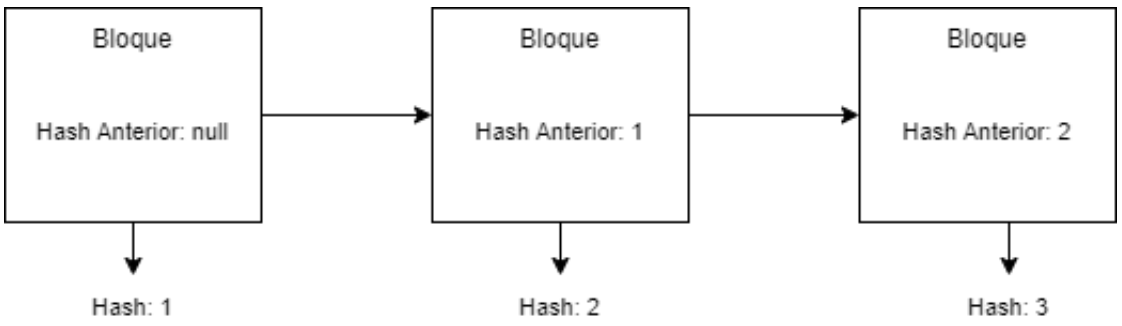

Figura 2.1: Ilustración de funcionamiento de un blockchain. Elaborado por el autor.

normal, que es validar la autenticidad e integridad de un documento. En el caso digital, esta

firma es generada mediante una operación matemática con la cual se aplica un mecanismo criptográfico mediante el cual se obtiene una cadena de caracteres. En el caso digital, en vez de tener un nombre se tienen dos claves, una que es la clave privada con la cual se cifra el documento o la información, y la otra que es la clave publica que es con la cual se descifra, de tal forma que se puede garantizar la autenticidad, en no repudio y la integridad de los datos. Si bien se mostró el funcionamiento del blockchain con las transacciones y criptomonedas. Este solo es un uso de los sin fin de usos que se le puede dar. Lo único que se necesita es información para ser puesta dentro de un bloque y atarlo a una cadena y de esta forma esa información será inmutable.

3 METODOLOGÍA

Para la realización de la investigación se usaron 3 metodologías, una para realización del proyecto que es la metodología DSR propuesta por Jan vom Brocke, Alan Hevner y Alexander Maedche en [2]. Para la elaboración de la revisión sistemática de la literatura se usó la metodología propuesta por B. Kitchenham and S. Charters [3]. Finalmente la metodología para la elaboración del prototipo de software se usó SCRUM, que se encuentra detallada en [4]. De forma resumida se presenta la Figura 3.1. A continuación, se detallan cada una de estas metodologías. Dado que este se trata de un proyecto de integración curricular esta sección fue realizada en conjunto con mi compañero Boris Caiza.

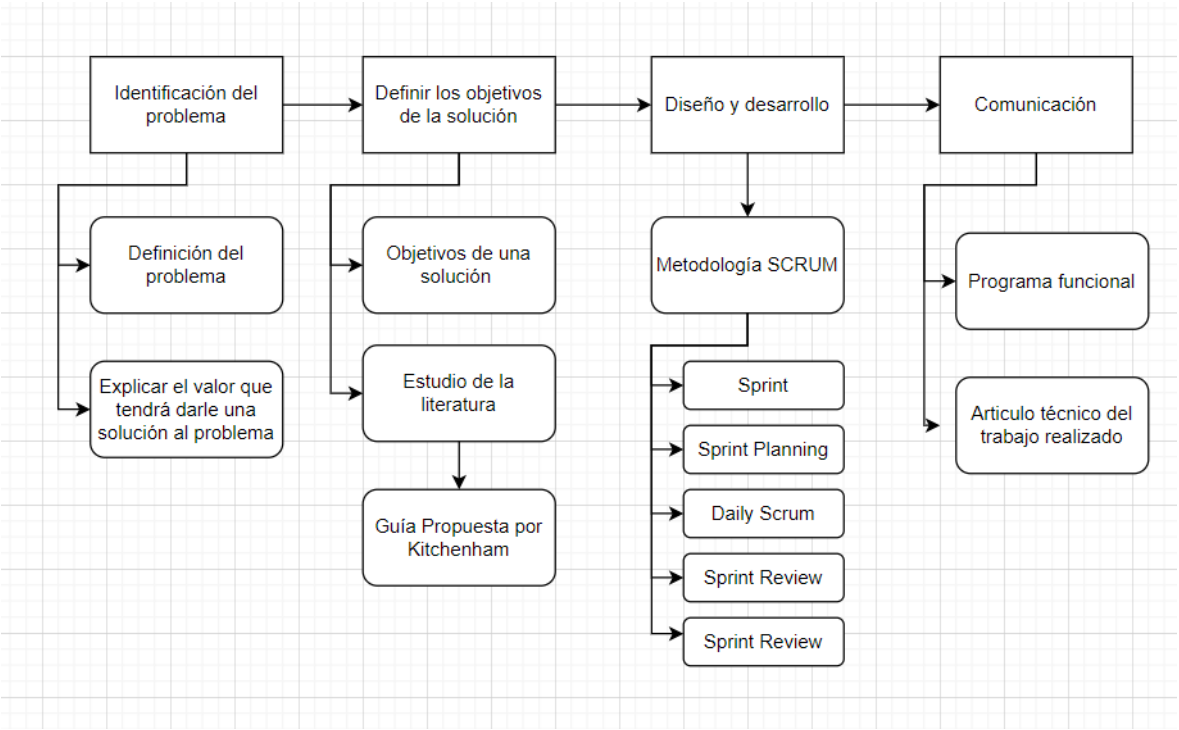

Figura 3.1: Metodología escogida para la investigación. Elaborado por el autor.

3.1 DESIGN SCIENCE RESEARCH (DSR)

"Design Science Research (DSR) es un paradigma de resolución de problemas que busca mejorar la conocimiento a través de la creación de artefactos innovadores. En pocas palabras, DSR busca mejorar bases de conocimiento tecnológico y científico a través de la creación de artefactos innovadores que resuelven problemas y mejorar el entorno en el que se instancian"[2].

DSR consta de 6 actividades las cuales se mencionan a continuación.

1. **Identificación de problemas y motivación**

   Esta actividad identifica un problema de investigación específico y verifica la validez de una solución.Logrando así:

   a) Motivar al investigador.

   b) Ayudar a la audiencia a la comprensión del problema que plantea el investigador.

2. **Definir los objetivos para una solución**

   El objetivo de una solución se puede inferir de definir el problema y saber que se puede hacer. "Los objetivos pueden ser cuantitativos, por ejemplo, términos en los que una solución deseada es mejor que las soluciones existentes, o cualitativos, por ejemplo, una descripción de cómo se espera que un nuevo artefacto ayude con las soluciones a problemas que hasta ahora han permanecido sin resolver [2]".

3. **Diseño y desarrollo**

   Se crea conceptualmente el artefacto. Mediante esta actividad primero se determinan las funcionalidades del producto, su arquitectura y finalmente se podrá crear el producto dadas las especificaciones.

4. **Demostración**

   Esta actividad implica el uso del artefacto como tal. Esto puede involucrar su uso en pruebas, simulaciones, estudios de casos, pruebas o cualquier otra actividad pertinente.

5. **Evaluación**

En esta actividad se evalúa que tan bien el artefacto soluciona el problema planteado. Se comparan los resultados obtenidos con los planteados en los objetivos. Al final de esta actividad, el investigador puede decidir volver al paso tres para intentar mejorar la efectividad del artefacto, o continuar comunicando y dejar otras mejoras para proyectos posteriores.

6. **Comunicación**

   Aquí, todos los aspectos del problema y los artefactos diseñados se comunican a las partes interesadas relevantes.

3.2 REVISIÓN SISTEMÁTICA DE LA LITERATURA

Kitchenham nos propone una guía para realizar revisiones sistemáticas de la literatura[3], específicamente en lo que se refiere a ingeniería de software. Este documento tiene como objetivo, dar las pautas a la comunidad de software para realizar revisiones rigurosas de evidencia empírica actual.

La mayoría de revisiones sistemáticas de la literatura son de temas relacionados a la medicina. Por lo que muchas personas se basaban en estas metodologías y las adaptaban a otras áreas, como en este caso a software. Y es aquí de donde nace esta guía la cual busca las necesidades de los investigadores de ingeniería de software. De igual forma se discuten temas en los cuales la investigación médica difiere de la investigación en ingeniería de software.

Una revisión sistemática de la literatura involucra muchas actividades por lo que para esta guía se han agrupado esas actividades en tres grandes fases: Planificar la revisión, conducir la revisión y reportar la revisión.

3.2.1 Planificar la revisión

En esta sección se planificará como se llevará a cabo la revisión es decir se identificará una necesidad, y se realizarán los protocolos necesarios para la revisión. las etapas relacionadas con esta fase son: Identificación de una necesidad, comisionar una revisión, especificar

las preguntas de investigación, desarrollar un protocolo de revisión y evaluar el protocolo de revisión.

- **Identificación de la necesidad de una revisión sistemática:** Debe existir una necesidad para realizar esta revisión, lo que primero se debe buscar si ya existen revisiones sobre el tema de interés. Y definir las razones por las cuales se decidirá realizar la revisión sistemática de la literatura.

- **Comisionar una revisión:** Este paso se lo realiza en caso de que no seamos nosotros quienes vamos a realizar la revisión, sino que queremos que un tercero lo haga, por lo que deberemos especificar el trabajo que se requiere. De igual forma, si lo miramos desde el otro extremo, este documento ayudará para saber que es lo que el cliente necesita.

- **Especificar las preguntas de investigación:** Esta es una de las partes más importantes de la revisión ya que se tendrá que formular preguntas las cuales se querrá que sean respondidas al final de todo el proceso. Mediante las preguntas se identificarán estudios primarios que aborden las mismas preguntas. El proceso de extracción se usarán los elementos que ayuden a responder estas preguntas y en el proceso de análisis se sintetizarán los datos, de tal forma que puedan responder las preguntas.

- **Desarrollar un protocolo de revisión:** En esta etapa se debe especificar los métodos que serán usados para realizar la revisión. Por ejemplo, este documento contendrá las estrategias para realizar las búsquedas, los criterios para determinar si un documento es válido o no, como serán evaluados los documentos, como se realizará la síntesis y el cronograma del proyecto.

- **Evaluar el protocolo de revisión:** Debido a que el protocolo de revisión es un elemento sumamente importante para todo el proceso, este documento debe ser revisado, y para esto se debe acordar un procedimiento para evaluar el protocolo.

3.2.2 Conducir la revisión

Una vez que el protocolo haya sido definido, se puede dar inicio a la realización de la revisión sistemática de la literatura. Las etapas que tendremos dentro de esta fase serán:

Identificación de la investigación, selección de estudios primarios, evaluación de la calidad del estudio, extracción y monitoreo de datos y finalmente al síntesis de datos.

- ❒ **Identificación de la investigación:** El objetivo de la revisión es encontrar el mayor numero de documentos los cuales respondan las preguntas. Por lo que en este punto de generan estrategias de búsqueda, se especifica de donde se van a extraer los documentos y se documenta todo el proceso.
- ❒ **Selección de estudios primarios:** En el anterior proceso se obtuvieron los estudios primarios potenciales. pues, en esta fase se va a evaluar su relevancia, para lo que se tendrá un criterio y luego será aplicado este criterio sobre los documentos potenciales.
- ❒ **Evaluación de la calidad del estudio:** Una vez que hemos aplicados los criterios en el anterior paso es hora de medir la calidad de estos documentos. para lo cual se pondrán los criterios de calidad y se evaluarán los documentos, para lo cual se puede usar una tabla para documentar el proceso.
- ❒ **Extracción y monitoreo de datos:** En este punto se diseñará un formulario, el cual debe permitir registrar detalladamente la información que nos interesa sobre los estudios primarios.
- ❒ **Síntesis de datos:** Los resultados obtenidos deben ser relacionados con las preguntas formuladas de tal forma que se resalten las similitudes y diferencias entre los resultados del estudio

3.2.3 Reportar la revisión

Esta es la parte final de la revisión donde se darán a conocer los resultados y se distribuirán los resultados a las partes interesadas. Para esto tendremos los siguientes pasos: Especificación de mecanismos de distribución, dar formato al informe principal y evaluar el informe.

- ❒ **Especificación de mecanismos de distribución:** Se debe tener una estrategia para distribuir los resultados para que así este documento sea utilizados por la mayor número de personas posible.
- ❒ **Dar formato al informe principal:** La revisión será formateada o bien como una sección de una tesis o como un paper.

❒ **Evaluar el informe:** Finalmente el documento será revisado, si es una sección de una tesis, pues los expertos lo revisarán. y si es un paper, se deberá buscar expertos para que puedan revisar el documento, antes de que este sea publicado en la web.

3.3 SCRUM

Esta es una metodología ágil de desarrollo de software. Tiene un conjunto de buenas practicas y eventos a seguir que buscan garantizar la calidad de un producto de software. Consta de 5 eventos principales de acuerdo con la guía de Scrum [4], las cuales se mencionan a continuación.

1. **Sprint**

   Un sprint es un periodo de tiempo en el cual se entrega un producto final. El producto final tiene que ser de mayor valor posible. Un sprint no puede comenzar antes que el anterior acabe. En otras palabras cada sprint es considerado un proyecto corto.

2. **Sprint Planning**

   Es una reunión en donde participa todo el equipo para poder determinar lo que se realizara en el Sprint. En general, de acuerdo con la guía de Scrum [4], se plantean 3 preguntas, las cuales se presentan a continuación de acuerdo con Ramos en [10].

   a) ¿Por qué es valioso este Sprint?

   b) ¿Qué se puede hacer en este Sprint?

   c) ¿Cómo se realizará el trabajo elegido?

   "La planificación de Sprint tiene un límite de tiempo de un máximo de ocho horas para un Sprint de un mes. Para Sprints más cortos, el evento suele ser más corto [4]."

3. **Daily Scrum**

   Es una reunión de 15 minutos por parte de los desarrolladores del equipo. En estas reuniones se busca ver el avance diario que ha tenido cada desarrollador. Se plantean las preguntas.

   a) ¿Qué hiciste ayer?

   b) ¿Que harás hoy?

c) ¿Hay impedimentos en tu camino?

4. **Sprint Review**

   El propósito de este evento es analizar lo que se ha logrado en el sprint. En pocas palabras esta reunión ocurre una vez que el sprint ha finalizado.

   "Durante el evento, el Equipo Scrum y las partes interesadas revisan lo que se logró en el Sprint y lo que ha cambiado en su entorno. Con base en esta información, los asistentes colaboran sobre qué hacer a continuación"[4].

5. **Sprint Retrospective**

   Al final del sprint se realiza una reunión, la cual tiene objetivo evaluar el sprint pasado. Discutiendo sobre las cosas que fueron realizadas de forma correcta y las que no, de tal forma que se pueda corregir, mejorar o mantener para el siguiente Sprint.

4 REVISIÓN SISTEMÁTICA DE LA LITERATURA

4.1 PLANTEAMIENTO DE LA NECESIDAD

Como bien sabemos nuestro objetivo no es crear o inventar herramientas que ya han sido propuestas. Por el contrario, queremos mapear todas esas herramientas ya propuestas con su respectiva solución al control de acceso y control de consentimiento. Y, si se da el caso generar un prototipo a partir de las herramientas ya existentes, las cuales nos permitan dar cumplimiento al control de acceso y al control del consentimiento.

Es ahí donde sale la motivación para realizar una revisión sistemática de la literatura. Como primer paso realizamos la búsqueda para determinar si ya existen una revisión sistemática de la literatura. Para lo cual no se tuvieron respuestas positivas por lo que se concluye que es totalmente realizable esta revisión. Para la realización de la revisión se tomó como principales temas el “Control de acceso” y el “Control de consentimiento”, los cuales deben ser cumplidos como manda la Ley Orgánica de Protección de Datos Personales en Ecuador. Controles los cuales deben ser cumplidos por todas las organizaciones dentro del Ecuador desde el 26 de mayo de 2023. A partir de estos temas se seguirá una metodología, la cual nos permita, de forma correcta realizar la investigación y obtener una conclusión.

4.2 MÉTODO

Se realizó el estudio, que se encuentra a partir del punto 4.3, mediante la metodología provista por Kitchenham en el Paper ”A systematic review of systematic review process research in software engineering"[3]. Debido a que importantes revisiones sistemáticas de la literatura han sido realizadas, basándose en la metodología propuesta por Kitchenham [3].

Las preguntas de investigación se las realizaron en base a la guías provistas por Mark

Petticrew and Helen Roberts en Systematic Review in the Social Science [11, pág 32]. En el cual se da pautas para escribir preguntas las cuales sean relevantes para la investigación.

4.3 PREGUNTAS DE INVESTIGACIÓN

Con esta investigación se desea determinar la existencia de técnicas o herramientas para la gestión del consentimiento y acceso de la información personal la cual está descrita en la Ley Orgánica de protección de Datos Personales. Por lo tanto, en una primera instancia se han plantado las siguientes preguntas las cuales nos ayudarán con el objetivo de la investigación:

PI1 ¿Qué soluciones existen para la gestión del consentimiento de la información personal?
PI2 ¿Qué soluciones existen para la gestión del acceso de la información personal?
PI3 ¿Cómo se deben almacenar los datos para cumplir con la portabilidad de los datos?

La portabilidad de los datos será resultado de las soluciones de consentimiento y acceso debido a que esta será la forma en la cual serán almacenados los datos. Por lo cual, la portabilidad será la forma ordenada de como se manejan el consentimiento y el control de acceso para enviar la información al dueño de los datos. Es por eso que nos centraremos únicamente con las primeras dos preguntas, quedando así: PI1, PI2.

4.4 PROCESO DE BÚSQUEDA

Para el proceso de búsqueda se hará uso de las bases de datos descritas a continuación:

- ACM Digital Library
- IEEE Xplore

Estas bases de datos digitales fueron seleccionadas debido a que estas bibliotecas almacenan mucho de los documentos relacionados específicamente a temas de ingeniería y al área de las ciencias de la computación.

Para la realización de la búsqueda en estas bases de datos se desarrolló una frase de búsqueda para poder responder las preguntas de investigación. La frase es:

(“access management” OR “consent management”) AND (“solution*” OR *“technique*”* OR *“tool*”*)

4.5 SELECCIÓN DE ESTUDIO

Para la selección de los artículos que forman parte del estudio, se realizó la aplicación de diferentes criterios de inclusión y exclusión. De tal forma que podamos tener el conjunto mas exacto y reducido posible. Los criterios de inclusión y exclusión fueron los siguientes:

Inclusión:

- ❒ Documentos que contengan en su título la cadena de búsqueda planteada.
- ❒ Documentos que contengan dentro de sus palabras claves “access” ó “consent”.

Exclusión:

- ❒ Documentos que sean anteriores al 2012. Debido que para este estudio se han considerado únicamente los artículos de máximo 10 años de antigüedad.
- ❒ Documentos que estén escritos en un idioma diferente al Inglés.

4.5.1 Fase 1

Utilizamos la cadena obtenida en el proceso de búsqueda en cada una de las bases de datos y utilizamos los criterios de inclusión y de exclusión, tenemos los siguientes resultados:

- ❒ ACM Digital Library: 33
- ❒ IEEE Xplore: 3
- ❒ Total: 36

4.5.2 Fase 2

Se leyó el título, resumen y palabras claves de cada uno de los documentos obtenidos en la fase dos, y se fue descartando todos aquellos que no estaban relacionados con el tema del proyecto, al igual que se eliminó documentos repetidos. Quedándonos así con el siguiente n[umero de artículos para la revisión:

- ACM Digital Library: 10
- IEEE Xplore: 2
- Total: 12

A modo de resumen podemos encontrar la Figura. 4.1 la cual muestra cuantos documentos se obtuvieron después de cada fase.

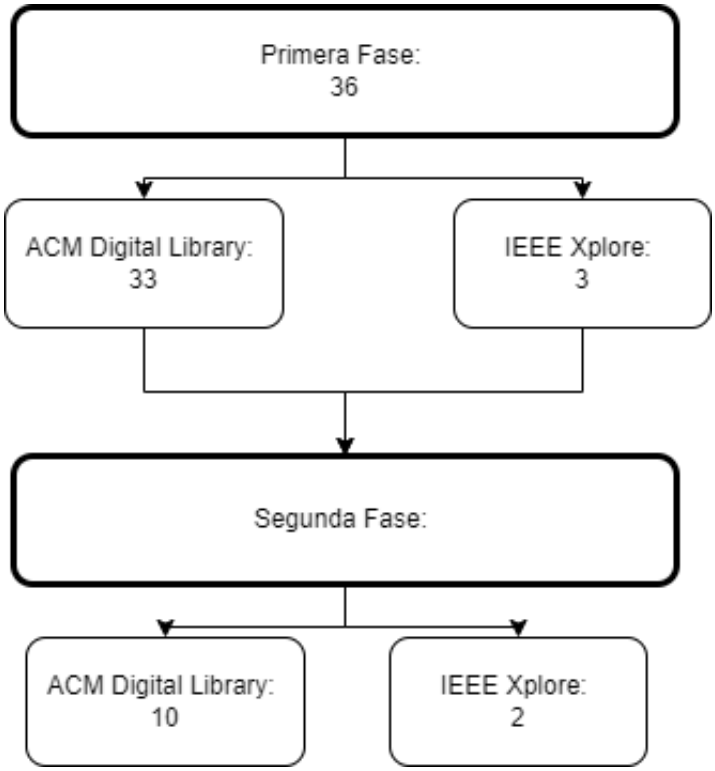

Figura 4.1: Fases del procesos de selección de artículos

4.6 EVALUACIÓN DE CALIDAD

Para la evaluación de calidad se tomará como referencia la revisión sistemática de problemas y soluciones a la seguridad en una E-commerce [12]. Por lo que se seleccionaron

preguntas las cuales pueden ser aplicadas a esta revisión sistemática de la literatura. Las preguntas seleccionadas son las siguientes:

- ❒ P1. ¿El artículo describe los objetivos de investigación claramente?
- ❒ P2. ¿El artículo muestra trabajos relacionados de investigaciones anteriores para mostrar la principal contribución de la investigación?
- ❒ P3. ¿Recomienda el artículo trabajo o mejoras en el futuro?
- ❒ P4. ¿Muestra el artículo conclusiones las cuales son relevantes para el objetivo del mismo?

Los documentos serán clasificados en función de que tan bien cumplan con los criterios de clasificación de calidad descritos en la Tabla 4.1. Por lo tanto, la puntuación de calidad será calculada sumando las puntuaciones de todos los criterios donde 0 será muy malo y 4 será muy bueno.

Tabla 4.1: Criterios de clasificación de calidad

	Si (puntaje 1.0)	Parcial (puntaje 0.5)	No (puntaje 0.0)
P1	Los objetivos de investigación se describen de manera clara y concisa.	Los objetivos de la investigación se detallan parcialmente.	No se definen los objetivos de investigación.
P2	El autor o autores describen trabajos relacionados que aporte a su investigación.	El autor o autores describen trabajos relacionados, pero estos no aportan a su investigación	El autor o los autores no describen trabajos relacionados con su investigación.
P3	Se recomiendan trabajos y mejoras en el futuro.	Se recomiendan implícitamente trabajos y mejoras en el futuro.	No se recomiendan trabajos y mejoras en el futuro.
P4	Se muestran conclusiones las cuales son relevantes para el objetivo del mismo.	Se muestran conclusiones las cuales no son totalmente relevantes para el objetivo del mismo.	No se muestran conclusiones las cuales son relevantes para el objetivo del mismo.

4.7 PROCESO DE EXTRACCIÓN Y ANÁLISIS DE DATOS

La extracción de datos se la realizará, haciendo uso de un formulario de Microsoft Excel el cual nos permitirá tener los documentos organizados de una mejor manera. Los siguientes datos serán extraídos:

- ❒ Información bibliográfica (título, resumen, año de publicación, tipo de publicación)
- ❒ Palabras claves.
- ❒ Soluciones o técnicas para la gestión del acceso a la información personal.
- ❒ Soluciones o técnicas específicas para la gestión del consentimiento de los datos.
- ❒ Puntaje de Calidad.

4.8 RESULTADOS

Como resultado del proceso de extracción se obtuvieron dos tablas. La Tabla 4.2 que corresponde a la Información Bibliográfica y la Tabla 4.3 que corresponde al Puntaje de calidad.

Tabla 4.2: Información Bibliográfica

Código	**Título**	**Año de Publicación**	**Palabras claves**	**Tipo de publicación**
[13]	Privacy of Fitness Applications and Consent anagement in Blockchain	2022	Privacy, Data Protection, Legal Framework, Consent Management, Consent Criteria, Fitness Data, Fitness Provider, Wearable Devices	RESEARCH-ARTICLE
[14]	Privacy Issues and Techniques in E-Health Systems	2015	Cloud computing; security; access controls; patterns; data encryption, cloud data security; cryptography; security monitoring, trusted computing; access control.	RESEARCH-ARTICLE"

Código	Título	Año de Publicación	Palabras claves	Tipo de publicación
[15]	Measuring the Emergence of Consent Management on the Web	2020	GDPR, CCPA, consent, privacy, web measurement	RESEARCH-ARTICLE
[16]	Kubernetes security and access management: a workshop exploring security & access features in Kubernetes	2019	Access Management, Cloud Deployment, Container, Kubernetes	RESEARCH-ARTICLE"
[17]	Iris: allocation banking and identity and access management for the exascale era	2020	allocation banking, identity and access management	RESEARCH-ARTICLE"
[18]	ICME: an informed consent management engine for conformance in smart building environments	2021	IoT, Smart Buildings, Smart office, Informed consent, Privacy Preservation, awareness, Privacy Rights, Privacy policies, Compliance	RESEARCH-ARTICLE"
[19]	DIAM-IoT: A Decentralized Identity and Access Management Framework for Internet of Things	2020	Decentralized Identity, Verifiable Credential, Internet of Things, Identity and Access Management	SHORT-PAPER
[20]	Centralized, Distributed, and Everything in between: Reviewing Access Control Solutions for the IoT	2021	Access control, Internet of Things, IoT, security, survey	RESEARCH-ARTICLE
[21]	Binary hash tree based certificate access management for connected vehicles	2017	Binary tree, certificate, access management, revocation, connected vehicles, SCMS	RESEARCH-ARTICLE
[22]	An analytical solution for consent management in patient privacy preservation	2012	Access control, Privacy Protection, Machine Learning, Data Analytics	RESEARCH-ARTICLE"

Código	Título	Año de Publicación	Palabras claves	Tipo de publicación
[23]	A Survey of Access ManagementTechniques in Machine TypeCommunications	2014	Machine-to-machine communication Access management, Quality of service, Telecommunication traffic, Radio access networks, Synchronization	Magazine Article"
[24]	Drivers and Obstacles for the Adoption of Consent Management Solutions by Ad-Tech Providers	2021	Consent management, CMPs, ad-tech vendors, GDPR, TCF, online advertising, cookies	Conference Paper"

Tabla 4.3: Puntaje de calidad

Código	Título	P1	P2	P3	P4	Calificación
[13]	Privacy of Fitness Applications and Consent anagement in Blockchain	1	1	1	0	3
[14]	Privacy Issues and Techniques in E-Health Systems	1	0,5	0	1	2,5
[15]	Measuring the Emergence of Consent Management on the Web	1	1	0,5	1	3,5
[16]	Kubernetes security and access management: a workshop exploring security & access features in Kubernetes	0,5	0	0	0,5	1
[17]	Iris: allocation banking and identity and access management for the exascale era	1	1	0	1	3
[18]	ICME: an informed consent management engine for conformance in smart building environments	1	0	0	1	2

Código	Título	P1	P2	P3	P4	Calificación
[19]	DIAM-IoT: A Decentralized Identity and Access Management Framework for Internet of Things	1	1	0	1	3
[20]	Centralized, Distributed, and Everything in between: Reviewing Access Control Solutions for the IoT	1	1	1	1	4
[21]	Binary hash tree based certificate access management for connected vehicles	1	1	0.5	0.5	3
[22]	An analytical solution for consent management in patient privacy preservation	1	1	1	1	4
[23]	A Survey of Access ManagementTechniques in Machine TypeCommunications	1	1	0.5	0	2.5
[24]	Drivers and Obstacles for the Adoption of Consent Management Solutions by Ad-Tech Providers	1	1	0.5	0.5	2

4.9 DISCUSIÓN DE LAS PREGUNTAS DE INVESTIGACIÓN

Para responder las preguntas de investigación se realizó la Tabla 4.4 la cual nos muestra las soluciones con respecto al “consent management” y al “access management” de cada documento.

Tabla 4.4: Soluciones propuestas por los documentos

Código	Título	Soluciones para“access"	Soluciones para“consent"
[13]	Privacy of Fitness Applications and Consent anagement in Blockchain	N/A	We propose a blockchainbased consent mechanism, which we suggest can improve privacy by designing a human-centric and legally compliant system that manages user consent dynamically around the sharing, collecting, and processing of fitness data between the requester and user under the GDPR's validity criteria.
[14]	Privacy Issues and Techniques in E-Health Systems	Central authenticating module. The actors to be authenticated, identify themselves to this authority and provide their verification. The central authority acts as the key distribution center for cloud server/e-health server, patients, doctors etc.	N/A
[15]	Measuring the Emergence of Consent Management on the Web	N/A	Transparency and Consent Framework (TCF), “the only GDPR consent solution built by the industry for the industry”
[16]	Kubernetes security and access management: a workshop exploring security & access features in Kubernetes	Kubernetes Role Based Access Control (RBAC)	N/A
[17]	Iris: allocation banking and identity and access management for the exascale era	Iris System: identity and access management	N/A

Código	Título	Soluciones para“access"	Soluciones para“consent"
[18]	ICME: an informed consent management engine for conformance in smart building environments	N/A	privacy policy document database (PDD) (The information in this paper doesn’t not work for our project, it just specify buildings environments)
[19]"	DIAM-IoT: A Decentralized Identity and Access Management Framework for Internet of Things	Decentralized identifiers (DIDs) Blockchain Smart Contracts	N/A"
[20]	Centralized, Distributed, and Everything in between: Reviewing Access Control Solutions for the IoT	Role Based Access Control (RBAC)	N/A
[21]	Binary hash tree based certificate access management for connected vehicles	Binary Hash Tree based Certificate Access Management (BCAM)	N/A
[22]	An analytical solution for consent management in patient privacy preservation	N/A	(The information in this paper doesn’t not work for our project, analitical solution)
[23]	A Survey of Access Management-Techniques in Machine TypeCommunications	N/A	N/A
[24]	Drivers and Obstacles for the Adoption of Consent Management Solutions by Ad-Tech Providers	N/A	CMP, Consent Management Provider

Es importante recalcar que una vez realizado el análisis varios documentos no presentaron soluciones orientadas al tema del proyecto por lo que fueron descartados. Entre estos documentos tenemos a:

- *ICME: an informed consent management engine for conformance in smart building environments* [18].
  Documento el cual nos da soluciones de consentimiento enfocado a casas inteligentes, es decir a dispositivos IoT.
- *Centralized, Distributed, and Everything in between: Reviewing Access Control Solutions for the IoT* [20].
  Documento el cual presenta soluciones de control de acceso específicamente para dispositivos IoT.
- *Binary hash tree based certificate access management for connected vehicles* [21].
  Documento el cual presenta soluciones de control de acceso para sistemas de vehículos de seguridad orientado específicamente a comunicaciones satelitales.
- *An analytical solution for consent management in patient privacy preservation* [22].
  Documento el cual presenta una solución analítica para la gestión del consentimiento.
- *A Survey of Access ManagementTechniques in Machine TypeCommunications* [23].
  Documento el cual presenta soluciones para la gestión de acceso específicamente para comunicaciones de máquina a máquina.
- *DIAM-IoT: A Decentralized Identity and Access Management Framework for Internet of Things*[19] Documento que propone un un marco descentralizado de IAM orientado unicamente a dispositivos IoT.

En las siguientes secciones desglosaremos las soluciones encontradas para cada una de las partes.

4.9.1 PI1 ¿Qué soluciones existen para la gestión del consentimiento de la información personal?

Se encontraron en tres documentos soluciones para la gestión del consentimiento. En el documento *"Privacy of Fitness Applications and Consent management in Blockchain"* [13].

se propone el hacer uso de un mecanismo de consentimiento basado en blockchain. De tal forma que mediante este mecanismo se pueda gestionar el consentimiento de forma dinámica (que los usuarios puedan decidir que información compartir o que se desea procesar y que información no) en un entorno de intercambio, recopilación y procesamiento de los datos según criterios del GDPR.

En el documento *"Measuring the Emergence of Consent Management on the Web"* [15], se informa que ya existen proveedores para la gestión de consentimientos, y que estos son llamados CMPs (Consent managment providers). Estos CMPs utilizan TCFs que son marcos de transparencia y consentimiento, estos marcos estandarizan y centralizan el almacenamiento de cookies de consentimiento 'globales'.

EL documento *"Drivers and Obstacles for the Adoption of Consent Management Solutions by Ad-Tech Providers"*[24], al igual que el documento mencionado anteriormente nos propone lo que son las CMPs y las TCFs. Con la diferencia de que este, se orienta más hacia el lado de como las empresas adoptan estas soluciones y todos los obstáculos que presentan en el camino.

4.9.2 PI2 ¿Qué soluciones existen para la gestión del acceso de la información personal?

Se encontraron en tres documentos soluciones para la gestión del consentimiento. En el documento *"Privacy Issues and Techniques in E-Health Systems"* [14] se propone un módulo de autenticación central. En el cual los actores a ser autenticados, se identifican ante esta autoridad y brindando así su verificación y asegurando su autenticidad. Esta autoridad central actual como centro de distribución de claves de tal forma que siempre se debe acceder a este para acceder a la infracción. Las claves distribuidas son creadas mediante criptosistemas de claves simétricas.

EL documento *"Kubernetes security and access management: a workshop exploring security access features in Kubernetes"*[16], nos hablan sobre Kubernet. Este es un sistema que mediante el uso de contenedores permite automatizar tanto la gestión, implementación

y escalado de una aplicación. Y para el control de acceso de esta aplicación, utilizan herramientas con arquitecturas en la nube.

En el documento *"Iris: allocation banking and identity and access management for the exascale era"* [17].se expone un sistema llamado Iris el cual fue creado específicamente para bancos y se basa en una arquitectura modular la cual le permite escalar y que soporta identificación y autenticación de nivel federal. Entre sus soluciones se pudo encontrar que para la gestión de acceso hacen uso de funciones IAM (manejo de identidad y acceso).

4.10 CONCLUSIONES DE LA REVISIÓN SISTEMÁTICA DE LA LITERATURA

Gracias a la respuestas de las preguntas planteadas se obtuvo como resultado que ya se han propuesto soluciones para la gestión de acceso y la gestión de consentimiento. Con respecto a la gestión de acceso concluimos que una buena solución sería tener una autenticación central que tenga como base las funciones IAM. Mientras que, con respecto a la gestión del consentimiento descubrimos que ya existen los CMPs que utilizan TCFs, que son proveedores de gestión de consentimientos que usan marcos de transparencia y consentimiento, los cuales almacenan todos los consentimientos de una forma centralizada y las demás empresas acceden a ella para saber que datos pueden guardar del usuario y como pueden utilizarlos. Los documentos utilizados para la extracción de datos tuvieron una buena calificación, por lo que podemos asegurar su calidad.

5 IDENTIFICACIÓN DE CONTROLES DE LOS ESTÁNDARES INTERNACIONALES

Con respecto a controles internacionales sobre la seguridad informática existen dos principales. La NIST 800-53 que es el acrónico para Instituto Nacional de Estándares y Tecnología y la ISO 27001 que se refiere a un estándar para la seguridad de la información aprobado Organización Internacional de Estandarización. A continuación, se mostrarán los estándares asociados a la gestión del consentimiento y gestión de acceso.

5.1 GESTIÓN DEL CONSENTIMIENTO - CONTROLES ISO 27001

En la Tabla 5.1 se podrá encontrar controles de la ISO 27001 asociados a la gestión del consentimiento. La tabla está dividida en 3 secciones. El código hace referencia al grupo y subgrupo del control, el control que es el nombre del mismo, y finalmente la descripción la cual contienen una pequeña descripción sobre el mismo.

Tabla 5.1: Controles ISO relacionados a la gestión del consentimiento. Información extraída de *ISO 27001 - software ISO 27001 de Sistemas de Gestión* [5]

Código	Control	Descripción
A.9.4.1	Restricción de acceso a la información	El acceso a la información ya las funciones del sistema de aplicación se restringirán de acuerdo con la política de control de acceso.
A.11.2.7	Eliminación segura o reutilización de equipos	Todos los elementos del equipo que contengan medios de almacenamiento se verificarán para garantizar que todos los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.

Código	Control	Descripción
A.13.2.4	Acuerdos de confidencialidad o no divulgación	Los requisitos para los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la organización para la protección de la información deben identificarse, revisarse periódicamente y documentarse.
A.18.1.4	Privacidad y protección de la información de identificación personal.	La privacidad y la protección de la información de identificación personal se garantizarán según lo exija la legislación y los reglamentos pertinentes, según corresponda.
A.18.2.1	Revisión independiente de la seguridad de la información.	El enfoque de la organización para gestionar la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) debe revisarse de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.
A.18.2.2	Cumplimiento de políticas y estándares de seguridad	Los responsables revisarán periódicamente la conformidad de los procesos y procedimientos de información dentro de su área de responsabilidad con las políticas, estándares y cualquier otra seguridad adecuada.
A.18.2.3	Revisión Cumplimiento técnico	Sistemas de información deben revisarse periódicamente para verificar que cumplan con las políticas de seguridad de la información de la organización

5.2 GESTIÓN DEL ACCESO - CONTROLES ISO 27001

En la Tabla 5.2 se podrá encontrar controles de la ISO 27001 asociados a la gestión del acceso. La tabla está dividida en 3 secciones. El código hace referencia al grupo y subgrupo del control, el control que es el nombre del mismo, y finalmente la descripción la cual contienen una pequeña descripción sobre el mismo.

Tabla 5.2: Controles ISO relacionados a la gestión del Acceso. Información extraída de *ISO 27001 - software ISO 27001 de Sistemas de Gestión* [5]

Código	Control	Descripción
A.9.1.1	Política de control de acceso	Se establecerá, documentará y revisará una política de control de acceso en función de los requisitos de seguridad empresarial y de la información.

Código	Control	Descripción
A.9.2.1	Alta y baja de usuario	Se implementará un proceso formal de registro y registro de usuarios para permitir la asignación de derechos de acceso.
A.9.2.5	Revisión de los derechos de acceso de los usuarios	Los propietarios de activos revisarán los derechos de acceso de los usuarios a intervalos regulares.
A.9.4.1	Restricción de acceso a la información	El acceso a la información ya las funciones del sistema de aplicación se restringirán de acuerdo con la política de control de acceso.
A.11.2.2	Utilidades de apoyo	El equipo debe estar protegido contra cortes de energía y otras interrupciones causadas por fallas en los servicios de apoyo.
A.11.2.3	Seguridad del cableado	El cableado de energía y telecomunicaciones que transporta datos o apoya servicios de información debe estar protegido contra intercepciones, interferencias o daños.
A.12.4.2	Protección de la información de registro	Las instalaciones de registro y la información de registro deben estar protegidas contra la manipulación y el acceso no autorizado.
A.13.2.1	Políticas y procedimientos de transferencia de información	Deben existir políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
A.14.1.3	Protección de transacciones de servicios de aplicaciones	La información involucrada en las transacciones de servicios de aplicaciones debe protegerse para evitar transmisiones incompletas, enrutamiento incorrecto, alteración de mensajes no autorizados, divulgación no autorizada, duplicación o reproducción de mensajes no autorizados.
A.15.1.1	Política de seguridad de la información en las relaciones con proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de los proveedores a los activos de la organización deben acordarse con el proveedor y documentarse.
A.15.1.2	Abordar la seguridad en los acuerdos con los proveedores	Todos los requisitos de seguridad de la información pertinentes deben establecerse y acordarse con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización.

Código	Control	Descripción
A.18.2.2	Cumplimiento de políticas y estándares de seguridad	Los responsables revisarán periódicamente la conformidad de los procesos y procedimientos de información dentro de su área de responsabilidad con las políticas, estándares y cualquier otra seguridad adecuada.

5.3 GESTIÓN DEL CONSENTIMIENTO - CONTROLES NIST 800-53

En la Tabla 5.3 se podrá encontrar controles de la NIST 800-53 asociados a la gestión del consentimiento. La tabla está dividida en 4 secciones. El código que únicamente es un identificador para el documento, el control que es el nombre del mismo, el literal el cual se relaciona con el control del consentimiento y finalmente la descripción la cual contienen una pequeña descripción sobre el mismo.

Tabla 5.3: Controles NIST relacionados a la gestión del consentimiento. Información extraída de Computer Security Division [6]

Código	Control	Literal	Descripción
PT-2	Autoridad para procesar información personal identificable	b	Restringir el tratamiento definido por la organización de la información personal identificable a la información autorizada.
PT-3	Fines de tratamiento de información personal identificable	d	Supervisar los cambios en el tratamiento de la información de identificación personal y aplicar mecanismos definidos por la organización para garantizar que los cambios se realicen de acuerdo requisitos definidos por la organización.
PT-4	Consentimiento		Implementar herramientas o mecanismos definidos por la organización para que los individuos consentimiento para el tratamiento de su información de identificación personal antes de su recopilación que faciliten la toma de decisiones informadas de los individuos.

Código	Control	Literal	Descripción
PT-5	Aviso de privacidad	b,c,d,e	❒ Ser claro y fácil de entender, expresando la información sobre el tratamiento de la información de identificación personal en un lenguaje sencillo; ❒ Identificar la autoridad que autoriza el tratamiento de la información personal identificable. ❒ Identificar la autoridad que autoriza el tratamiento de la información personal identificable; ❒ Incluir información definida por la organización.

5.4 GESTIÓN DEL ACCESO - CONTROLES NIST 800-53

En la Tabla 5.3 se podrá encontrar controles de la NIST 800-53 asociados a la gestión del acceso. La tabla está dividida en 4 secciones. El código que únicamente es un identificador para el documento, el control que es el nombre del mismo, el literal el cual se relaciona con el control del consentimiento y finalmente la descripción la cual contienen una pequeña descripción sobre el mismo.

Tabla 5.4: Controles NIST relacionados a la gestión del acceso. Información extraída de Computer Security Division [6]

Código	Control	Literal	Descripción
AC-1	Política y procedimientos	a	Desarrollar, documentar y diseminar al personal o roles definidos por la organización: 1. Política de control de acceso que: (a) aborda el propósito, el alcance, las funciones, las responsabilidades, el compromiso de la dirección, la coordinación entre las entidades organizativas y el cumplimiento; y (b) es coherente con las leyes, órdenes ejecutivas, directivas, reglamentos, políticas, normas y directrices aplicables; 2. Procedimientos para facilitar la implementación de la política de control de acceso y los controles de acceso asociados;
AC-1	Política y procedimientos	c	Revise y actualice el control de acceso actual: 1. Política 2. Procedimientos
AC-2	Administración de cuentas	a	Definir y documentar los tipos de cuentas permitidas y específicamente prohibidas para su uso dentro del sistema
AC-2	Administración de cuentas	d	Especificar: 1. Usuarios autorizados del sistema; 2. Membresía de grupo y rol; y 3. Autorizaciones de acceso (es decir, privilegios) y atributos definidos por la organización (según se requiera) para cada cuenta;
AC-2	Administración de cuentas	i	Autorizar el acceso al sistema en base a: 1. Una autorización de acceso válida; 2. Uso previsto del sistema; y 3. atributos definidos por la organización (según se requiera);
AC-3	Cumplimiento de acceso		Hacer cumplir las autorizaciones aprobadas para el acceso lógico a la información y los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.

6 DISEÑO Y DESARROLLO DE LA APLICACIÓN

Como se había propuesto en la Sección 3, Metodología para el diseño y el desarrollo, se usó de la metodología SCRUM. Debido a que en el equipo solo estuvimos presentes tres personas, los papeles de Srum Master y Desarrolladores fueron compartidos por ambos integrantes y nuestra tutora tomo el papel de Product Owner, quedando los papeles de la siguiente manera:

- ❒ Product Owner: Gabriela Suntaxi
- ❒ Scrum Master: Boris Caiza y Milan Contreras
- ❒ Desarrolladores: Boris Caiza y Milan Contreras

Para el desarrollo del proyecto se estimó un tiempo de desarrollo de tres sprints, de tres semanas cada uno. Esta sección junto con la siguiente sección, fué realizada en conjunto con el compañero del trabajo de integración curricular. Dado que sus requerimientos y los míos fueron tomados en conjunto para crear una aplicación funcional tomando en cuenta tanto el lado del usuario (titular de los datos) como de las empresas (responsable del tratamiento).

6.1 ANÁLISIS DE REQUERIMIENTOS Y DISEÑO

Para el diseño de hizo uso de una herramienta del SCRUM que es el product backlog el cual es el listado de todas las tareas que deberán ser realizadas a lo largo del desarrollo del proyecto. A continuación se mostrará la lista del product backlog que fue dividida en dos grandes grupos, el frontend que se refiere a todas las funcionalidades visibles y el backend que se refiere a toda la lógica que funciona en el servidor:

- ❒ Frontend

- ✧ La pantalla de inicio para Titular lista todas las empresas que están haciendo uso de sus datos personales, así como la fecha en la cual se terminar el tratamientos de los datos.
- ✧ La pantalla de inicio para Titular debe permitir ver todos los datos así como los tratamientos que están siendo usados por un responsable de tratamientos.
- ✧ La pantalla de inicio para Titular debe permitir exportar los datos así como los tratamientos que están siendo usados por un responsable de tratamientos en los formatos Csv y Excel.
- ✧ Pantalla de inicio para Titular.
- ✧ La pantalla de inicio para Responsable de tratamientos debe permitir filtrar los usuarios a los cuales se les realiza el tratamiento, el filtrado podrá ser por nombre o tratamiento.
- ✧ La pantalla de inicio para Responsable de tratamientos debe permitir observar los datos y tratamientos que se pueden usar para un usuario en específico.
- ✧ La pantalla de inicio para Responsable de tratamientos debe permitir exportar los datos y tratamientos de los datos filtrados.
- ✧ La pantalla de inicio para Responsable de tratamientos debe permitir ver un historial del consentimiento y cambios en los datos personales de los Titulares
- ✧ La pantalla de solicitud de tratamiento para el Titular debe permitir ver todas las solicitudes enviadas por los Responsables del tratamiento.
- ✧ La pantalla de solicitud de tratamiento para el Titular debe permitir ver el detalle de una solicitud.
- ✧ La pantalla de solicitud de tratamiento para el Titular debe permitir rechazar individualmente los tratamientos de una solicitud y llenar los datos necesarios en caso de la aceptación de una solicitud. A continuación, se muestra la lista mencionada, en este caso se decidió dividir en dos grupos grandes los cuales son el Frontend que corresponde a todas las funcionalidades visuales y el backend que se refiere a la lógica que se ejecuta dentro del servidor.
- ✧ La pantalla de solicitud de tratamiento para el Titular debe permitir rechazar individualmente los tratamientos de una solicitud y llenar los datos necesarios en caso de la aceptación de una solicitud.
- ✧ Pantalla de inicio para Responsable de tratamientos.
- ✧ La pantalla de solicitud de tratamiento para el Titular debe permitir crear trata-

mientos con los respectivos datos que son necesarios para el mismo.

- ✧ La pantalla de solicitud de tratamiento para el Titular debe permitir crear solicitudes de tratamientos, haciendo uso de los tratamientos ya creados.
- ✧ El historial de los datos debe ser almacenado en una blockchain.

❒ Backend

❒ Endpoint para que una empresa se registre.

❒ Endpoint para obtener una empresa por su identificador único.

❒ Endpoint para actualizar una empresa.

❒ Endpoint para enviar un email a un usuario.

❒ Endpoint para que se pueda obtener una lista de todos los usuarios de los cuales una empresa tiene su consentimiento.

❒ Endpoint para que una empresa pueda logearse en nuestro sistema.

❒ Endpoint para obtener un consentimiento por su identificador único.

❒ Endpoint para crear un tratamiento.

❒ Endpoint para obtener todos tratamiento que ha creado una empresa.

❒ Endpoint para obtener un solo tratamiento por su identificador único.

❒ Endpoint para obtener los emails no respondidos que una empresa ha enviado.

❒ Endpoint para que una empresa pueda exportar todos los datos y consentimiento de sus usuarios.

❒ Endpoint para que una empresa pueda exportar todos los datos y consentimiento de un solo usuario.

❒ Endpoint para que un usuario se registre.

❒ Endpoint para obtener un usuario por su identificador único.

❒ Endpoint para que un usuario se pueda logear en nuestro sistema.

❒ Endpoint para que un usuario pueda modificar su información básica.

- ❒ Endpoint para que un usuario pueda obtener todos los emails de las empresas que le han enviado un email.
- ❒ Endpoint para que un usuario pueda obtener un email especifico por su identificador único.
- ❒ Endpoint para que un usuario pueda aceptar el consentimiento de una determinada empresa.
- ❒ Endpoint para obtener que el usuario pueda obtener todos los consentimientos de todas las empresas que el ha aceptado.
- ❒ Endpoint para obtener que el usuario pueda editar el consentimiento de los que ya ha aceptado con anterioridad.
- ❒ Endpoint para que el usuario pueda eliminar el consentimiento de los que ya ha aceptado con anterioridad.
- ❒ Endpoint para que el usuario pueda modificar la fecha de finalización de consentimiento.
- ❒ Endpoint para que el usuario puede comprobar que la empresa esta usando sus datos tal cual lo declaro al aceptar el consentimiento.

Para asegurar la inmutabilidad de los datos se decidió que en lugar de que cada uno de los usuarios tenga su propia cadena de blockchain, exista una sola cadena principal la cual contenga la información de todos los responsables del tratamiento y de los titulares de los datos.
Los responsables del tratamiento buscan cumplir las leyes de la LOPDP, por lo que, si nos centramos en las leyes respecto a la gestión de acceso y gestión del consentimiento existen varios escenarios que deben ser cumplidos:

- ❒ Tratar los datos únicamente de la forma que el usuario a dado su consentimiento.
- ❒ Actualizar los datos siempre que el titular lo requiera.

Por lo tanto, hay varios escenarios en los cuales se debe generar un nuevo bloque en la cadena del blockchain. Y estos son:

- ❒ Se crea una nueva solicitud de tratamiento.
- ❒ El titular actualiza uno de los datos que está siendo usado por los responsables del tratamiento.
- ❒ El titular rechaza un tratamiento por parte de un responsables de los tratamientos.

Cada bloque está atado a otro por medio de un hash el cual es creado a partir de toda la información del documento y existirá otro hash el cual atará el bloque a un usuario en especifico y una empresa. Dado que estos dos hash están conectados, el mínimo cambio en algún elemento del documento hará que los hashes de los bloques no concuerden por lo que se podrá detectar si hubo alguna manipulación de los datos. A continuación, se mostrarán los documentos de las bases de datos con sus respectivas explicaciones, de tal forma que se pueda apreciar de mejor manera como es el funcionamiento de las mismas.

EL documento de la Figura 6.1 muestra dos datos principales del titular, es decir los datos necesarios para su registro. Los cuales son: email, Nombre, Apellido, Cédula y Contraseña. En Figura 6.2, se presentan los datos necesarios para el registro del responsable de tratamientos.

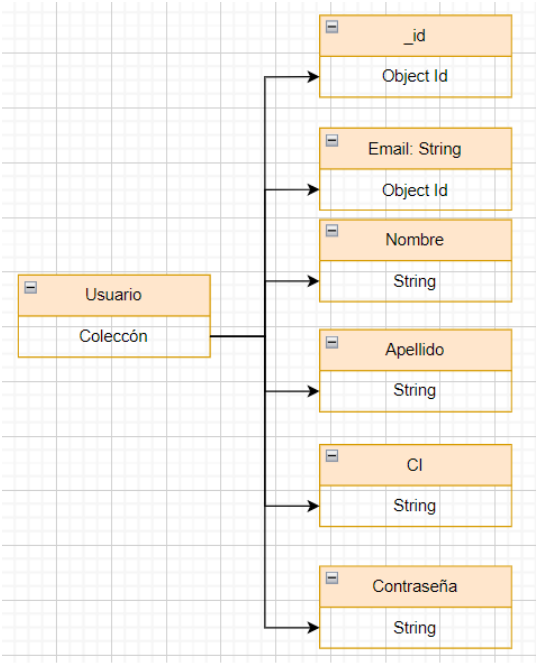

Figura 6.1: Diagrama de la base de datos no relacional del documento del Titular. Elaborada por el autor

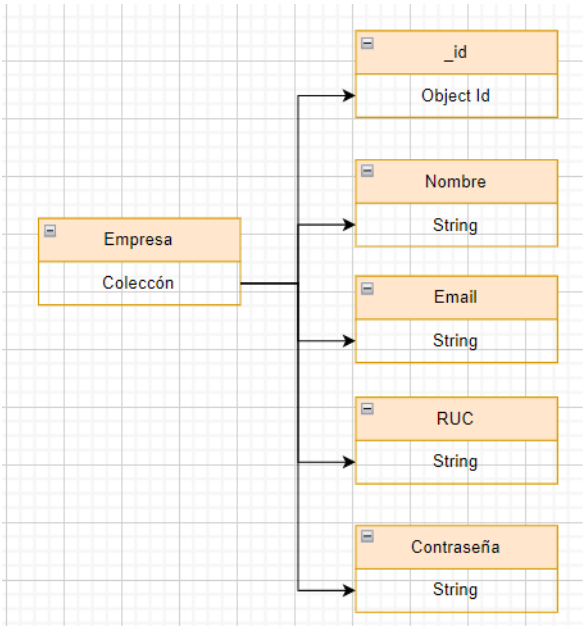

Figura 6.2: Diagrama de la base de datos no relacional del documento del Responsable del Tratamiento. Elaborado por el autor

En la Figura 6.3 tenemos el tratamiento el cual es generado por la empresa, y el el mismo que será enviado dentro de la solicitud de tratamientos. Este documento contendrá un Nombre, los datos que se necesitarán por parte del titular, y una descripción.

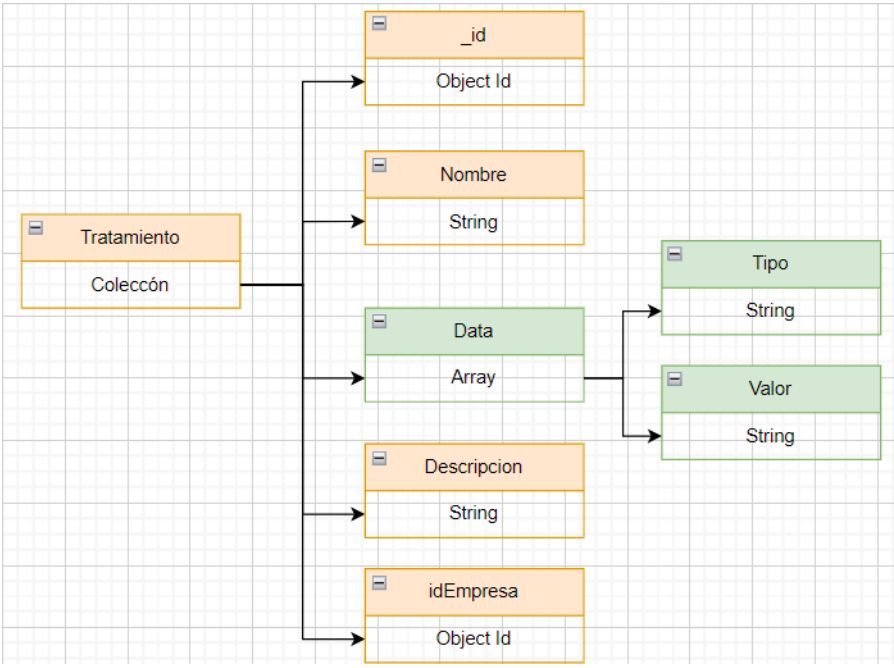

Figura 6.3: Diagrama de la base de datos no relacional del documento del Responsable del Tratamiento. Elaborado por el autor

En la Figura 6.4 tenemos la solicitud del consentimiento, el cual contendrá la información

del destinatario, en este caso el titular, el remitente que es el Responsable del tratamiento, los tratamientos y la fecha fin del tratamiento.

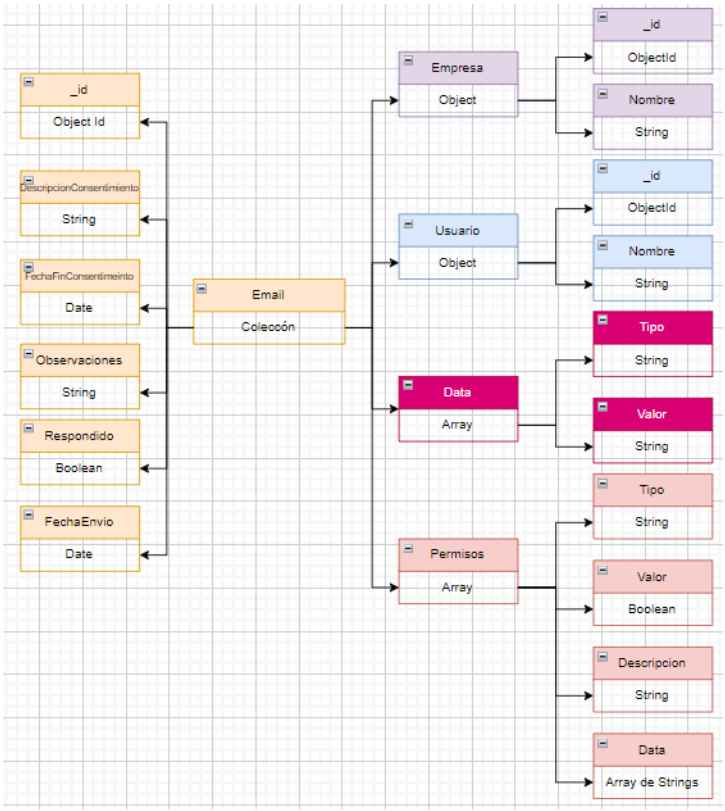

Figura 6.4: Diagrama de la de la base de datos no relacional del documento de la Solicitud del Consentimiento. Elaborado por el autor

En la Figura 6.5 tenemos el consentimiento que es el documento que se generaría a partir de la solicitud del consentimiento. Este contendrá los datos del titular y del responsable de los tratamientos. Así como los tratamientos aceptados por el titular y la fecha de finalización de los tratamientos y los datos que serán usados en los tratamientos.

Finalmente, se presenta la Figura en 6.6 todos los datos presentes en el consentimiento, y se añadirán los hashes, uno referente a todos lo bloques y uno específico asociado a cada empresa y de la misma forma dos alturas una asociada a todos los bloques y otra asociada a la empresa. De tal forma que todos los bloque estén conectados y de igual forma poder crear una conexión entre el titular y el responsable de los tratamientos para poder visualizar un historial.

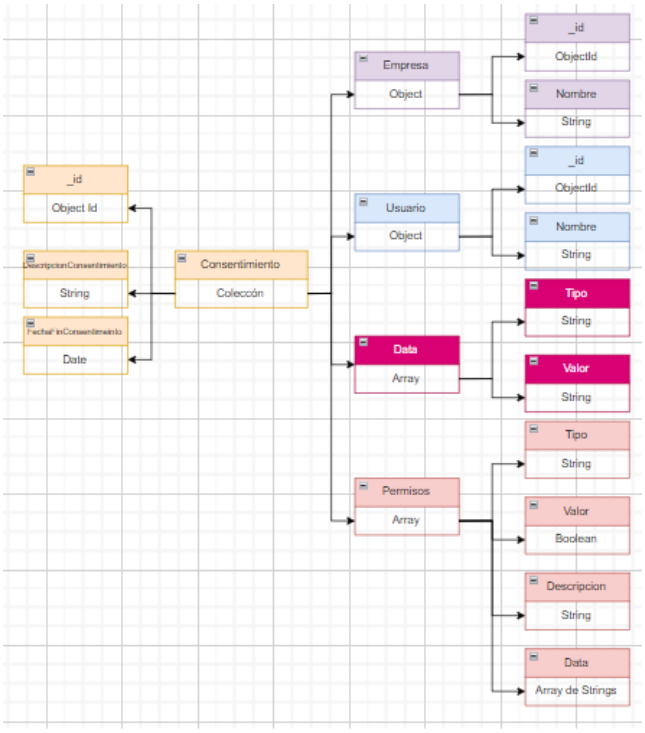

Figura 6.5: Diagrama de la de la base de datos no relacional del documento del Consentimiento. Elaborado por el autor

6.2 DESARROLLO

Para el desarrollo se identificó que se requiere de tres elementos principales, el frontend, el backend y la base de datos. Para el frontend se decidió hacer uno de React debido a que es una herramienta para la creación de interfaces de usuario de código abierto. Para el backend se hizo uso de Nodejs el cual es un entorno de servidor de código abierto, es decir es donde se desarrollará la lógica del programa fuera de los navegadores de los usuarios. Finalmente, para las bases de datos decidimos hacer uso de la base de datos MongoDB que es una base de datos no relacional.

Tanto el frontend como el backend pudieron ser desarrollados con el uso de cualquier tipo de otra tecnología o lenguaje de programación, React, Nodejs, MongoDB y Javascript fueron elegidas estas debido al conocimiento de los desarrolladores. En el caso de la base de datos no relacional si fue necesario hacerlo con este tipo de base de datos debido a que la seguridad de nuestra aplicación se basa en el blockchain y tomando en cuenta que el blockchain es un documento de información teníamos que usar una base la cual nos permita guardar los datos a manera de documentos.

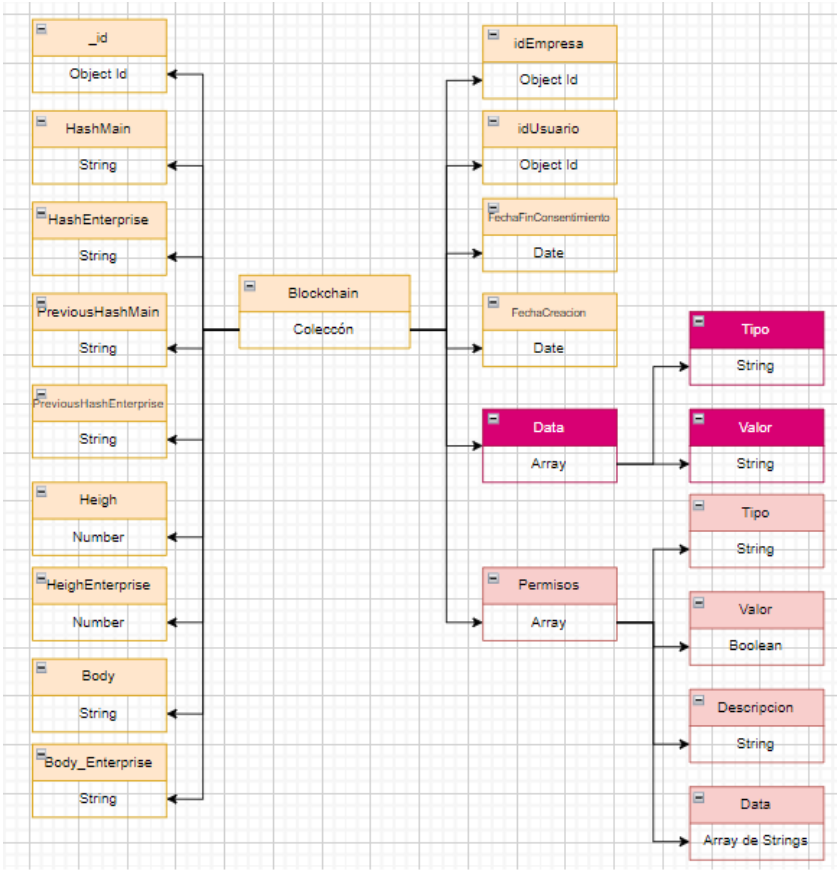

Figura 6.6: Diagrama de la de la base de datos no relacional del Blockchain. Elaborado por el autor

En la fase de diseño se realizó un listado de las tareas que se deben realizar para cumplir con la LOPDP. Para poder entender un poco mas de como funciona la aplicación en este apartado de desarrollo se explicará el porque de las funcionalidades que fueron desarrolladas o de las herramientas que fueron usadas.

Como primer punto el objetivo de este proyecto es desarrollar una aplicación la cual nos permita cumplir con la portabilidad, el consentimiento y la gestión de acceso por parte del usuario. Es importante mencionar que debido a la interacción de dos usuarios, (titular y responsable del tratamiento de los datos) y otros requerimientos (control de consentimiento de los dato y gestión de acceso por parte de la empresa responsable del tratamiento de los mismos), la aplicación tiene mas funcionalidades las cuales complementan el funcionamiento de toda la aplicación.

La base de la aplicación para cumplir los requerimientos de consentimiento y gestión de acceso es el blockchain. De esta forma los consentimientos de los usuarios estarán almacenados de tal forma que siempre se podrá ver el historial de los datos y que el usuario

pueda tener un control sobre los mismos. De tal forma que se pueda observar qué empresas están haciendo uso de sus datos, que datos tienen las empresas y poder tener la decisión en cualquier momento de actualizar sus datos o decidir si querer que un empresa siga tratando mis datos.

Si bien se sabe que una de las bases de los blockchain es que su arquitectura se basa en ser descentralizada, para desarrollo de este proyecto se planteó que se use las bases del blockchain pero con una arquitectura centralizada. Tomando en cuenta las conclusiones tomadas de la revisión sistemática de la literatura nos orientamos a solución donde tendríamos una autenticación centralizada así como se habla en *"Privacy Issues and Techniques in E-Health Systems"* [14] para controlar la gestión de acceso por parte del usuario, y usaremos el blockchain mencionado en *"Privacy of Fitness Applications and Consent management in Blockchain"* [13] para la gestión del consentimiento.

Por lo tanto, se desarrolló una aplicación la cual haga uso de la autenticación para poder acceder a la información de los datos, tanto del lado del usuario para ver que datos están siendo usados por la empresa, y por el lado de las empresas para ver los datos del usuario que pueden usarlos. El uso del blockchain nos ayudó a la parte del consentimiento de tal forma que existe un documento el cual muestra el historial de los datos del titular y el consentimiento para hacer uso de los mismos. Finalmente, para cumplir con el requisito de la portabilidad se agregó un módulo de exportación el cual exportará los datos en un formato entendible y es por eso que hemos elegido poder exportar un archivo como excel que es el documento mas fácil de entender por una persona sin conocimientos en lenguajes de programación, pero de igual forma se hizo que se pueda exportar como JSON ya que actualmente ese es el documento global para todos los programadores y gestores de la información.

7 RESULTADOS: APLICACIÓN WEB

Como resultado de la investigación y desarrollo realizado, se obtuvo una aplicación funcional la cual internamente hace uso de la lógica del blockchain para mostrar al titular los datos el consentimiento que están haciendo uso los responsables del tratamiento, y al responsable del tratamiento de igual forma se le presentan los datos y consentimientos de los titulares de una forma amigable.
En esta sección se encontrarán los flujos de la aplicación los cuales mostrarán su funcionamiento. al igual que se encontrará el funcionamiento del blockchain el cual mediante un ejemplo se mostrará su flujo. De igual forma el código del prototipo funcional tanto del FrontEnd como del BackEnd pueden ser encontrados en el Anexo 2 y Anexo 3 respectivamente, que llevará a un repositorio de Github con el código de la aplicación.

7.1 FLUJOS

El funcionamiento de la aplicación puede ser dividido en ocho flujos:

1. Registro de un titular o responsable de tratamientos.
2. Inicio de sesión de un titular o responsable de tratamientos.
3. Creación de solicitud de tratamiento por parte del responsable de tratamientos.
4. Aceptación o rechazo y llenado de información para una nueva solicitud de tratamiento.
5. Rechazo de tratamiento por parte del titular.
6. Exportación de datos por parte del responsable de tratamientos.
7. Exportación de datos por parte del titular de los datos.

8. Comprobar inmutabilidad en el historial de los datos y de los tratamientos.

Estos flujos ayudarán a entender el funcionamiento de la aplicación de una manera mas gráfica. A continuación de explicarán a detalle el funcionamiento de cada flujo. Como adicional se presenta en el Anexo 1 un video de cada uno de los flujos.

7.1.1 Registro de un titular o responsable de tratamiento

Para que el titular o el responsable del tratamiento pueda ingresar al sistema por primera vez, debe registrarse. Para lo cual deberá llenar los datos principales los cuales se mostrarán en el flujo presentado a continuación, acompañado de una vista mas gráfica en la Figura 7.1.

1. Llenar formulario de registro.
    - ❒ El titular deberá llenar los siguientes datos:
        - ✧ Nombre.
        - ✧ Apellido.
        - ✧ Cédula.
        - ✧ Mail.
        - ✧ Contraseña.
    - ❒ El responsable del tratamiento deberá llenar los siguientes datos:
        - ✧ Nombre.
        - ✧ Mail.
        - ✧ Ruc.
        - ✧ Contraseña.
2. El responsable del tratamiento o el titular, envía los datos del formulario.
3. La lógica del backend crea un bloque con la información

Nota: El orden de registro no es importante, es decir puede bien o registrarse un titular o un responsable del tratamiento. Lo que si es necesario es que antes de realizar una solicitud de tratamiento el titular ya esté registrado.

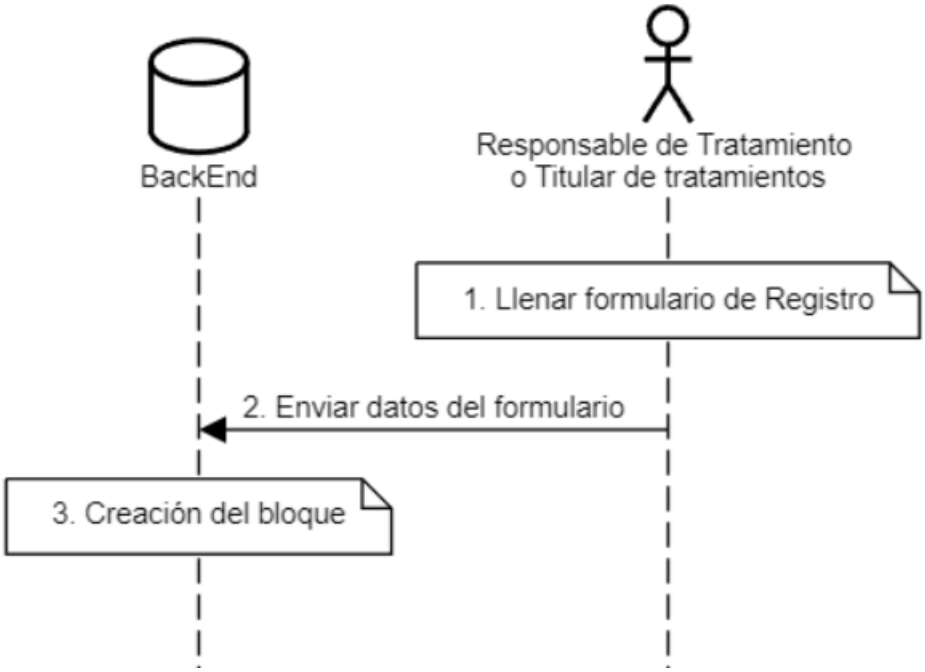

Figura 7.1: Diagrama de flujo de registro. Elaborado por el autor.

7.1.2 Inicio de sesión de un titular o responsable de tratamientos

Como requisito para este flujo, se necesita que el titular o el responsable del tratamiento ya esté registrado. Para iniciar sesión necesitará de su correo y contraseña, que serán llenados por medio de un formulario, como se muestra en el flujo a continuación, acompañado de una vista mas gráfica en la Figura 7.2.

1. Llenar formulario de inicio de sesión.
    - ❒ El titular deberá llenar los siguientes datos:
        - ✧ Mail.
        - ✧ Contraseña.
    - ❒ El responsable del tratamiento deberá llenar los siguientes datos:
        - ✧ Mail.
        - ✧ Contraseña.
2. El responsable del tratamiento o el titular envía los datos del formulario.

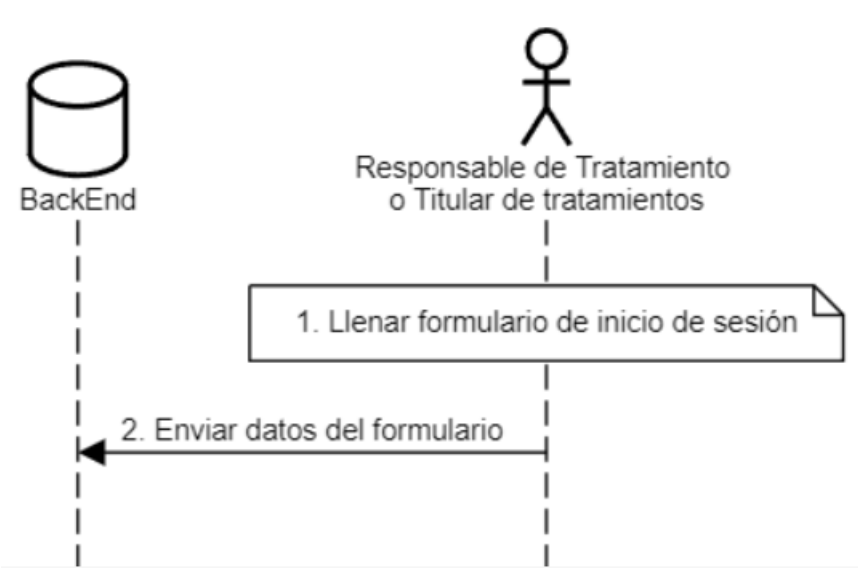

Figura 7.2: Diagrama de inicio de sesión. Elaborado por el autor.

7.1.3 Creación de solicitud de tratamiento por parte del responsable de tratamientos

En este paso el responsable del tratamiento crea una solicitud, la cual contienen los tratamientos que se darán a los datos del Titular. A continuación, se puede observar el flujo, acompañado de una vista mas gráfica en la Figura 7.3.

1. El responsable del tratamiento crea un tratamiento el cual contendrá:
    - ❒ Nombre, que se refiere al título del tratamiento
    - ❒ Descripción, la cual es un explicación de cómo serán usados los datos del titular en ese tratamiento en específico.
    - ❒ Datos, que será una lista de los datos que se requerirán para realizar el tratamiento.
2. El responsable del tratamiento envía el tratamiento al backend.
3. El backend almacena el tratamiento es almacenado en la base de datos.
4. El backend envía todos los tratamientos generados por el responsable del tratamiento.
5. El responsable del tratamiento crea una solicitud de tratamiento la cual contendrá:
    - ❒ Correo del titular
    - ❒ Asunto, una descripción que el titular podrá ver previo a ver toda la solicitud.

- ❒ Descripción, descripción general sobre la solicitud.
- ❒ Fecha fin, fecha en la cual se dará por terminado el tratamiento de los datos.
- ❒ Tratamientos, lista de tratamientos creados en el paso anterior, que se quiere para el titular.

6. EL responsable del tratamiento envía la solicitud
7. La solicitud es guardada en la base de datos

Notas:

- ❒ La fecha fin podrá ser cambiada por el titular al momento de revisar la solicitud.
- ❒ Será decisión del usuario escoger con que tratamientos desea acepta.

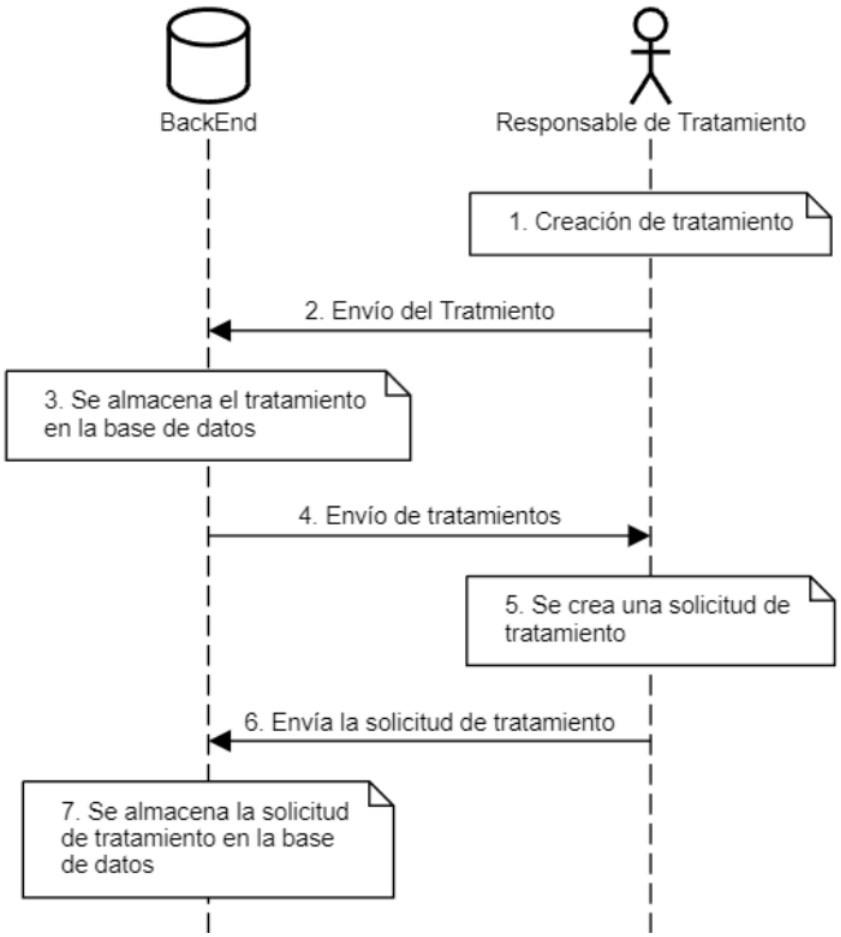

Figura 7.3: Diagrama de creación de solicitud de tratamiento. Elaborado por el autor.

7.1.4 Aceptación o rechazo y llenado de información para una nueva solicitud de tratamiento

El titular recibirá la solicitud de tratamientos, y será el quien acepte o rechace los tratamientos según su criterio, de igual forma será el quien pueda modificar la fecha fin para el tratamiento de sus datos. A continuación, se muestra el flujo del proceso, acompañado de acompañado de una vista mas gráfica en la Figura 7.4.

1. El titular consulta las solicitudes de tratamientos.
2. El backend busca en la base de datos las solicitudes de tratamientos correspondientes.
3. El backend retorna las solicitudes de tratamientos.
4. El titular selecciona una solicitud
5. El titular consulta toda la información de la solicitud.
6. El backend busca la información de la solicitud de tratamiento seleccionada.
7. El backend retorna la información de la solicitud de tratamiento.
8. De forma opcional el titular cambia la fecha fin que fue elegida por el responsable de tratamiento.
9. El titular rechaza los tratamientos en caso de desearlo.
10. Dependiendo de los tratamientos que se desee que se de tratamiento, el titular deberá llenar los datos que son necesarios. Por ejemplo nombre, apellido, celular, etc.
11. El titular envía la respuesta de la solicitud de tratamiento.
12. El backend crea un bloque con el consentimiento y los datos seleccionados por el titular y los datos de la empresa.
13. En caso de que los datos ingresados por el titular cambien es decir se actualicen y sean utilizados por otros responsables de tratamiento se crea un nuevo bloque por cada responsable de tratamiento que use ese dato en específico.

7.1.5 Rechazo de tratamiento por parte del titular

El titular de los datos tiene el poder de terminar con el tratamiento de sus datos por parte del responsable del tratamiento, en cualquier momento, o de igual forma tiene el poder de

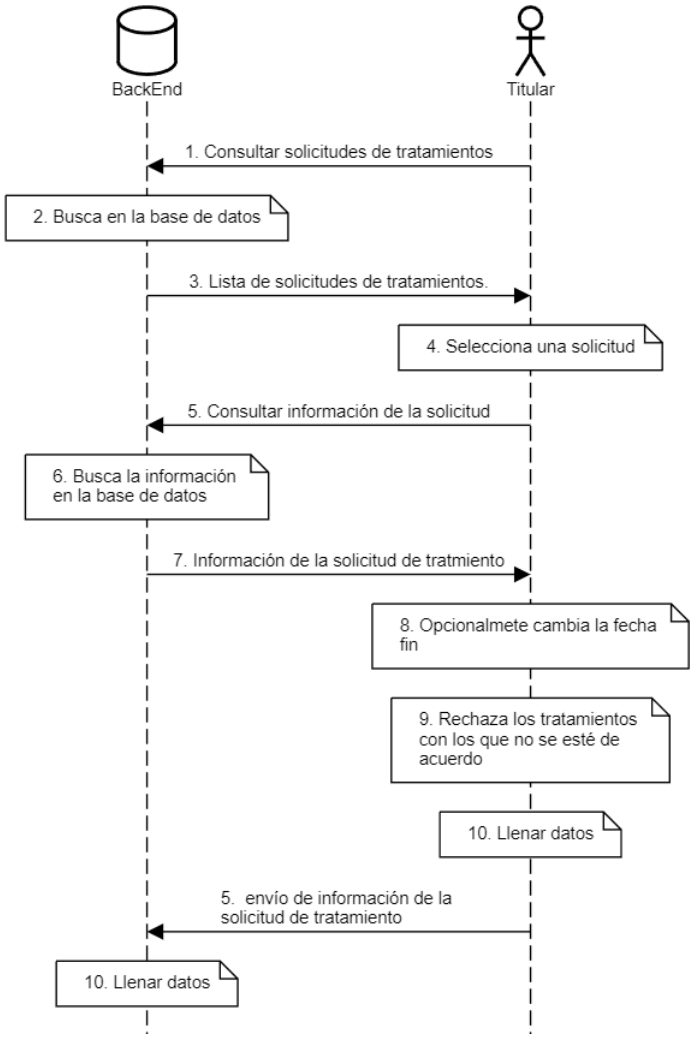

Figura 7.4: Diagrama de aceptación o rechazo para una solicitud de tratamiento. Elaborado por el autor.

cambiar la fecha fin del mismo. Es por eso que el tendrá el poder de realizar estas acciones por medio de la aplicación. A continuación, se muestra el flujo del proceso, acompañado de una vista mas gráfica en la Figura 7.5.

1. EL titular consulta los consentimientos.
2. El titular selecciona un consentimiento.
3. El titular rechaza los tratamientos que desee dentro del consentimiento.
4. El titular envía los tratamientos rechazados
5. El backend crea un nuevo bloque con el nuevo consentimiento.

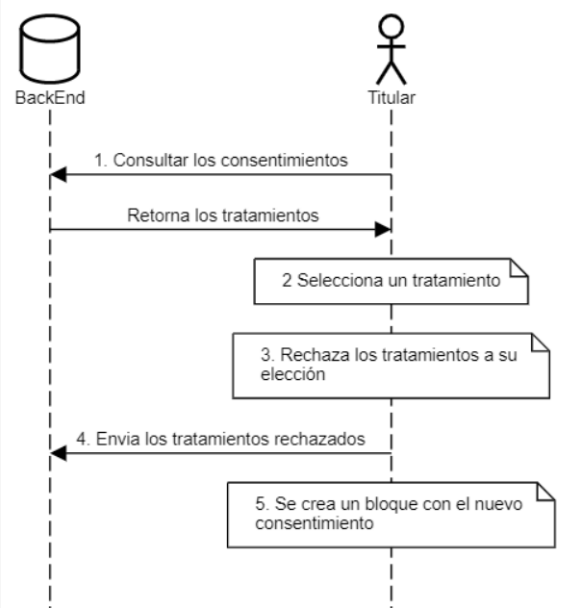

Figura 7.5: Diagrama de rechazo de tratamientos por parte del titular. Elaborado por el autor.

7.1.6 Exportación de datos por parte del responsable de tratamientos

Para poder hacer uso de los datos el responsable del tratamiento deberá obtenerlos directamente desde la aplicación, es por esto que se brindó la opción de exportación, para que de esta manera pueda exportar únicamente los datos a los que puede realizar un tratamiento y de igual forma que pueda obtener siempre los datos actualizados. A continuación, se muestra el flujo del proceso, acompañado de una vista mas gráfica en la Figura 7.6.

1. Filtra los usuarios por nombre o tratamientos.
    - ❒ En el caso de filtrar por nombre, se puede exportar los datos de todos los titulares o de un titular en específico.
    - ❒ En el caso de filtrar por tratamiento, retorna todos los datos de los titulares asociados a ese tratamiento.

7.1.7 Exportación de datos por parte del titular de los datos

La portabilidad de los datos es uno de los puntos mas importantes, y esto se traduce de igual forma a una exportación de datos en un formato entendible para el Titular. A conti-

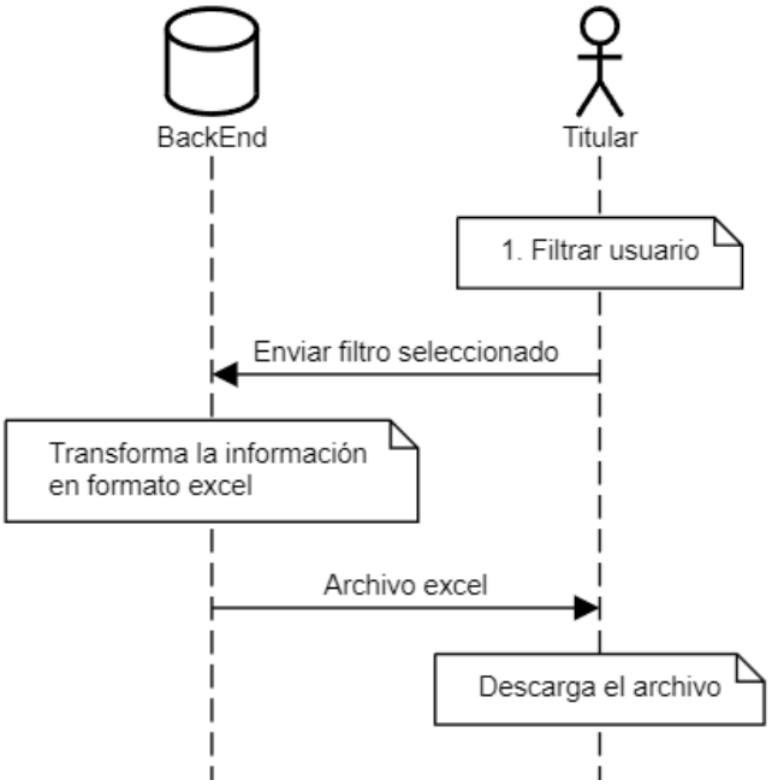

Figura 7.6: Diagrama de exportación de datos por parte del responsable de tratamiento. Elaborado por el autor.

nuación, se muestra el flujo del proceso, acompañado de una vista mas gráfica en la Figura 7.7.

1. El titular consulta todas las solicitudes de tratamiento.
2. El backend retorna de forma resumida los tratamientos.
3. El titular selecciona una solicitud.
4. El backend retorna la información del tratamiento.
5. El titular exporta los datos.

7.1.8 Comprobar inmutabilidad en el historial de los datos y de los tratamientos

Para comprobar la inmutabilidad de los datos se optó por la creación de un historial. Este historial es mostrado a forma del blockchain, en el cual se podrá comprobar la inmutabilidad mediante la comprobación de los hashes. A continuación, se muestra el flujo del proceso,

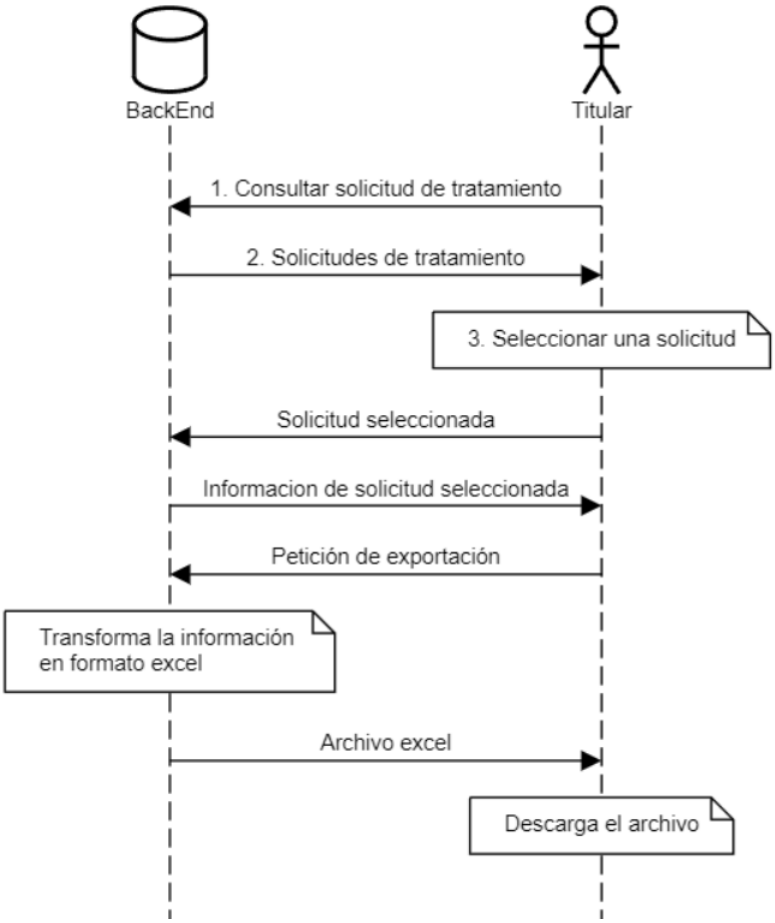

Figura 7.7: Diagrama de exportación de datos por parte del titular. Elaborado por el autor.

acompañado de una vista mas gráfica en la Figura 7.8.

1. El responsable del tratamiento consulta todas los tratamientos.
2. El backend retorna de forma resumida los tratamientos.
3. El responsable del tratamiento selecciona una solicitud.
4. El backend retorna todos los bloques asociados al titular y el responsable de los tratamientos.
5. El responsable del tratamiento toma la información para generar el hash y en una aplicación externa se genera el hash con SHA 256
6. Se comparan los hash, si son iguales los datos no han sido mutados, caso contrario la información ha sido manipulada.

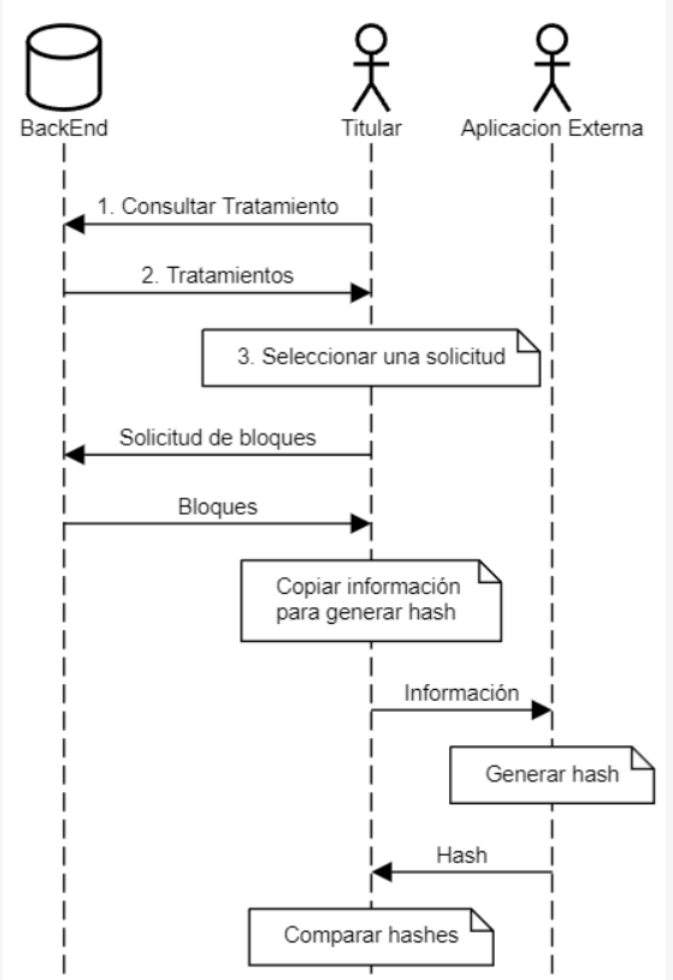

Figura 7.8: Diagrama de inmutabilidad en el historial de los datos y tratamientos. Elaborado por el autor.

7.2 FUNCIONAMIENTO DEL BLOCKCHAIN

En la siguiente sección se mostrará el funcionamiento del blockchain dentro de la aplicación. Para esto se mostrará a manera de un ejemplo como se crean los bloques. Para comenzar con el ejemplos debemos asumir la siguiente información.

Titulares registrados:

- ❒ **Titular 1**
  - ✧ **_id**: Titular 1
  - ✧ **nombre**: Boris
  - ✧ **apellido**: Caiza
  - ✧ **email**: boris.caiza@hotmail.com

- ✧ **ci**: 1756894512
- ✧ **contraseña**: 123456

❒ **Titular 2**

- ✧ **_id**: Titular 2
- ✧ **nombre**: Javier
- ✧ **apellido**: Jimenez
- ✧ **email**: javier.jimenez@hotmail.com
- ✧ **ci**: 0456454517
- ✧ **contraseña**: 123456

Responsables del tratamiento:

❒ **Responsable del tratamiento 1**

- ✧ **_id**: Responsable del tratamiento 1
- ✧ **nombre**: Pichincha
- ✧ **email**: usuario@pichincha.com
- ✧ **ruc**: 1789455623
- ✧ **contraseña**: 123456

❒ **Responsable del tratamiento 2**

- ✧ **_id**: Responsable del tratamiento 2
- ✧ **nombre**: Pichincha
- ✧ **email**: usuario@pichincha.com
- ✧ **ruc**: 1789455623
- ✧ **contraseña**: 123456

7.2.1 Creación del primer bloque

Para la creación del primer bloque de deben llevar a cabo los flujos de **Creación de solicitud de tratamiento por parte del responsable de tratamientos** y **Aceptación o rechazo y llenado de información para una nueva solicitud de tratamiento**.

La empresa1 creará una solicitud con la estructura que contendrá solicitudes para facturación electrónica y marketing. A continuación de mostrará la estructura que contendrá esta información.

Existe un parámetro data global, este contiene los datos globales que contendrán los permisos. Por ejemplo, el permiso facturación electrónica contiene en data el nombre y el apellido, mientras que el permiso de marketing contiene nombre, apellido y teléfono. El parámetro data global contiene la unión de estos data que se encuentran dentro de permisos, es decir nombre, apellido y teléfono, pero adicional contiene su valor como tal.

- ❒ **Email 1**
  - ✧ **_id**:Email 1
  - ✧ **Empresa**: {
    - ○ **_id**: Responsable del tratamiento 1
    - ○ **nombre**: Pichincha }
  - ✧ **Usuario**: {
    - ○ **_id**: Titular 1
    - ○ **nombre**: Boris }
  - ✧ **descripcionConsentimiento**: Por favor acepte el tratamiento de datos para una mejor experiencia.
  - ✧ **data**: [
    - ○ { **tipo**: nombre, **valor**: ”},
    - ○ { **tipo**: apellido, **valor**: ”},
    - ○ { **tipo**: celular, **valor**: ”}

    ]
  - ✧ **Permisos**: [{
    - ○ **tipo**: Facturación Electrónica
    - ○ **valor**: null,
    - ○ **descripción**: ’..’
    - ○ **data**: [nombre, apellido]

    },{
    - ○ **tipo**: Marketing

- **valor**: null,
- **descripción**: '..'
- **data**: [nombre, apellido, celular]

}]

- **fechaFin**: 28/02/2023
- **Observaciones**: '..'
- **Observaciones**: false
- **FechaEnvio**: 20/02/2023

El titular en su pantalla tendrá que aceptar los permisos que el considere apropiados, puede aceptar todo, rechazar todo o simplemente seleccionar los que el desee aceptar.
Si se rechaza todo no se añade un bloque nuevo al blockchain. Por otro lado, si decide aceptar alguno de los permisos se añadirá un nuevo bloque al blockchain con la estructura presentada a continuación.
Una vez respondido el email el atributo "Respondido" del email pasará a true. En este caso, asumimos que el titular de los datos ha decidió aceptar todos los permisos.
Hay que recordar que el atributo heigh representa la longitud de la cadena, en este caso como es el bloqueo génesis, es decir el primero, heigh es cero.
Si el blockchain tiene 20 bloques, entonces el atributo heigh del último bloque será 20, por otra parte, el atributo heighEnterprise representa el tamaño de la cadena, pero en la que el id de la empresa aparece, en otras palabras, si se añade un bloque y el id de la empresa es nuevo, es decir es la primera vez que la empresa se añade al blockchain, heighEnterprise será cero. Si el id de alguna empresa vuelve aparecer se coloca en heighEnterprise las veces que ha aparecido el id de la empresa en la cadena. Si el id de la empresa ha aparecido 5 veces en el blockchain heighEnterprise será 5. Más adelante se presenta un ejemplo de lo mencionado.
hashMain se genera a través de una función hash que contiene todo el bloque, el hashEnterprise es el hash del id del responsable del tratamiento concatenado con la hora en la que se creó que el bloque. Al tratarse del bloque génesis los previous hash (hash anteriores) son nulos. Para este ejemplo, el hashMain y el hashEnterpise son colocados con nombres fáciles de recordar a manera ilustrativa, el tributo body también esta remplazado por una cadena corta dado que su original es el bloque mismo.

- **Bloque 1**

- **_id**: Hash 1
- **hashMain**: Hash 1
- **hashEnterprise**: Hash responsable del tratamiento 1
- **previousHashMain**: null
- **previousHashEnterprise**: null
- **heigh**: 0
- **heighEnterprise**: 0
- **body**: body 1
- **body_enterprise**: body_enterprise
- **data**: [
    - { **tipo**: nombre, **valor**: 'Boris'},
    - { **tipo**: apellido, **valor**: 'Caiza'},
    - { **tipo**: celular, **valor**: '0999999999'}

  ]
- **Permisos**: [{
    - **tipo**: Facturación Electrónica
    - **valor**: True,
    - **descripción**: True
    - **data**: [nombre, apellido]

  },{
    - **tipo**: Marketing
    - **valor**: True,
    - **descripción**: '..'
    - **data**: [nombre, apellido, celular]

  }]
- **idUsuario**: Titular 1
- **idEmpresa**: Responsable del tratamiento 1
- **FechaFin**: 28/02/2023
- **FechaCreacion**: 20/02/2023

7.2.2 Creación del segundo bloque

Ahora el responsable de tratamiento 2, decide enviar un email de solicitu de tratamiento al titular 2, el email contendrá el consentimiento para facturación electrónica y markenting, al igual que el email anterior.
El email contendrá la misma estructura que el email anterior por lo tanto solo se colocará los cambios relevantes, en este caso los ids y los nombres.

- ❒ **Email 2**
  - ✧ **_id**:Email 2
  - ✧ **Empresa**: {
    - ○ **_id**: Responsable del tratamiento 2
    - ○ **nombre**: Guayaquil }
  - ✧ **Usuario**: {
    - ○ **_id**: Titular 2
    - ○ **nombre**: Javier }

Suponiendo que el usuario ha aceptado todos los permisos se creará el siguiente bloque, el cual es igual igual al bloque 1, por lo cual aquí únicamente se colocará los atributos más representativos, en este caso hashMain. HashEnterprise, previousHasMain, previousHashEnterprise, heihg y heighEnterprise. El bloque 2 se representa a continuación.

- ❒ **Bloque 2**
  - ✧ **_id**: Bloque 2
  - ✧ **hashMain**: Hash 2
  - ✧ **hashEnterprise**: Hash responsable del tratamiento 2
  - ✧ **previousHashMain**: Hash 1
  - ✧ **previousHashEnterprise**: null
  - ✧ **heigh**: 1
  - ✧ **heighEnterprise**: 0

7.2.3 Creación del tercer bloque

Ahora supongamos que el responsable de tratameinto 1 “Pichincha” decide enviar un email con el consentimiento de factura electrónica y marketing al titular 2, la estructura del email se presenta a continuación. Al igual que el email anterior solo se han colocado los atributos más representativos.

- ❒ **Email 3**
  - ✧ **_id**: Email 3
  - ✧ **Empresa**: {
    - ○ **_id**: Responsable del tratamiento 1
    - ○ **nombre**: Pichincha }
  - ✧ **Usuario**: {
    - ○ **_id**: Titular 2
    - ○ **nombre**: Javier }

Asumiremos que el usuario también aceptará el permiso de facturación electrónica y marketing dado que si lo rechaza no se creará un nuevo bloque. El bloque tendrá la siguiente estructura presentada a continuación, de igual manera solo se colocan sus atributos más representativos.

- ❒ **Bloque 3**
  - ✧ **_id**: Bloque 3
  - ✧ **hashMain**: Hash 3
  - ✧ **hashEnterprise**: (Hash responsable del tratamiento 1) 2
  - ✧ **previousHashMain**: Hash 2
  - ✧ **previousHashEnterprise**: Has responsable del tratamiento 1
  - ✧ **heigh**: 2
  - ✧ **heighEnterprise**: 1

Como se puede observar ahora previousHashEnterprise tiene el hashEnterprise del primer bloque, es decir del bloque de donde apareció la empresa 1 por última vez, y esta es la razón de la cual heighEnterpise ahora es 1, dado que es la segunda vez que el id de la empresa aparece, por otro lado, heigh es 2 dado que es tercer bloque de la cadena.

7.2.4 Creación del cuarto bloque

Ahora supongamos que el titular 2 decide cambiar uno de sus datos, como por ejemplo su nombre actualmente es “Javier” ahora se llama “Ricardo”.
Ahora las empresas tendrán que trabajar con el nombre “Ricardo” en vez de “Javier”, con lo que quiere decir que le data del usuario ha cambiado, por ende se tiene que añadir un bloque por cada empresa que tenga el consentimiento del usuario y en el cual se use su nombre.
Como se puede observar en el bloque a continuación, dentro de data el valor de nombre ha cambiado a Ricardo en este ejemplo se coloca únicamente hasta el atributo data del bloque, ya que los de más atributos son iguales a los del primero bloque. Adicional, se crearán dos bloques uno por cada empresa.

- ❒ **Bloque 4**
  - ✧ **_id**: Bloque 4
  - ✧ **hashMain**: Hash 4
  - ✧ **hashEnterprise**: (Hash responsable del tratamiento 2) 2
  - ✧ **previousHashMain** :Hash 3
  - ✧ **previousHashEnterprise**: Hash responsable del tratamiento 2
  - ✧ **heigh**: 3
  - ✧ **heighEnterprise**: 1
  - ✧ **body**: body 4
  - ✧ **body_enterprise**: body_enterprise
  - ✧ **data**: [
    - { **tipo**: nombre, **valor**: ’Ricardo’},
    - { **tipo**: apellido, **valor**: ’Jimenez’},
    - { **tipo**: celular, **valor**: ’0999999999’}

    ]

El bloque cinco contendrá la misma estructura del bloque 4, por lo tanto al igual que los bloques 2 y 3, solo se colocan sus atributos más representativos. Recordando que en este bloque dentro de data también cambio el valor de nombre de Javier a Ricardo.

❒ **Bloque 5**

- ✧ **_id**: Bloque 5
- ✧ **hashMain**: Hash 5
- ✧ **hashEnterprise**: (Hash responsable del tratamiento 1) 3
- ✧ **previousHashMain**: Hash 4
- ✧ **previousHashEnterprise**: (Hash responsable del tratamiento 1) 2
- ✧ **heigh**: 4
- ✧ **heighEnterprise**: 2

7.2.5 Creación del sexto bloque

Ahora supongamos que el Titular 1 decide eliminar el consentimiento de marketing del responsable del tratamiento 1, se creará el bloque presentado a continuación, en donde ya no se tiene en permisos el tratamiento marketing. Al igual que los bloques anteriores no se colocará todo el contenido del bloque.

❒ **Bloque 6**

- ✧ **_id**: Bloque 6
- ✧ **hashMain**: Hash 6
- ✧ **hashEnterprise**: (Hash responsable del tratamiento 1) 4
- ✧ **previousHashMain**: Hash 5
- ✧ **previousHashEnterprise**: (Hash responsable del tratamiento 1) 3
- ✧ **heigh**: 5
- ✧ **heighEnterprise**: 3
- ✧ **body**: body 6
- ✧ **body_enterprise**: body_enterprise
- ✧ **data**: [
  - ○ { **tipo**: nombre, **valor**: 'Boris'},
  - ○ { **tipo**: apellido, **valor**: 'Caiza'},
  - ○ { **tipo**: celular, **valor**: '0999999999'}

  ]

- ✧ **Permisos**: [{
  - **tipo**: Facturación Electrónica
  - **valor**: True,
  - **descripción**: True
  - **data**: [nombre, apellido]

}]

7.2.6 Resumen de la creación de bloques

A manera de resumen se presenta los atributos, hashMain, hashEnterprise, previousHash-Main, previousHashEnterprise, heigh y heighEnterprise en la Figura 7.9.

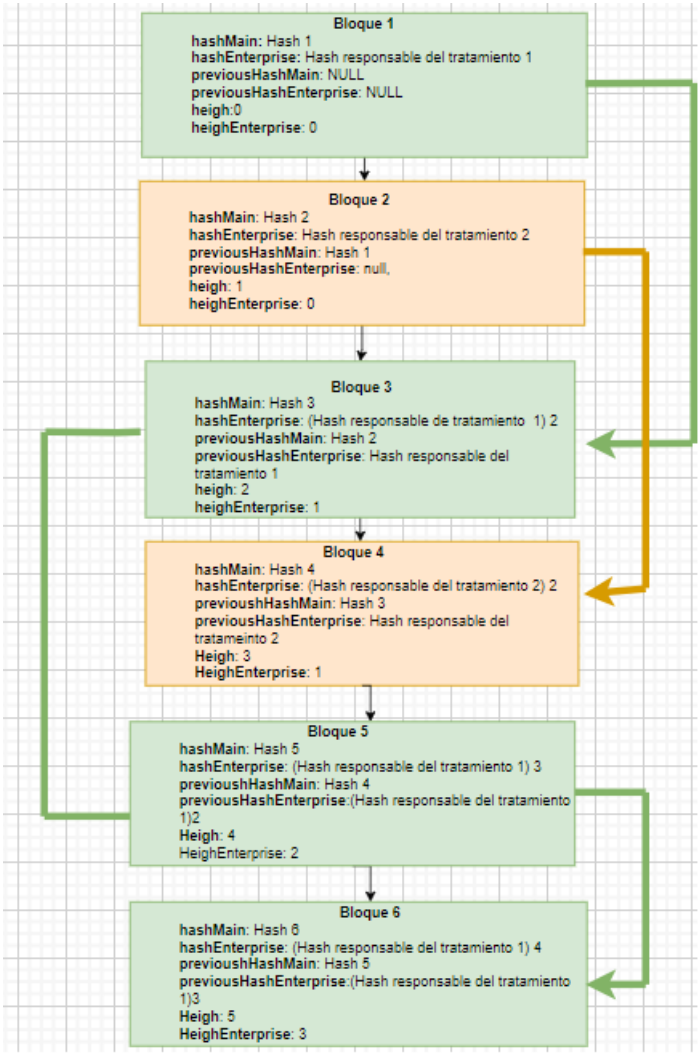

Figura 7.9: Representación de la creación de los primeros bloques: Creado por el Autor

8 CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

El presente proyecto tuvo como objetivo el generar un prototipo de una solución para la gestión del consentimiento y acceso a su información. Para llegar a un prototipo funcional, se realizó una revisión sistemática de la literatura. A través de la cual se encontraron posibles soluciones para atacar a la gestión del consentimiento, control de acceso y la portabilidad de los datos.

Además, se realizó el análisis de las soluciones encontradas para así encontrar las mejores y a partir de estas crear una solución propia. Como resultado de este análisis, tomando factores como el alcance del proyecto y el tiempo establecido se concluyó que la mejor opción fue crear un sistema central que haga de CMP el cual es un proveedor de gestor del consentimiento utilizando funciones de autenticación, para el acceso. De igual forma para tratar la gestión del consentimiento funcionalmente dentro del prototipo se hizo uso del blockchain.

Para el desarrollo del prototipo se utilizó la metodología de SCRUM la cual permitió un desarrollo ágil y rápido al igual que ayudó para poder adaptarnos a cambios o problemas que surgieron durante el desarrollo.

Finalmente, se obtuvo un prototipo funcional el cual permite gestionar el consentimiento, controlar el acceso y dar la portabilidad a los datos de los usuarios. Importante mencionar que la LOPDP fue la base para este proyecto por lo que es un documento de suma importancia la cual ayudará a los Ecuatorianos a tener el control sobre sus datos.

Como recomendación principal, es de vital importancia definir correctamente los objetivos y alcance del proyecto. De tal forma que no exista ambigüedad en los temas a tratar y que el proyecto fluya de una forma mas rápida.

Las metodologías tanto del desarrollo del proyecto como del prototipo son fundamentales ya que deben adecuarse a las necesidades que se tengan. En este caso el marco de re-

ferencia de SCRUM es perfecto para poder adaptarse a cambios rápidamente y avanzar progresivamente con entregas funcionales del prototipo.
Gracias al uso del lenguaje Javascript junto con al biblioteca de React y su entorno de ejecución Node.js, se pudo codificar en caliente, es decir que cada que se escribe una linea de código uno puede ver en tiempo real los cambios, sin necesidad de compilar el programa cada vez que se deseen ver los nuevos cambios. Lo cual ayuda a tener un desarrollo mas rápido y eficiente.

Durante el desarrollo se fueron detectando opciones de mejora las cuales caían fuera del alcance y tiempo por lo que no fueron ejecutadas. Por lo cual proponemos como primer punto cambiar la arquitectura de la aplicación cambiando de tener un blockchain centralizado a tenerlo de forma descentralizado pudiendo así asegurar de una forma mas fuerte la inmutabilidad de los datos y de igual forma generando mayor confianza para los usuarios al no tener una entidad centralizadora. Para esto se podría hacer que todos los responsables del consentimiento sean un nodo de la red descentralizada o se podría optar por usar una red como la de Etherium y utilizar lenguajes de programación como solidity que ayudarán a crear los contratos inteligentes.

9 REFERENCIAS BIBLIOGRÁFICAS

[1] M. Watts, *Why data is the new oil*. dirección: https://futurescot.com/why-data-is-the-new-oil/ (visitado 17-01-2022).

[2] J. vom Brocke, A. Hevner y A. Maedche, «Introduction to Design Science Research,» 2020, págs. 1-13. DOI: 10.1007/978-3-030-46781-4_1.

[3] B. Kitchenham y P. Brereton, «A systematic review of systematic review process research in software engineering,» *Information and Software Technology*, vol. 55, n.º 12, págs. 2049-2075, 2013, ISSN: 0950-5849. DOI: https://doi.org/10.1016/j.infsof.2013.07.010. dirección: https://www.sciencedirect.com/science/article/pii/S0950584913001560.

[4] CertiProf, *Scrum guide 2020*. dirección: https://certiprof.com/pages/scrum-guide-2020?mc_cid=a03704b479&mc_eid=8b5649b23c.

[5] *ISO 27001 - software ISO 27001 de Sistemas de Gestión*, jul. de 2022. dirección: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/.

[6] I. T. L. Computer Security Division, *Release search - NIST risk management framework: CSRC*, mayo de 2022. dirección: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/.

[7] *Ley de Protección de Datos Personales*, nov. de 2021. dirección: https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/.

[8] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System,» 2008.

[9] *¿Qué es la tecnología blockchain? - IBM Blockchain*. dirección: https://www.ibm.com/es-es/topics/what-is-blockchain.

[10] J. Ramos, *¿Qué es el daily scrum meeting?* Dirección: https://programacionymas.com/blog/daily-scrum-meeting.

[11] M. Petticrew y H. Roberts, *Systematic reviews in the Social Sciences: A practical guide*. Blackwell Pub., 2006.

[12] R. K. Jamra, B. Anggorojati, Kautsarina, D. I. Sensuse y R. R. Suryono, «Systematic Review of Issues and Solutions for Security in E-commerce,» en *2020 International Conference on Electrical Engineering and Informatics (ICELTICs)*, 2020, págs. 1-5. DOI: 10.1109/ICELTICs50595.2020.9315437.

[13] M. Alhajri, A. Salehi Shahraki y C. Rudolph, «Privacy of Fitness Applications and Consent Management in Blockchain,» en *Australasian Computer Science Week 2022*, ép. ACSW 2022, Brisbane, Australia: Association for Computing Machinery, 2022, págs. 65-73, ISBN: 9781450396066. DOI: 10.1145/3511616.3513100. dirección: https://doi.org/10.1145/3511616.3513100.

[14] T. Francis, M. Madiajagan y V. Kumar, «Privacy Issues and Techniques in E-Health Systems,» en *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*, ép. SIGMIS-CPR '15, Newport Beach, California, USA: Association for Computing Machinery, 2015, págs. 113-115, ISBN: 9781450335577. DOI: 10.1145/2751957.2751981. dirección: https://doi.org/10.1145/2751957.2751981.

[15] M. Hils, D. W. Woods y R. Böhme, «Measuring the Emergence of Consent Management on the Web,» en *Proceedings of the ACM Internet Measurement Conference*, ép. IMC '20, Virtual Event, USA: Association for Computing Machinery, 2020, págs. 317-332, ISBN: 9781450381383. DOI: 10.1145/3419394.3423647. dirección: https://doi.org/10.1145/3419394.3423647.

[16] C. Felix, H. Garg y S. Dikaleh, «Kubernetes Security and Access Management: A Workshop Exploring Security amp; Access Features in Kubernetes,» en *Proceedings of the 29th Annual International Conference on Computer Science and Software Engineering*, ép. CASCON '19, Toronto, Ontario, Canada: IBM Corp., 2019, págs. 395-396.

[17] G. Torok, M. R. Day, R. J. Hartman-Baker y C. Snavely, «Iris: Allocation Banking and Identity and Access Management for the Exascale Era,» en *Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis*, ép. SC '20, Atlanta, Georgia: IEEE Press, 2020, ISBN: 9781728199986.

[18] C. Pathmabandu, J. Grundy, M. B. Chhetri y Z. Baig, «ICME: An Informed Consent Management Engine for Conformance in Smart Building Environments,» en *Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, ép. ESEC/FSE 2021,

Athens, Greece: Association for Computing Machinery, 2021, págs. 1545-1549, ISBN: 9781450385626. DOI: 10.1145/3468264.3473118. dirección: https://doi.org/10.1145/3468264.3473118.

[19] X. Fan, Q. Chai, L. Xu y D. Guo, «DIAM-IoT: A Decentralized Identity and Access Management Framework for Internet of Things,» en *Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure*, ép. BSCI '20, Taipei, Taiwan: Association for Computing Machinery, 2020, págs. 186-191, ISBN: 9781450376105. DOI: 10.1145/3384943.3409436. dirección: https://doi.org/10.1145/3384943.3409436.

[20] S. Dramé-Maigné, M. Laurent, L. Castillo y H. Ganem, «Centralized, Distributed, and Everything in between: Reviewing Access Control Solutions for the IoT,» *ACM Comput. Surv.*, vol. 54, n.º 7, sep. de 2021, ISSN: 0360-0300. DOI: 10.1145/3465170. dirección: https://doi.org/10.1145/3465170.

[21] V. Kumar, J. Petit y W. Whyte, «Binary Hash Tree Based Certificate Access Management for Connected Vehicles,» en *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ép. WiSec '17, Boston, Massachusetts: Association for Computing Machinery, 2017, págs. 145-155, ISBN: 9781450350846. DOI: 10.1145/3098243.3098257. dirección: https://doi.org/10.1145/3098243.3098257.

[22] Q. Wang y H. Jin, «An Analytical Solution for Consent Management in Patient Privacy Preservation,» en *Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium*, ép. IHI '12, Miami, Florida, USA: Association for Computing Machinery, 2012, págs. 573-582, ISBN: 9781450307819. DOI: 10.1145/2110363.2110427. dirección: https://doi.org/10.1145/2110363.2110427.

[23] M. T. Islam, A.-e. M. Taha y S. Akl, «A survey of access management techniques in machine type communications,» *IEEE Communications Magazine*, vol. 52, n.º 4, págs. 74-81, 2014. DOI: 10.1109/MCOM.2014.6807949.

[24] P. J. Pesch, «Drivers and Obstacles for the Adoption of Consent Management Solutions by Ad-Tech Providers,» en *2021 IEEE European Symposium on Security and Privacy Workshops (EuroSPW)*, 2021, págs. 269-277. DOI: 10.1109/EuroSPW54576.2021.00034.

10 ANEXOS

1. **Video del Prototipo Funcional.** https://epnecuador-my.sharepoint.com/:f:/g/personal/milan_contreras_epn_edu_ec/EluJPpobTmVCmaaJ7NC0NwMB2b3WtPsHPy-U8i_jeYz00g?e=uldR9x
2. **Código FrontEnd.** https://github.com/TRABAJO-INTEGRACION-CURRICULAR-2022/frontend
3. **Código BackEnd.** https://github.com/TRABAJO-INTEGRACION-CURRICULAR-2022/backend