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

BORIS JAVIER CAIZA JIMÉNEZ
boris.caiza@epn.edu.ec

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

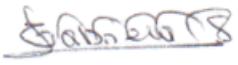
Quito, 03 marzo 2023

CERTIFICACIONES

Yo, BORIS JAVIER CAIZA JIMÉNEZ 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.

BORIS JAVIER CAIZA JIMÉNEZ

Certifico que el presente trabajo de integración curricular fue desarrollado por BORIS JAVIER CAIZA JIMÉNEZ, 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 DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

BORIS JAVIER CAIZA JIMÉNEZ

DRA. GABRIELA LORENA SUNTAXI OÑA

MILAN LEONARDO CONTRERAS ANDRADE

DEDICATORIA

A mi madre Francica, por todo el cariño brindado durante todo el trayecto de la carrera y por mantenerme motivado cada vez que me sentía cansado.
A mi padre Hernán, por siempre estar para mi cuando más lo necesitaba.
A mi hermano Mateo, que con sus ocurrencias siempre me mantenía feliz a pesar de estar agobiado con tanto trabajo.

AGRADECIMIENTOS

A todos mis grandes amigos, colegas de la universidad que hicieron de este viaje una experiencia maravillosa.

A mis familiares que siempre me alentaron y siempre estaban dispuestos a darme un consejo.

A mis amigos del colegio que a pesar del tiempo seguimos siendo grandes amigos.

A mi tutora la doctora Gabriela Lorena Suntaxi Oña por todo el apoyo y asesoramiento que me dio para cumplir esta meta.

CONTENIDO

RESUMEN

Actualmente la protección de datos personales ha sido un tema de discusión a nivel mundial. A nivel de leyes y reglamentos relacionados a este tema, en Europa existe la RGDP (Reglamento General de Protección de Datos), en California existe la CCPA (Ley de Privacidad del Consumidor), y en Ecuador se estableció la LOPDP (La Ley Orgánica de Protección de Datos Personales de Ecuador). Todas estas leyes dieron a las empresas un periodo de tiempo para que puedan adaptarse a este nuevo reglamento, en Ecuador la LOPDP, se publicó el 26 de mayo del 2021; las empresas ecuatorianas tienen un periodo de adaptación de dos años para cumplir con lo establecido en la LOPDP.

Estas leyes se han implementado para que cualquier usuario tenga total autoridad sobre sus datos personales. Con estas leyes se busca que las empresas antes de tratar los datos personales de cualquier usuario, primero deban tener su consentimiento, caso contrario no podrán tratar o manejar los datos de los usuarios.

Resulta crucial para toda empresa implementar una correcta gestión del consentimiento y control de acceso a la información personal para los datos del usuario. En el presente trabajo, se investigará por medio de una revisión sistemática de la literatura, acerca de las soluciones que permitan la gestión de consentimiento y control de acceso. Luego, se desarrollará un prototipo de software que permita garantizar la gestión de consentimiento y el control de acceso conforme lo establece la LOPDP. El prototipo a realizar contendrá las técnicas o soluciones que se concluyan de la revisión sistemática de la literatura.

PALABRAS CLAVE: LOPDP, Protección de datos personales, Gestión de Consentimiento, Control de Acceso

ABSTRACT

Currently, the protection of personal data has been a topic of discussion worldwide. At the level of laws and regulations related to this topic, in Europe there is the RGDP (General Data Protection Regulation), in California there is the CCPA (Consumer Privacy Act), and in Ecuador the LOPDP (The Organic Law for the Protection of Personal Data of Ecuador) was established. All these laws gave companies a period of time to adapt to this new regulation, in Ecuador the LOPDP was published on May 26, 2021; Ecuadorian companies have a period of two years to adapt to comply with the provisions of the LOPDP.

These laws have been implemented so that any user has full authority over their personal data. The purpose of these laws is that companies, before processing the personal data of any user, must first have the user's consent, otherwise they will not be able to process or handle the user's data.

It is crucial for any company to implement a proper management of consent and access control to personal information for user data. In this paper, we will investigate through a systematic literature review, about the solutions that allow the management of consent and access control. Then, a software prototype will be developed to ensure consent management and access control as established by the LOPDP. The prototype to be developed will contain the techniques or solutions concluded from the systematic literature review.

KEY WORDS: LOPDP, Personal Data Protection, Consent Management, Access Control

1 INTRODUCCIÓN

Muchas empresas ecuatorianas usan datos personales de sus usuarios para realizar varios procesos, como marketing, facturación electrónica, etc. Es muy común en estos días que recibamos una llamada desconocida y al contestar es una empresa ofreciéndonos algún tipo de servicio, la pregunta es, ¿Cómo consiguieron nuestro número telefónico? La LOPDP (Ley Orgánica de Protección de datos Personales) busca solucionar problemas como el mencionado anteriormente.

En algunas ocasiones resulta fastidioso que recibamos llamadas o correos de empresas que ni siquiera conocemos, con la LOPDP se busca que sea el usuario quien esté dispuesto a dar su consentimiento para que las empresas puedan utilizar sus datos. Es decir, la empresa primero deberá preguntar al usuario, por ejemplo, si está dispuesto o no recibir correos relacionados con el marketing, si es así, la empresa podrá utilizar los datos del usuario para enviar correos relacionados con el marketing.

Dadas estas nuevas necesidades de las empresas, es necesario optar por soluciones que permitan satisfacer los requerimientos de la LOPDP. Por esta razón, resulta indispensable realizar una revisión sistemática de la literatura para determinar soluciones a este tipo de problemas.

Para que las empresas puedan realizar un correcto consentimiento y que los usuarios puedan comprobar que sus datos están usando como ellos lo permitieron, se propone usar la tecnología blockchain. Dado la naturaleza y funcionamiento de blockchian de acuerdo con Welivesecurity en [1] cada vez que ocurre un cambio se crea un nuevo bloque, el conjunto de bloques formará una cadena que se encuentra entrelazada entre sí, de esta forma se garantiza la integridad de los datos.

1.1 OBJETIVO GENERAL

Realizar un prototipo que satisfaga la gestión del consentimiento del usuario y control de acceso a la información personal de acuerdo con lo establecido en la LOPDP.

1.2 OBJETIVOS ESPECÍFICOS

- ❒ Llevar a cabo una revisión sistemática de la literatura para identificar las soluciones tecnológicas orientados al control de acceso y gestión de consentimiento de datos personales.
- ❒ Identificar una solución tecnológica para el control de acceso y gestión de consentimiento de datos personales.
- ❒ Desarrollar un prototipo de software que garantice la gestión de consentimiento y control de acceso de datos personales de acuerdo con la LOPDP.

1.3 ALCANCE

Se utilizará la metodología propuesta por J. vom Brocke, A. Hevner y A. Maedche en [2] para realizar el presente estudio. 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 define el problema de investigación el cual es encontrar una solución para dar cumplimiento con lo establecido en la LOPDP.
- ❒ En la fase de definición de objetivos para una solución, se definen los objetivos del problema de investigación planteado. En esta fase, 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 en [3]. Esta metodología contiene 6 pasos estos son: 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 ejecutaron en base al marco Scrum que se plantea en [4] por CertiProf. Estas fases contemplan el desarrollo del prototipo de software que contendrá la solución encontrada en la revisión sistemática de la literatura.

- ❒ Finalmente, en la fase de comunicación, se realiza una publicación formal con los hallazgos, resultados y conclusiones del proyecto.

2 MARCO TEÓRICO

2.1 PRIVACIDAD DE LOS DATOS

Para entender el concepto de privacidad de datos primero hay que entender que es la privacidad. Según la real académica española en [5], la privacidad es el derecho de una persona a impedir la difusión de datos relativos a su vida privada que, aunque no sean difamatorios o nocivos, no desea que se divulguen.

Basados en este concepto, la privacidad de los datos no tiene un significado diferente. Muchas personas actualmente no tienen conocimiento de como se manejan sus datos en el internet. No es novedad que las personas tengan preocupación por su privacidad, pero no se preocupan por su privacidad en internet. La privacidad en internet es un tema relativamente nuevo del que no mucha gente es consciente. Muchas empresas contienen datos personales de sus usuarios y a menudo comparten estos datos con empresas terceras. Anteriormente no existían leyes que controlen este tipo de problemas. Las empresas al momento de compartir nuestros datos personales sin nuestro consentimiento violan directamente nuestra privacidad. Actualmente la mayoría de los países ya posee al menos una ley que regule este tipo de problemas. En esta investigación únicamente nos enfocaremos en la gestión de consentimiento y control de acceso, nos concentraremos en estos temas para encontrar una solución tecnológica adecuada conforme la Ley orgánica de Protección de Datos Personales en Ecuador.

En la siguiente subsección se describen las leyes de protección de datos personales más reconocidas a nivel mundial, se detalla brevemente la GDPR (Reglamento General de Protección de Datos) y la CCPA (Ley de privacidad del consumidor de California). En Ecuador se creó La Ley Orgánica de Protección de Datos Personales la cual se describe con más detalle en la siguiente sección.

2.1.1 GDRP (Reglamento General de Protección de Datos)

Es el reglamento europeo que tiene como objetivo dar el control a cualquier persona sobre sus datos personales. El reglamento entró en vigencia el 24 de mayo de 2016 y finalmente se aplico dos años después, el 25 de mayo de 2018. Al ser un reglamento europeo aplica a toda empresa que se encuentre en la unión europea que maneje todo tipo de información personal. En la referencia [6] se el reglamento en su versión en español.

2.1.2 CCPA (Ley de privacidad del consumidor de California)

La ley de privacidad del consumidor de California tiene el objetivo de brindar a los consumidores control sobre sus datos personales. De acuerdo con el Departamento de Justicia de California en [7], los consumidores tienen los siguientes derechos:

1. Derecho a saber que información tienen las empresas y con quien las comparte.

2. Derecho a que las empresas eliminen sus datos (aplican condiciones).

3. Derecho a negarse a la venta de su información.

4. Derecho a no ser descriminado por ejercer los derechos de la CCPA.

2.2 LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES

La Ley Orgánica de Protección de Datos Personales (LOPDP) entró en vigencia en Ecuador el 26 de mayo del 2021, dando a la empresas públicas y privadas un periodo de 2 años para poder adaptarse a esta norma.

De acuerdo con la Asamblea Nacional del Ecuador en [8], la LOPDP busca que los titulares de los datos tengan total control sobre los mismos y sean ellos quienes decidan a quien le entregan sus datos personales.

La ley también nos habla de los actores involucrados que existen en la LOPDP. El artículo 5 presenta los actores que existen en la ley, los cuales se mencionan a continuación.

2.2.1 Actores en la Ley Orgánica de Protección de Datos

1. **Titular:** Persona natural dueña de sus datos personales, sus datos personales son objeto de tratamiento.
2. **Responsable del tratamiento:** Persona encargada del tratamiento de datos de uno o varios titulares.
3. **Encargado del tratamiento:** Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo que solo o conjuntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales.
4. **Destinatario:** Persona natural o jurídica que ha sido comunicada con datos personales.
5. **Autoridad de protección de datos personales:** Una autoridad estatal independiente, es responsable de monitorear la aplicación de esta ley.
6. **Delegado de protección de datos personales:** Persona natural encargada de informar al responble o al encargado del tratamiento sobre sus deberes a cumplir en relación con la protección de datos, también es el encargado de supervisar que se cumpla la ley.

La LOPDP contiene un total de 77 artículos. La LOPDP tiene una similitud con la GDPR (Reglamento General de Protección de Datos) que es la ley aplicada para protección de datos personales de la unión europea, después de una lectura de ambas leyes se concluyó que ambas tienen los mismos derechos individuales, los cuales se mencionan a continuación y que son resumidos, para su completa lectura en la referencia [9] se encuentra la LOPDP completa.

2.2.2 Derechos indivivuales de Ley Organica de Protección de Datos Personales

Los derechos individuales se refieren a los derechos que tienen los titulares de sus datos sobre los mismos. A continuación se resumen los artículos que representan los derechos individuales.

1. **Derecho a la información (Artículo 12)**
   Los titulares de los datos personales tienen derecho a ser informados de cualquier forma o medio, con base en los principios de lealtad y transparencia.

2. **Derecho al acceso (Artículo 13)**
   El titular tiene derecho a conocer y obtener todos sus datos personales y la información descrita en el artículo 12 del responsable del tratamiento en forma gratuita y sin dar razón alguna.

3. **Derecho de rectificación y actualización (Artículo 14)**
   El titular tiene derecho a solicitar al responsable del tratamiento la corrección y actualización de sus datos personales inexactos o incompletos.

4. **Derecho de eliminación (Artículo 15)**
   El responsable del tratameinto tiene que eliminar los datos personales de un titular, si el titular lo solicita.

5. **Derecho de oposición (Artículo 16)**
   El responsable del tratamiento tiene que detener el tratamiento de los datos personales de un titular, si el titular lo solicita.

6. **Derecho a la portabilidad (Artículo 17)**
   El responsable del tratamiento tiene que envíar los datos al titular en un formato compatible, común, estructurado, actualizado y de lectura mecánica, si el titular lo solicita.

7. **Derecho a la suspensión del tratamiento (Artículo 19)**
   El responsable del tratamiento deberá suspender el tratamiento de datos del titular, si el titular lo solicita.

8. **Derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas (Artículo 20)**
   El titular tiene derecho a no ser sometido a una decisión basada única o parcialmente en valoraciones que sean producto de procesos automatizados.

Todos estos artículos se aplican una vez que los datos personales del usuario ya han sido recolectados, es decir una vez que el usuario nos ha entregado su consentimiento. Basado en lo dicho anteriormente existe el artículo 8 de la LOPDP, el cual menciona que se podrá comunicar y tratar datos personales siempre y cuando el titular de los datos haya dado su voluntad para hacerlo.

2.3 CONTROL DE ACCESO

Un control de acceso permite el uso de recursos a usuarios que tienen los respectivos permisos. Por ejemplo, un guardia en una entrada de una fiesta privada es un control de acceso dado que solo tiene que permitir el acceso a las personas que se encuentran invitadas. La definición formal de acuerdo con Jones y Bartlett Learning en [10] es que un control de acceso ofrece la capacidad de acceder a recursos tanto físicos como lógicos, si hablamos de recuros físicos nos referimos a un edificio, ciudad o país, si hablamos de recursos lógicos nos referimos a una aplicación web, movil, etc.

Basado en estas premisas podemos decir que el control de acceso es parte fundamental para que los derechos individuales mencionados en el apartado 2.2.2 puedan cumplirse. Por ende, también es esencial para que las empresas ecuatorianas puedan adaptarse a LOPDP. Existen diferentes tipos de control de acceso. Sin embargo, la mayoría de autores menciona 3 principales estos son el control de acceso discrecional también conocido como DAC, control de acceso basado en roles también conocido como RBAC y control de acceso obligatorio también conocido como MAC. De estos tres modelos se derivan una gran variedad de controles de acceso. A continuación, se presentan los requerimientos relacionados con el control de acceso concorde lo establecido en la LOPDP para el prototipo de software a desarrollarse.

Tabla 2.1: Requerimientos relacionados al control de acceso conforme la LOPDP

Código.	Requerimiento	Artículo
A001	Cuando el titular de los datos solicita sus datos, el sistema mostrará los datos al titular.	13
A002	Cuando el titular de los datos decida ver sus datos y para que están siendo usados en una empresa, el sistema deberá mostrar dicha información.	34

2.3.1 Política de control de acceso

De acuerdo con IBM en [11] una política de control de acceso son un conjunto de condiciones que tienen una evaluación, una vez se hayan evaluado estas condiciones se determinar las decisiones de acceso.

Entonces podemos decir que un control de acceso permite al usuario acceder a recursos de acuerdo a una política de control de acceso, la cual tiene que estar definida con antelación. El control de acceso permitirá al usuario acceder a los recursos si el usuario cumple la política, si no la cumple el usuario no podrá acceder a los recursos.

2.3.2 Tipos de control de acceso

1. **Control de acceso discrecional (DAC)**

   En el control de acceso discrecional, el propietario de los datos o recursos es el que se encarga de permitir o no que otros usuarios accedan a sus datos o recursos.

   Por ejemplo, en la Figura 2.1, se puede observar tres pasos que son representados por círculos. En el primer paso un grupo de usuarios quiere acceder a recursos propietarios de otro usuario, lo que hace el control de acceso discrecional es preguntar en el segundo paso las políticas de control de acceso que ha definido el usuario propietario. En el tercer paso se da respuesta en base a que si el grupo de usuarios tiene acceso o no, en caso de que si, los usuarios pueden acceder a los recursos en caso de que no se deniega la solicitud planteadas por los usuarios inicialmente.

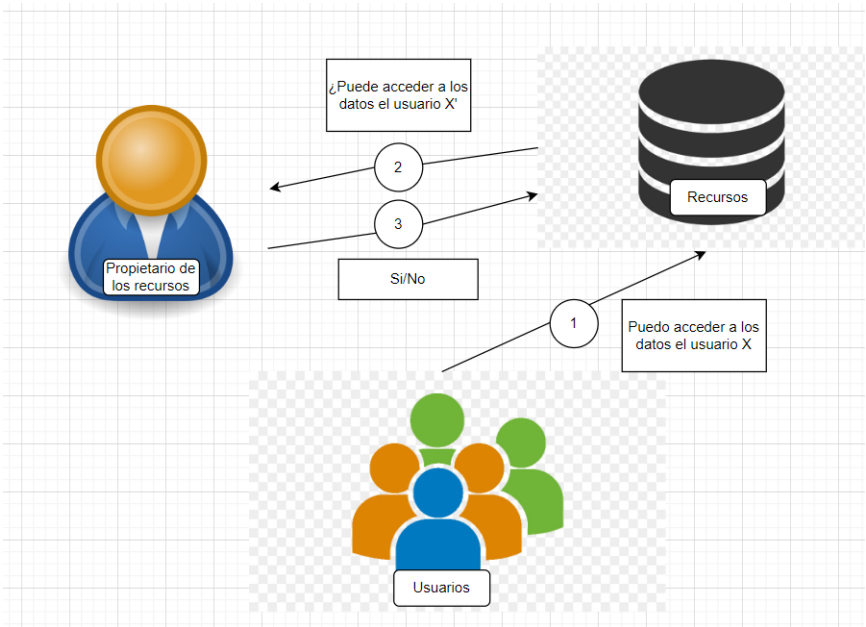


Figura 2.1: Ejemplo de control de acceso discrecional Fuente: Elaborada por el autor

2. **Control de acceso basado en roles (RBAC)**

   El control de acceso basado en roles se centra en asignar permisos a usuarios de acuerdo con sus funciones. Por ejemplo, en una empresa existe el departamento de contabilidad y el departamento de ventas. Las personas que trabajan en el departamento de contabilidad solo deben tener acceso a los datos que un contador debe tener, y lo mismo ocurre con las personas que trabajan en el departamento de ventas. En la Figura 2.2 se puede observar un ejemplo del control de acceso basado en roles en donde en primera instancia los usuarios son asignados a un rol, luego este rol tiene acceso a ciertos recursos.

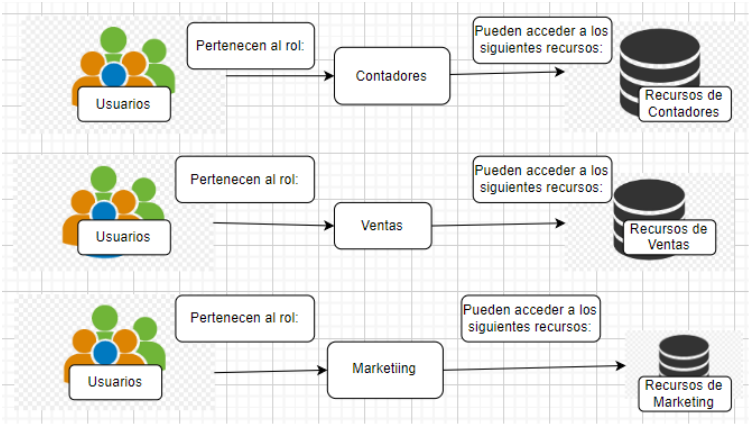


Figura 2.2: Ejemplo de control de acceso basado en roles Fuente: Elaborada por el autor

3. **Control de acceso obligatorio (MAC)**

   El control de acceso obligatorio se basa en politicas de control de acceso definidos por una autoridad central. Es decir, él administrador del sistema es quien define las reglas, en pocas palabras define que usuarios tienen acceso a ciertos recursos. En la Figura 2.3, se observa un ejemplo de este control de acceso. Esta representación consta de tres pasos, los pasos son representados por círculos. En el primer paso los usuarios hacen una solicitud para acceder a los recursos, en el segundo paso se comprueba que los usuarios puedan acceder a los recursos si estos tienen los permisos, en el tercer paso acceden a los recursos como tal.

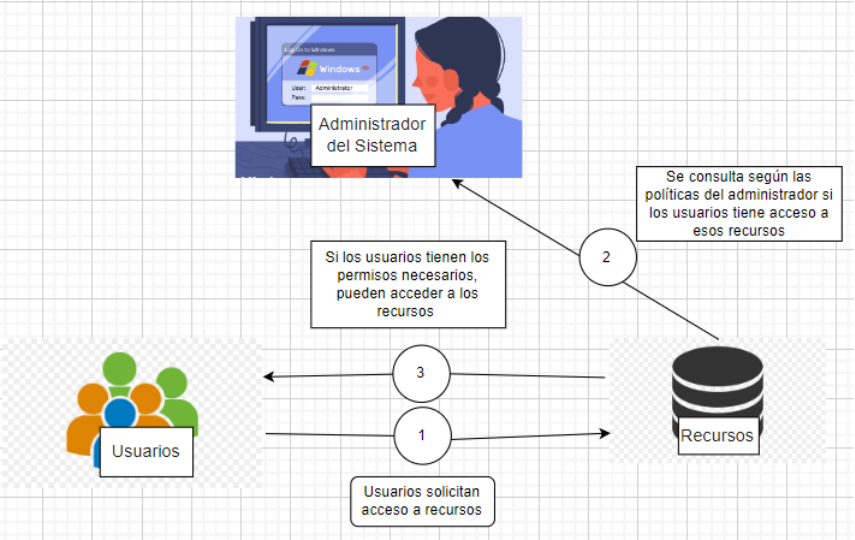


Figura 2.3: Ejemplo de control de acceso obligatorio Fuente: Elaborada por el autor

2.4 GESTIÓN DE CONSENTIMIENTO

De acuerdo con Cookiebot en [12], la gestión de consentimiento es la acción de obtener el consentimiento de los usuario para poder tratar su dados personales. Con esta definición básicamente necesitamos el consentimiento del usuario para poder realizar cualquier tipo de tratamiento sobre sus datos. Existen diversos productos de software que ya realizan esta tarea y que surgieron de la necesidad de las recientes leyes relacionadas a la protección de datos personales. Los productos de software que realizan ese tipo de acciones se llaman plataformas de gestión de consentimiento o CMP por sus siglas en inglés. Varios de estos productos de software son usados para poder cumplir con las leyes de protección de datos personales que han sido impuestas en los diferentes países. Los CMP son muy requeridos y han tenido bastante fama con la llegada de estas leyes, por lo cual hay muchas empresas que optan por subcontratar estos productos de software para poder cumplir con las leyes actuales como puede ser la GDPR o la CCPA.

A continuación, en la Tabla 2.2 se presentan los requerimientos relacionados con la gestión de consentimiento de acuerdo con la LOPDP para el prototipo de software a realizar.

Tabla 2.2: Requerimientos relacionados la gestión de consentimiento conforme la LOPDP

Código.	Requerimiento	Artículo
C001	Cuando el titular entregue su consentimeinto el sistema almacenerá sus datos personales para el tratamiento de los mismos	7
C002	Cuando el titular de los datos requiere cualquier información respecto al artículo 12 el sistema mostrará los mismos.	12
C003	Cuando el titular decida rectificar o actualizar sus datos, el sistema actualizara sus datos personales.	14
C004	Cuando el titular decida eliminar sus datos personales el sistema eliminara los datos personales del titular.	15
C005	Cuando el titular decida oponerse al tratamiento de sus datos personales el sistema restringera el tratamiento de los mismos.	16
C006	Cuando el titular decida suspender el tratamiento de sus datos personales el sistema restringera el tratamiento de los mismos.	19
C007	Cuando los datos de un titular lleguen a su fecha de finalización de acuerdo con el consentimiento firmado, el sistema deberá eliminarlos automáticamente	34

2.5 CONTROLES INTERNACIONALES PARA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

A continuación, se detallan brevemente dos de los estándares más famosos en el mundo, estos estándares contienen varios controles relacionados con los sistemas de información que pueden ser relacionados con nuestro tema de estudio, es decir el control de acceso y la gestión de consentimiento.

2.5.1 ISO 27001

ISO significa Organización Internacional de Normalizació de acuerdo con ISOTOOLS en [13], la ISO 27001 es una norma internacional que tiene como objetivo garantizar la confidencialidad e integridad de la información.

La norma contiene controles de todo tipo que pueden ser aplicado a las organizaciones para que así estas puedan asegurar la confidencialidad e integridad de sus sistemas de información.

2.5.2 NIST sp 800-53

NIST es el instituto de nacional de estándares y tecnología. De acuerdo con la página oficina de la NIST en [14] la NIST sp 800-53 contiene temas relacionados a los controles de seguridad para sistemas de información y organizaciones.

2.6 BLOCKCHAIN

Blockachain es una tecnología que se basa en bloques, el conjunto de bloques crea una cadena. Cada que se modifique un dato se creará un nuevo bloque en la cadena, de esta manera se tiene un historial de todos los cambios que se han realizado sobre los datos. A parte de esto cada bloque está unido al anterior a través de un hash, el hash se genera a través de una función hash de datos que contiene el bloque, la unión de bloques se representa en la Figura 2.4 en donde cada bloque contiene el hash del bloque anterior. El hash anterior del primer bloque es null dado que no existe un bloque anterior. Los datos que contiene cada bloque varían de acuerdo con la lógica del negocio. Por ejemplo, en las criptomonedas por lo general el hash del bloque se lo genera a través de las transacciones realizadas.

Blockchain también se caracteriza por ser una red descentralizada, es decir hay varios nodos y no existe un servidor. Cada nodo contiene el blockchain como tal y al haber un cambio en el blockchain cada nodo la transmite a todos los demás nodos el nuevo cambio. En pocas palabras la base de datos que en este caso es el blockchain, se encuentra en

todos los nodos por lo cual es muy difícil de violar su integridad.

Figura 2.4: Enlace entre los bloques de un blockchain Fuente: Elaborado por el autor

3 METODOLOGÍA

Al tratarse de un trabajo de integración curricular el siguiente cápitulo fue desarrollado en conjunto por parte del los miembros del grupo.

Para el desarrollo de la presente investigación se usaron tres metodologías, una para realización del proyecto que es la metología DSR propuesta por Jan vom Brocke, Alan Hevner y Alexander Maedche en [2]. Para la realización de la revisión sistematica de la literatura se usó la metodología propuesta por B. Kitchenham and S Charters en [3]. Finalmente para la elaboración del prototipo de software se uso el marco SCRUM, que se encuentra detallada de acuerdo con CertiProf en [4]. A continuación se detalla cada una de estas metodologías y el marco Scrum. Adicionalmente, la Figura 3.1 presenta un resumen de lo descrito anteriormente.

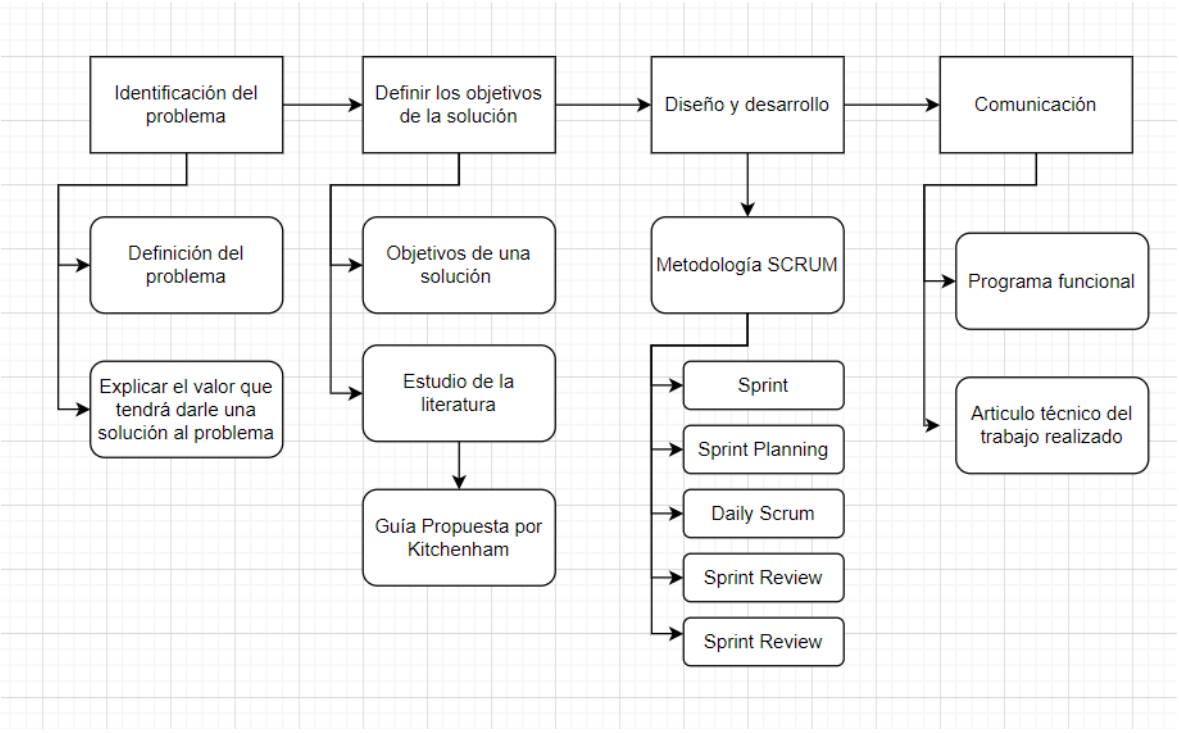


Figura 3.1: Metología escogida para la investigación Fuente: Elaborado por el autor

3.1 DSR

De acuerdo con Jan vom Brocke, Alan Hevner y Alexander Maedche en [2], DSR es un paradigma de resolución para mejorar el conocimiento, por medio de la realización de artefactos innovadores.

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. Demostrar lo importante que es una solución, hace dos cosas:

   a) Motiva al investigador

   b) Ayuda a la audiencia a la comprensión del problema que plantea el ivestigador

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. Estos objetivos pueden ser tanto cualitativos como cuantitativos.

3. **Diseño y desarrollo**

   Se crea conceptualmente el artefacto. Esta actividad implica desarrollar la función que se desea que el artefacto tenga, así como también su arquitectura.

4. **Demostración**

   Esta actividad implica el uso del artefacto como tal. Se realizan pruebas, simulaciones, estudios de casos, pruebas o cualquier otra actividad pertinente.

5. **Evaluación**

   En esta actividad se evaluá 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 SCRUM

Scrum es un marco ágil de desarrollo de software. Tiene un conjunto de buenas prácticas y eventos a seguir que buscan garantizar la calidad de un producto de software. Consta de 5 eventos principales de acuerdo con CertiProf en [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 realizará en el Sprint. En general de acuerdo con CertiProf en [4] se plantean tres preguntas, las cuales se presentan a continuación.

   a) ¿Por qué es importante el Sprint?

   b) ¿Qué se puede realizar en el Sprint?

   c) ¿Cómo se desarrollaá el trabajo elegido?

3. **Daily Scrum**

   Es una ruenión de 15 minutos como mínimo por parte de los desarrolladores del equipo. En estas reuniones se busca ver el avance diario que ha tenido cada desarrollador. Por lo general se realizan las siguientes preguntas de acuerdo con Ramos en [15].

   a) ¿Qué hiciste ayer?

   b) ¿Que harás hoy?

   c) ¿Hay impedimentos en tu camino?

4. **Sprint Review**

   El objetivo del sprint review es analizar lo que se ha logrado en el sprint. En pocas palabras esta reunión ocurre una vez que el sprint ha finalizado. Con la información obtenida en el análisis, los presentes en la reunión determinar sobre que se hará a continuación.

5. **Sprint Retrospective**

   Con esta fase se concluye el sprint, es una reunión para descrubir las fortalezas y problemas del sprint para de esta manera mejorar para el siguiente sprint.

3.3 REVISIÓN SISTEMÁTICA DE LA LITERATURA

Kitchenham nos propone una guía para realizar una revision sistemática de la literatura de acuerdo con [16], esta metodología se centra en la 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.

3.3.1 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: Identificar una necesidad, comisionar una revisión, especificar las preguntas de investigación, desarrollar un protocolo de revisión y evaluar el protocolo de revisión.

- ❒ **Identificar 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. Además, se debe definir las razones por las cuales decidiremos realizar la revisión.

- ❒ **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:** Se formulan 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, en 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 sistemática de la literatura. 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.

3.3.2 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 la síntesis de datos.

- ❒ **Identificación de la investigación:** El objetivo esta fase es encontrar el mayor número 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 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 estar relacionados con las preguntas formuladas para resaltar las similitudes y diferencias entre los resultados de la investigación.

3.3.3 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. Si es un paper, se deberá buscar expertos para que puedan revisar el documento, antes de que este sea publicado en la web.

4 REVISIÓN SISTEMÁTICA DE LA LITERATURA SOBRE EL CONTROL DE ACCESO Y GESTIÓN DEL CONSENTIMIENTO

Para la revisión sistemática de la literatura se usó la metodología propuesta por Kitchenham en [3]. Se decidió escoger Kichenham ya que es una metodología centrada en la comunidad de la ingeniería de software. La metodología consta de 5 pasos que se desarollan a continuación.

4.1 PREGUNTAS DE INVESTIGACIÓN

Las preguntas de investigación se las realizó con el objetivo de determinar las técnicas usadas para poder realizar una correcta gestión del consentimiento y control de acceso. Basada en esta declaración se planteó las siguientes preguntas:
RQ1 ¿Cuáles son las soluciones para poder realizar una correcta gestión del consentimiento de datos personales?
RQ2 ¿Cuáles son las soluciones para poder realizar una correcta gestión del acceso a los datos personales?
Con las preguntas RQ1 Y RQ2 se busca obtener mediante el análisis de publicaciones soluciones para una correcta gestión de consentimiento y acceso de datos personales

4.2 PROCESO DE BÚSQUEDA

Para realizar la búsqueda se decidió buscar artículos que contengan la siguiente cadena de búsqueda:

(consent management OR access control) AND (solution OR technique)

Para el proceso de búsqueda se escogió las bases de datos con más reconocimiento con respecto al área de la ingeniería y al área de las ciencias de computación, las librerías usadas fueron las siguientes:

- ACM Digital Library
- IEEE Xplore
- ScienceDirect

4.3 CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

A continuación, se presentan los criterios de inclusión planteados para la presente revisión sistemática de la literatura:

- Artículos que contengan en su título la cadena de búsqueda planteada
- Artículos publicados entre el 1 de enero de 2012 y 2 de mayo del 2022.

Se escogieron los artículos publicados en los último 10 años dado que la protección de datos personales es relativamente un tema nuevo. Por ejemplo, la RGDP (Reglamento General de Protección de datos) se aprobó el 14 de abril de 2016 y entró en vigor el 25 de mayo de 2018. Sin embargo, esto no quiere decir que no existan leyes relacionadas a la protección de datos personales, por ejemplo en España existía la LOPD (Ley Orgánica de Protección de Datos de Carácter Personas), que quedó obsoleta con la RGDP, la LOPD fue aprobada en 1999, basada en estos dos argumentos consideremos que un margen de 10 años es un margen correcto para nuestra investigación.

A continuación, se presentan los criterios de exclusión:

- Artículos que tengan contenido menor o igual a 5 páginas sin contar las citas bibliográficas.
- Artículos que estén escritos en un idioma diferente al inglés.
- Artículos que no contengan DOI.
- Artículos que no contengan soluciones o técnicas específicas para la gestión del consentimiento de datos personales

- ❒ Artículos que no contengan técnicas específicas para la gestión de acceso de datos personales.
- ❒ Artículos que realicen una comparación, una revisión sistematica de la literatura, discusión, taller y encuesta sobre técnicas de control de acceso o gestión de consentimiento.
- ❒ Artículos que traten sobre técnicas de control de acceso que no estén relacionados directamente al manejo de datos personales, como por ejemplo técnicas de control de acceso en el área de redes de computadoras.

4.4 SELECCIÓN DE ARTÍCULOS

En la primera fase de la búsqueda se filtró los artículos que contengan en su título la cadena planteada anteriormente, con este criterio en la primera fase de la búsqueda se encontraron 863 artículos desglosados de la siguiente manera:

- ❒ ACM Digital Library: 756
- ❒ IEEE Xplore: 67
- ❒ ScienceDirect: 40

En la segunda fase de la búsqueda se filtró los artículos que hayan sido publicados entre las fechas 1 de Enero del 2012 y el 13 de Junio del 2022. De esta manera se encontraron los 410 artículos, desglozados de la siguiente manera:

- ❒ ACM Digital Library: 351
- ❒ IEEE Xplore: 36
- ❒ ScienceDirect: 23

En la tercera fase de búsqueda se filtraron los artículos de acuerdo con los criterios de inclusión y exclusión planteados, esta búsqueda fue realizada manualmente. De esta manera en la tercera búsqueda se encontraron 14 artículos distribuidos de la siguiente manera:

- ❒ ACM Digital Library: 5

- ❒ IEEE Xplore: 5
- ❒ ScienceDirect: 4

En la cuarta fase de la búsqueda se procedió a eliminar los artículos duplicados de esta manera se obtuvo un total de 13 artículos finales.

La Figura 4.1 muestra un resumen del procesos realizado para poder llegar a la selección final de artículos.

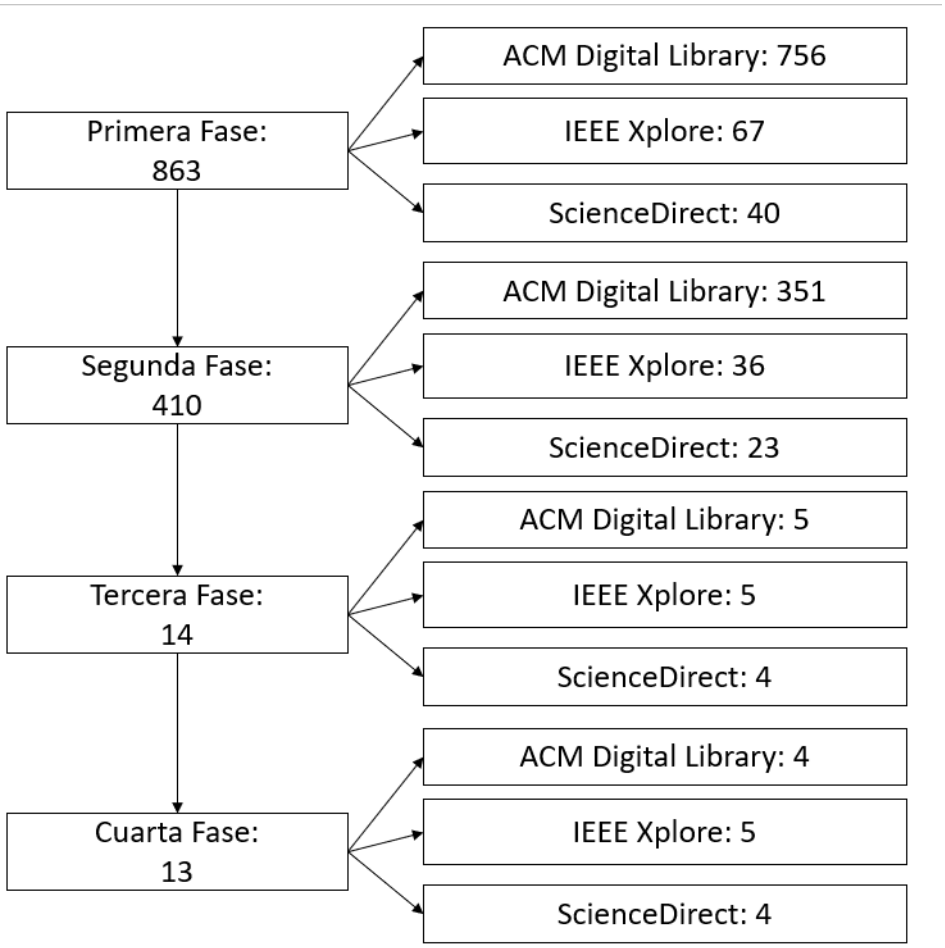


Figura 4.1: Fases del procesos de selección de artículo Fuente: Elaborada por el autor

4.5 EVALUACIÓN DE CALIDAD

Para este paso se siguieron los criterios de calidad propuestos por Kurnia Jamra, Anggorojati, Kautsarina, Indra Sensure y Randy Sutyono en [17], se seleccionaron las preguntas que pueden ser aplicadas a esta revisión sistemática de la literatura, estas 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. ¿El artículo describe la arquitectura propuesta de la metodología utilizada?
- ❒ P4. ¿El artículo tiene resultados de investigación?
- ❒ P5. ¿El artículo muestra conclusiones que son relevantes para el propósito/problema planteado de la investigación?
- ❒ P6. ¿El artículo recomienda trabajo futuro o mejoras para el futuro?

Los artículos serán clasificados con un puntaje de acuerdo con la Tabla 4.1. Por ende, la calificación 1 será “si”, la calificación 0.5 será “parcialmente” y 0.0 será “No”.

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	El artículo detalla de manera clara y concisa la metología usada.	El artículo detalla de manera parcial la metología usada..	El artículo no detalla la metología usada.
P4	El articulo detalla claramente los resultados obtenidos en la investigación.	El articulo detalla parcialmente los resultados obtenidos en la investigación.	El articulo no detalla los resultados obtenidos en la investigación.
P5	El articulo detalla claramente las conlcusiones obtenidos en la investigación.	El articulo detalla parcialmente las conlcusiones obtenidos en la investigación.	El articulo no detalla las conlcusiones obtenidos en la investigación.

	Si (puntaje 1.0)	Parcial (puntaje 0.5)	No (puntaje 0.0)
P6	El articulo recomienda mejoras en su investigación o mejoras para el futuro.	El articulo recomienda parcialmente mejoras en su investigación o mejoras para el futuro.	El articulo no recomienda mejoras en su investigación o mejoras para el futuro.

4.6 EXTRACCIÓN DE DATOS

Los datos extraídos de los artículos fueron los siguientes:

- ❒ Información bibliográfica (titulo, año de publicación, tipo de publicación)
- ❒ Soluciones para la gestión de consentimiento de datos personales.
- ❒ Soluciones para la el control de acceso a los datos personales de los usuarios.
- ❒ Palabras clave de cada artículo.

4.7 RESULTADOS

Los 13 artículos finales se describen en la Tabla 4.2. Por cada artículo se ha extraído el puntaje de calidad obtenido basado en la Tabla 4.1, el año de publicación, el tipo de publicación, la solución o técnica para un correcto control de acceso o gestión de consentimiento y las palabras clave de cada artículo, adicionalmente en la primera columna de la Tabla 4.2, se referencia al artículo con un identificador único que es su cita bibliográfica.

Tabla 4.2: Artículos seleccionados para la revisión

Ref.	Calidad	Año	Tipo	Solucion	Palabras Clave
[18]	5	2017	Artículo de investigación	Listas de control de acceso de Unix	almacenamiento de datos, datos de investigación, gestión de acceso, deposito de datos.
[19]	5	2016	Paper Corto	Control de acceso basada en atributos	Almacenamiento en la nube, control de acceso, CP-ABE, delegado.
[20]	5	2019	Paper de conferencia	Control de acceso basada en atributos	control de acceso, control de acceso centrado en el usuario; blockchain, Internet de las cosas; atributos; contrato inteligente, control de acceso basado en atributos, abac, IoT.
[21]	4	2017	Paper de conferencia	Control de acceso basado en datos biométricos como lo son el escáner de iris y huellas dactilares	Computación móvil en la nube, técnica biométrica, autenticación de huellas dactilares, escáner de iris, códigos de seguridad.
[22]	3.5	2017	Artículo de revista	Control de acceso basado en datos biométricos como lo es el reconocimiento de voz	Reconocimiento de voz, biometría, sistemas integrados, control de acceso.
[23]	5.5	2018	Paper de conferencia	Control de acceso de próxima generación	N/A
[24]	5	2018	Artículo de investigación	Control de acceso basado en capacidad	Internet de los objetos; cuestiones éticas y de privacidad; IoT; autorización; control de acceso; marco.
[25]	6	2020	Artículo de investigación	Control de aceso basado en sensabilidad	Teléfono inteligente, control de acceso centrado en los roles, ingeniería social, amenaza persistente avanzada (APT), sensor, consciente del contexto.

Ref.	Calidad	Año	Tipo	Solucion	Palabras Clave
[26]	5.5	2012	Artículo de revista	Control de aceso basado en conjuntos de atributos jerárquico	Control de acceso, computación en nube, seguridad de los datos.
[27]	5	2013	Paper Corto	Control de aceso basado en criptografía	Control de acceso; sistemas de control de versiones; subversión; cifrado convergente; confidencialidad; almacenamiento eficaz.
[28]	6	2019	Artículo de investigación	Control de aceso basado en riesgos	Riesgo de seguridad, Estimación del riesgo, Internet de las cosas, Modelo de control de acceso basado en el riesgo, Sistema de lógica difusa.
[29]	3	2013	Artículo de investigación	Consentimiento electrónico	Consentimiento informado, Dispositivos móviles, Sistemas de consentimiento electrónico, iPad, Personal de registro, Recogida de datos, Informática.
[30]	5	2019	Artículo de investigación	Consentimeinto autenticado	Internet de las cosas (IoT); consentimiento; consentimiento autenticado; consentimiento que preserva la privacidad; privacidad; seguridad; Reglamento General de Protección de Datos (GDPR); HIBS; AVISPA.

También se realizó una tabla resumen con el puntaje de calidad obtenido por cada artículo, la Tabla 4.3 muestra el puntaje obtenido por cada pregunta de cada artículo.

Tabla 4.3: Puntaje de la evaluación de calidad por cada pregunta de los artículos analizados .

Ref.	P1	P2	P3	P4	P5	P6	Total
[18]	1	1	0	1	1	1	5
[19]	1	1	1	1	1	0	5
[20]	1	1	1	1	1	0	5
[21]	1	1	0	1	1	0	4
[22]	0.5	1	0	1	1	0	3.5
[23]	1	1	0.5	1	1	1	5.5
[24]	1	1	0	1	1	1	5
[25]	1	1	1	1	1	1	6
[26]	0.5	1	1	1	1	1	5.5
[27]	1	1	1	1	1	0	5
[28]	1	1	1	1	1	1	6
[29]	1	0	0	1	1	0	3
[30]	1	1	1	1	1	0	5

En la Figura 4.2 se agrupó la calidad obtenida por cada uno de los artículos. Se puede observar que existe un artículo con calificación de calidad de 3, un artículo con calificación de calidad de 3.5, un artículo con calificación de calidad de 4, cero artículos con calificación de calidad 4.5, seis artículos con calificación de calidad 5, dos artículos con calificación de calidad 5.5 y dos artículos con calificación de calidad de 6.

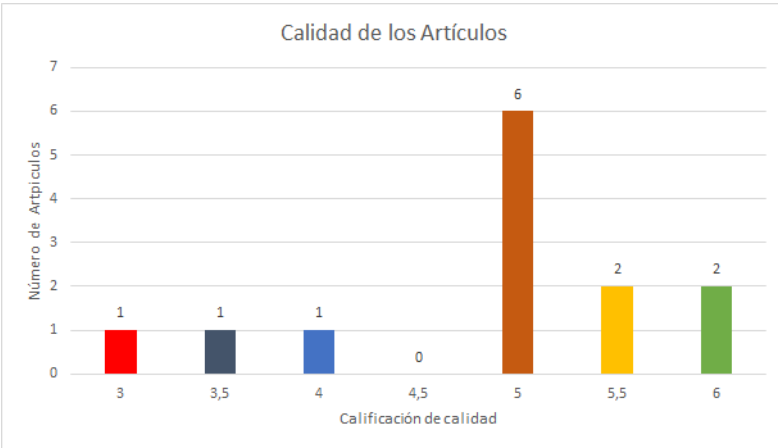


Figura 4.2: Calificación de calidad de los artículos seleccionados Fuente: Elaborada por el autor

Adicionalmente, se decidió clasificar las técnicas o soluciones para el control de acceso y gestión de consentimiento. Se procedió primero a clasificar las técnicas de control de

acceso. En la Tabla 4.2, se puede observar las técnicas encontradas, a continuación se brinda una pequeña descripción de cada una de ellas, que se obtuvo de la lectura de los artículos:

- **Listas de control de acceso de Unix**

  Las listas de control de acceso de Unix, fueron diseñadas para otorgar y denegar permisos de lectura y escritura a un usuario o grupo de usuarios.

- **Cifrado basado en atributos de política de texto cifrado (CP-ABE)**

  Implementa el control de acceso basado en atributos. Este control de acceso define permisos basándose en ciertos atributos que posea el solicitante. Además cifra los archivos del usuario, la clave del cifrado contiene atributos del usuario. La clave para otros usuarios autorizados se genera a partir de sus atributos.

- **Control de acceso basada en atributos y blockchain**

  Implementa el control de acceso basado en atributos, este control de acceso define permisos basándose en ciertos atributos que posea el solicitante. De acuerdo con S. Drame-Maigne, M. Laurent y L. Castillo en [20], blockchain se utiliza en el Servicio de atributos, que está compuesto por todas las transacciones para colocar o revocar atributos.

- **Acceso basado en datos biométricos**

  Se realiza una autenticación con respecto a datos biométricos del usuario, los datos biométricos se refieren a datos que son únicos por cada usuario, como puede ser las huellas dactilares, escaneo de iris e incluso la voz.

- **Control de acceso de próxima generación (NGAC)**

  De acuerdo con K. K. Kolluru en [23], NGAC expresa las políticas a través de atributos. Estos atributos caracterizan a los usuarios y objetos de una solicitud de acceso. NGAC concede o deniega el acceso basándose en las relaciones definidas entre los atributos en las políticas.

- **Control de acceso basado en capacidad (CapBAC)**

  La acuerdo con la definición de S. Nakamura, T. Enokido y M. Takizawa en [31], el propietario de cada dispositivo emite un token de capacidad, es decir, un conjunto de derechos de acceso, a un sujeto. Solo un sujeto que tenga la ficha de capacidad puede manipular el dispositivo.

- **Control de acceso basado en sensibilidad (Sensative)**

De acuerdo con Z. Zulkefli y M. M. Singh en [25] , combina los permisos basándose en roles y atributos y la seguridad multinivel de esta forma mantiene la integridad y la confidencialidad de la información que puede ser infringida.

- **Cifrado basado en conjuntos de atributos jerárquicos**
  Control de acceso basado en el cifrado de un conjunto de atributos del usuario, similar a CP-ABE, pero adicionalmente los usuarios están estructurados de forma jerárquica.
- **Control de acceso basado en criptografía**
  Este control de acceso de acuerdo con D. Leibenger y C. Sorge en [27], se basa en un protocolo criptográfico, que establece llaves entre las partes, utilizando un canal de comunicación seguro en una arquitectura centralizada.

Por otro lado, las soluciones de gestión de consentimiento de acuerdo con la Tabla 4.2, se presentan a continuación con una breve descripción obtenida de los mismos artículos:

- **Consentimiento electrónico**
  Se basa en tener interfaces amigables para el usuario con herramientas de usabilidad para que cualquier usuario pueda leer detenidamente el contrato que debe firmar para entregar su consentimiento.
- **Consentimiento autenticado**
  Esta gestión de consentimiento se basa en comprobar que el usuario es realmente quien dice ser, es él mismo quien autoriza y acepta entregar su consentimiento.

Con esta información se decidió clasificar las soluciones de control de acceso encontradas. La clasificación incluye las siguientes soluciones: lista de control de acceso, control de acceso basado en atributos, control de acceso basado en datos biométricos, control de acceso de próxima generación, control de acceso basado en capacidad, control de acceso basado en sensibilidad, control de acceso basado en criptografía y control de acceso basado en riesgos. La Tabla 4.4 representa la clasificación de cada uno de los artículos. La primera columna es el identificador del artículo que es su cita bibliografía, la segunda columna es la solución encontrada con respecto al control de acceso y la tercera columna representa su clasificación con respecto a la misma solución.

Tabla 4.4: Clasificación de las soluciones de control de acceso

Ref.	Solución	Clasificación
[18]	Listas de control de acceso de Unix	Listas de control de acceso
[19]	Cifrado basado en atributos de política de texto cifrado (CP-ABE)	Control de acceso basado en atributos
[20]	Control de acceso basada en atributos y blockchain	Control de acceso basado en atributos
[21]	Control de acceso basado en datos biométricos (escaneo de iris y escaneo de huellas dactilares)	Control de acceso basado en datos biométricos
[22]	Control de acceso basado en datos biométricos (Gestión de acceso basado en la voz del usuario)	Control de acceso basado en datos biométricos
[23]	Control de acceso de proxima generación (NGAC)	Control de acceso de proxima generación
[24]	Control de acceso basado en capacidad (CapBAC)	Control de acceso basado en capacidad
[25]	Control de acceso basado en sensibilidad (Sensative)	Control de acceso basado en sensibilidad
[26]	Cifrado basado en conjuntos de atributos jerárquicos (HASBE)	Control de acceso basado en atributos
[27]	Control de acceso basado en criptografía	Control de acceso basado en criptografía
[28]	Control de acceso basado en riesgos	Control de acceso basado en riesgos

La Figura 4.3 representa cuales fueron las soluciones más comunes. Se puede observar que la solución más frecuente es un control de acceso basado en atributos. Tres artículos se basaron en esta solución. Dos artículos se basaron en un control de acceso basado en datos biométricos. Las soluciones lista de control de acceso, control de acceso de próxima generación, control de acceso basado en capacidad, control de acceso basado en criptografía, control de acceso basado en riesgos y control de acceso basado en sensibilidad se encontraron únicamente en un artículo, es decir un artículo diferente por cada solución.

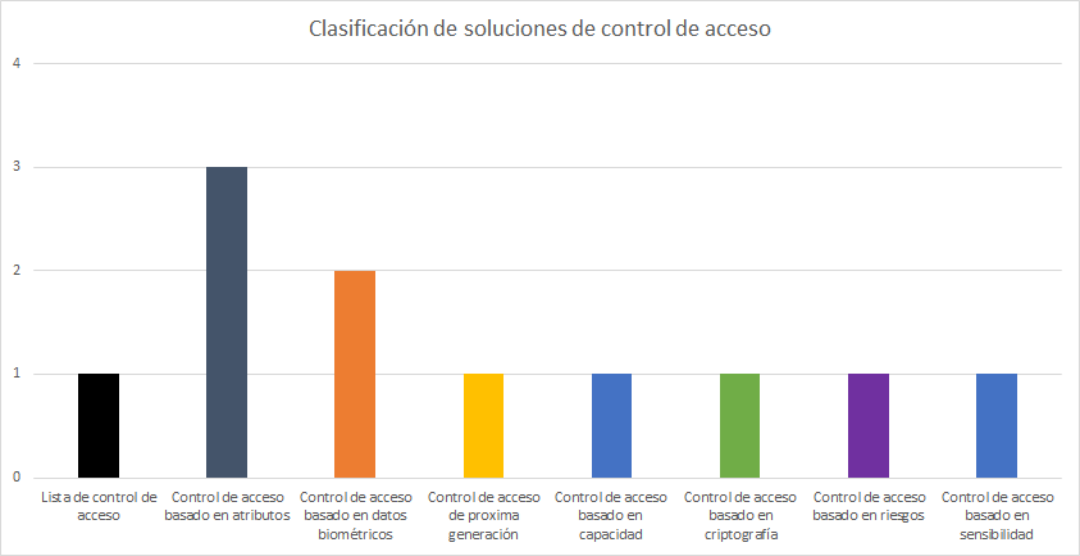


Figura 4.3: Soluciones encontradas en los artículos Fuente: Elaborada por el autor

Dado que se cuenta únicamente con dos soluciones para una correcta gestión de consentimiento se decidió no clasificarlas.

4.7.1 Discusión de las preguntas de investigación

En esta sección se presentan las respuestas a las preguntas de investigación descritas en la parte inicial de la revisión sistemática de la literatura.

RQ1 ¿Cuáles son las soluciones para poder realizar una correcta gestión del consentimiento de datos personales?

La gestión del consentimiento y el control de acceso están relacionados. Por ejemplo, si se realiza un buen control de acceso se realizará a la vez una buena gestión del consentimiento. Si un usuario desea limitar algunos de sus datos personas a una empresa, primero se tiene que cambiar las reglas del control de acceso para que esta empresa ya no tengo acceso a los datos personales que el usuario decidió limitar, al garantizar este cambio de regla también se garantiza una correcta gestión de consentimiento. Entre las soluciones encontradas en los artículos se encuentra realizar un consentimiento electrónico a través de interfaces amigables para el usuario, de tal forma que estos puedan leer las políticas y condiciones de un acuerdo, y así estos poder aceptar o rechazar el acuerdo. Otra solución involucra la autenticidad del usuario para garantizar que el propio usuario, esté entregando su consentimiento.

Hay que mencionar que con las soluciones de control de acceso encontradas también se puede realizar una correcta gestión de consentimiento.

RQ2 ¿Cuáles son las soluciones para poder realizar una correcta gestión del acceso a los datos personales?

El 100 % de los artículos relacionados a soluciones de control de acceso, se basan en controles de acceso ya existentes, en algunos casos modificados y en otros casos permanecían tal cual lo dice su definición, los controles de acceso encontrados en los artículos como se puede ver en la Tabla 4.2 son: listas de control de acceso de Unix, control de acceso basado en atributos, control de acceso basado en datos biométricos, control de acceso de próxima generación, control de acceso basada en sensibilidad, control de acceso basada en criptografía y control de acceso basado en riesgos.

4.7.2 Conclusiones

Gracias a la revisión sistemática de la literatura, se pudo identificar las técnicas y soluciones sobre el control de acceso y la gestión de consentimiento. A partir de esto se encontró que la solución más efectiva para un correcto control de acceso de datos personales es aplicar un control de acceso. Dependiendo del contexto de seguridad el control de acceso puede ser diferente como el control de acceso basado en sensibilidad, riesgo, atributos, etc. En este caso la solución más usada fue un control de acceso basado en atributos ya que es ideal para proteger datos personales. Por otro lado, para la gestión de consentimiento se encontró que realizar una interfaz amigable para el usuario es sumamente importante para que este mismo pueda dar su consentimiento. Otra técnica más sofisticada es aplicar una autenticación del usuario que valida que el usuario este autenticado y entrega su consentimiento. Finalmente, la mayoría de los artículos posee una buena calidad de acuerdo con nuestra evaluación.

5 IDENTIFICACIÓN DE CONTROLES DE LOS ESTÁNDARES INTERNACIONALES

Para esta sección se ha revisado dos estándares internacionales en el ámbito de la seguridad informática estos son la NIST sp 800-53 y la ISO 27001, ambos estándares contienen varios controles de seguridad informática diversificados en varios temas, en esta sección nos concentraremos únicamente en control de acceso y gestión de consentimiento.

5.1 CONTROLES DE LA ISO 27001 QUE SE RELACIONAN CON EL CONTROL DE ACCESO

A continuación se presentan los controles de la ISO 27001 relacionados con el control de acceso, la Tabla 5.1 presente en su primera columna un código que representa el grupo y subgrupo a la que pertenece el control, la segunda columna denominada control es el nombre del control como tal. Finalmente la tercera columna contiene una pequeña descripción. Adicionalemnte, la Tabla completa se enecuentra en el Anexo 1. El Anexo 1 es una hoja de Excel, los controles relacionados con el control de acceso se encuentran en la hoja ”Control de Acceso” del documento Excel. En la Tabla 5.1 únicamente se presentan 5 controles.

Tabla 5.1: Controles relacionados con el control de acceso de acuerdo al estándar ISO 27001

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.
A.12.4.2	Protección de la información de registro	La información de registro debe estar protegidas contra el acceso no permitido.
A.13.2.2	Acuerdos de transferencia de información	Los Acuerdos deberán ser transmetidos de manera segura y en todas las partes externas.
A.14.2.7	Desarrollo subcontratado	La empresa deberá supervisar sistemas subcontrados que fueron desarollados por terceros.
A.15.1.1	Política de seguridad de la información en las relaciones con proveedores	Los requisitos de seguridad de la información deben acordarse con el proovedor, además de esto deben estár documentados.
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.

5.2 CONTROLES DE LA ISO 27001 QUE SE RELACIONAN CON LA GESTIÓN DE CONSENTIMEINTO

A continuación se presentan los controles presentados en la ISO 27001 relacionados con la gestión de consentimiento. La Tabla 5.2 presenta en su primera columna un código que representa el grupo y subgrupo a la que pertenece el control, la segunda columna denominada control, es el nombre del control como tal finalmente la tercera columna contiene una pequeña descripción. En el Anexo 1 se encuentra la Tabla completa. El Anexo 1 es una hoja de Excel, los controles relacionados con la gestión de consentimiento se encuentran en la hoja ”Gestión de Consentimiento ” del documento Excel. La Tabla 5.2 contiene únicamente 5 controles.

Tabla 5.2: Controles relacionados con la gestión de consentimiento de acuerdo al estándar ISO 27001

Código	Control	Descripción
A.9.4.1	Restricción de acceso a la información	El acceso a los sistemas de información estará restringido de acuerdo a una 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.
A.13.2.4	Acuerdos de confidencialidad o no divulgación	Los requisitos de confidencialidad deben revisarse periódicamente y documentarse.
A.15.2.1	Seguimiento y revisión de servicios de proveedores	Los Organismos deberán monitorear, revisar y auditar periódicamente el servicio de los proveedores.
A.18.1.4	Privacidad y protección de la información de identificación personal.	La privacidad y la protección de la información deberá ser tratada tal cual los reglamentos de la legislación lo exijan.

5.3 CONTROLES DE LA NIST SP 800-53 QUE SE RELACIONAN CON EL CONTROL DE ACCESO

El estándar NIST sp 800-53, contiene controles más variados y extensos que la ISO 27001, por esta razón en la Tabla 5.3 se colocan únicamente los 5 primeros controles relacionados con el control de acceso. La tabla completa se encuentra en el Anexo 2 respectivamente. El Anexo 2 es un documento Excel, en la hoja ”Control de Acceso” de documento Excel se encuentra todos los controles relacionados con el control de acceso.

La Tabla 5.3 en su primera columna contiene el código del control, la segunda columna es el control como tal, la tercera columna es el literal que se relaciona con el control de acceso y finalmente la última columna contiene su descripción.

Tabla 5.3: Controles relacionados con el control de acceso de acuerdo al estándar NIST sp 800-53

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	b	Designar un funcionario definido por la organización para gestionar el desarrollo, la documentación y la difusión de la política y los procedimientos de control de acceso
AC-1	POLÍTICA Y PROCEDIMIENTOS	c	Revise y actualice el control de acceso actual: 1. Política 2. Procedimientos

Código	Control	Literal	Descripción
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	c	Requerir requisitos previos y criterios definidos por la organización para la asignación a grupos y roles

5.4 CONTROLES DE LA NIST SP 800-53 QUE SE RELACIONAN CON LA GESTIÓN DE CONSENTIMIENTO

Como se mencionó anteriormente el estándar NIST sp 800-53 contiene controles más extensos que la ISO 27001, la Tabla 5.4 contiene los primeros 5 controles relacionados con la gestión de consentimiento. En su primera columna se encuentra el código del control, la segunda columna es el control como tal, la tercera columna es el literal que se relaciona con un control concorde a la gestión de consentimiento y finalmente la última columna contiene su descripción. La Tabla completa se encuentra en el Anexo 2. El anexo 2 es una hoja de Excel, los controles relacionados con la gestión de consentimiento se encuentran en la hoja ”Gestión de Consentimiento” del documento Excel.

Tabla 5.4: Controles relacionados con la gestión de consentimiento de acuerdo al estándar NIST sp 800-53

Código	Control	Literal	Descripción
PT-2	AUTORIDAD PARA PROCESAR INFORMACIÓN PERSONAL IDENTIFICABLE	a	Determinar y documentar la [Asignación: autoridad definida por la organización] que permite el [Asignación: tratamiento definido por la organización] de información personal identificable
PT-2	AUTORIDAD PARA PROCESAR INFORMACIÓN PERSONAL IDENTIFICABLE	b	Restringir el [Asignación: tratamiento definido por la organización] de la información personal identificable a la información autorizada.

Código	Control	Literal	Descripción
PT-3	FINES DE TRATAMIENTO DE INFORMACIÓN PERSONAL IDENTIFICABLE	a	Identificar y documentar los [Asignación: propósito(s) definido(s) por la organización] para el tratamiento de información de identificación personal]
PT-3	FINES DE TRATAMIENTO DE INFORMACIÓN PERSONAL IDENTIFICABLE	b	Describa la(s) finalidad(es) en los avisos y políticas públicas de privacidad de la organización
PT-3	FINES DE TRATAMIENTO DE INFORMACIÓN PERSONAL IDENTIFICABLE	c	Restringir el [Asignación: tratamiento definido por la organización] de la información personalmente identificable sólo a lo que sea compatible con los fines identificados]

6 DISEÑO Y DESAROLLO DE LA APLICACIÓN

Como se había propuesto, para el diseño y el desarrollo se hizo uso del marco SCRUM. Debido a que en el equipo solo estuvimos presentes tres personas, los papeles de Scrum Master y Desarrolladores fueron compartidos por ambos integrantes y nuestra tutora tomó 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 3 sprints, de 3 semanas cada uno. Este cápitulo al igual que el siguiente fue realizado de manera grupal, es decir con el compañero del trabajo de integración curricular. Los requerimientos tanto suyos como los míos fueron tomados en conjunto para desarrollar una sola aplicación. Se tomó en cuenta tanto el lado del usuario (titular de los datos) como el del 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.

- ❒ 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 termina 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 tratamientos 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 los 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 él 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 está usando sus datos tal cual lo declaró 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 LODPD, 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 ha 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 presenta las colecciones creadas para la base de datos.

Se usó la base de datos no relacional MongoDB. Hay que recordar que en MongoDB el atributo _id de cada colección es creado automáticamente por MongoDB, este es un identificador único de cada colección y es el que se usará para crear relaciones entre colecciones. En MongoDB los tipos de datos que comienzan y terminan con [], son arreglos, puede ser de Strings, Numbers, etc. Los atributos que comienzan y terminan con {} son objetos dentro de estos, pueden haber más de un tipo de datos como por ejemplo Strings o Numbers. Si el tipo de datos comienza y termina con [{}] significa que es un arreglo de objetos. En total se crearon seis colecciones que son: Usuario, Empresa, Trastamiento, Email, Consentimeinto y Blockchain.
La colección Usuario contiene los siguientes atributos.

- Usuario
  - _id: Object Id
  - Nombre: String
  - Apellido: String
  - Email: String
  - Ci: String
  - Contraseña: String

La Figura 6.1 presenta el diagrama de la colección Usuario descrita, la Figura presenta los atributos de la colección y el tipo de dato de cada atributo.

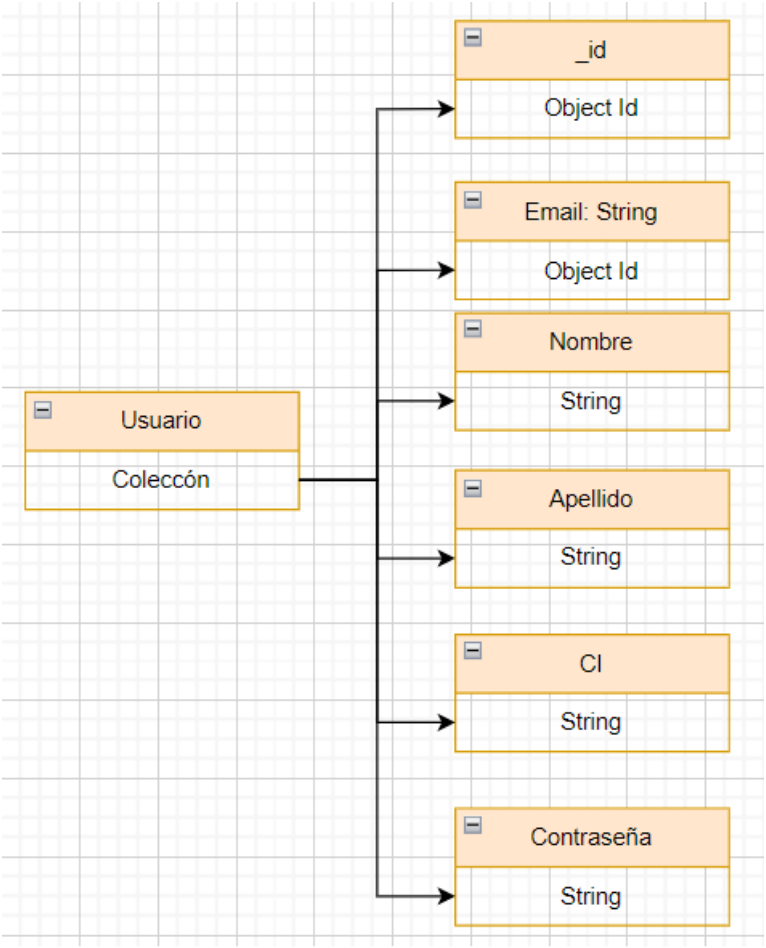


Figura 6.1: Colección Usuario Fuente: Elaborada por el autor

La colección Empresa contiene los siguientes atributos.

- Empresa
  - _id: Object Id
  - Nombre: String
  - Email: String
  - Ruc: String
  - Contraseña: String

La Figura 6.2 presenta el diagrama de la colección Empresa.

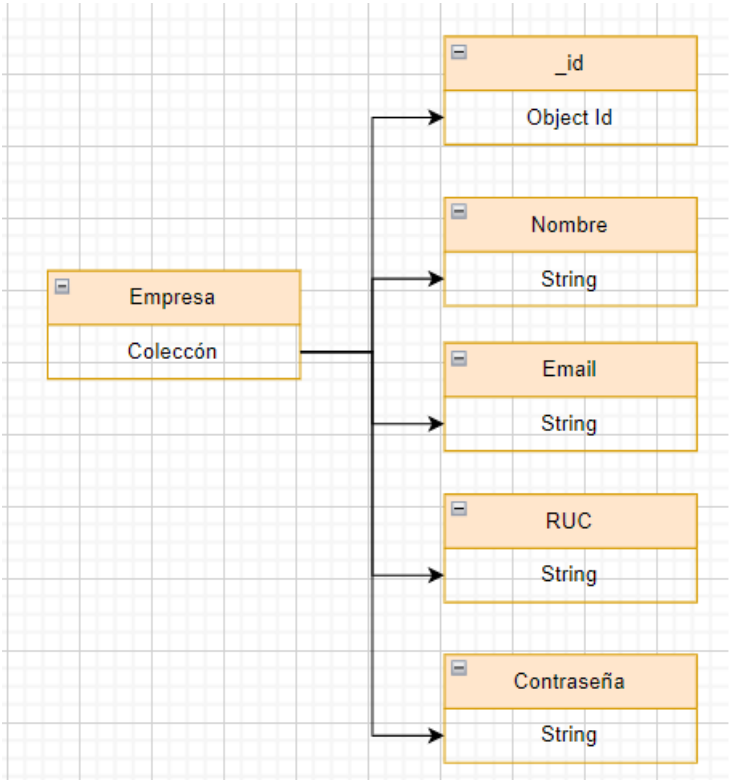


Figura 6.2: Colección Empresa Fuente: Elaborada por el autor

La colección Tratamiento contiene los siguientes atributos.

- ❒ _id: Object Id
- ❒ Nombre: String
- ❒ Data:[{
  - ✧ Tipo:String
  - ✧ Valor: String }]
- ❒ Descripcion: String
- ❒ idEmpresa: Object Id de Empresa

La Figura 6.3 presenta el diagrama de la colección Tratamiento.

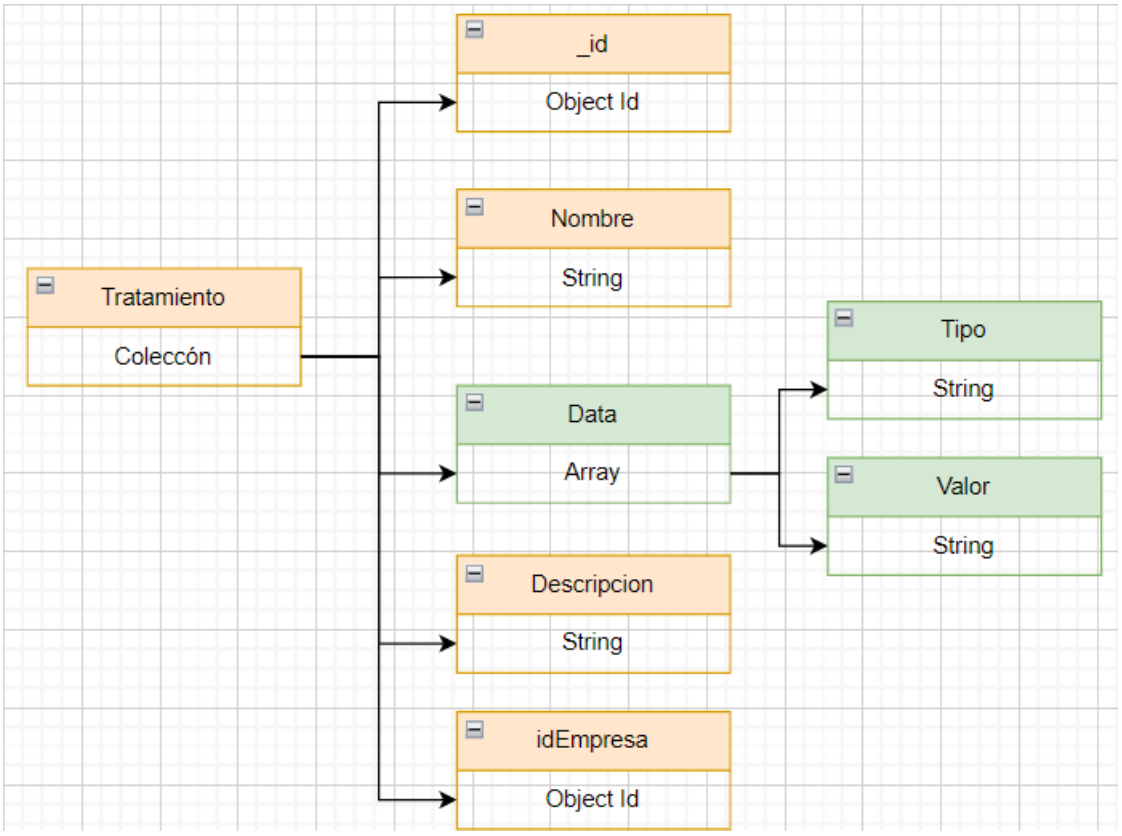


Figura 6.3: Colección Tratamiento Fuente: Elaborada por el autor

La colección Email contiene los siguientes atributos.

- ❒ _id: Object Id
- ❒ Empresa:{
  - ✧ _id: Object Id de Empresa
  - ✧ _id: Nombre:String}
- ❒ Usuario:{
  - ✧ _id: Object Id de Usuario
  - ✧ _id: Nombre:String }
- ❒ DescripcionConsentimiento: String
- ❒ Data:[{
  - ✧ Tipo:String
  - ✧ Valor: String }]

- Permisos:[{
  - Tipo: String
  - Valor: Boolean
  - Descripcion: String
  - Data: [String] }]
- FechaFin:Date
- Observaciones: String
- Respondido:Boolean
- FechaEnvio:Date

La Figura 6.4 presenta el diagrama de la colección Email.

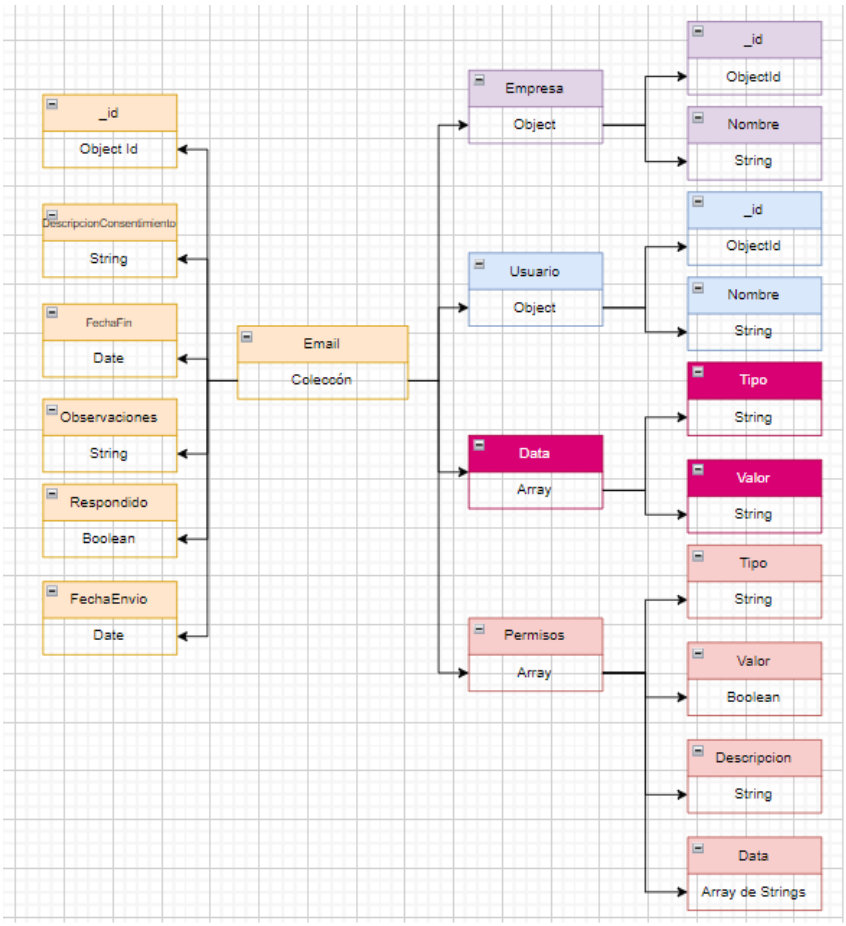


Figura 6.4: Colección Email Fuente: Elaborada por el autor

La colección Consentimiento contiene los siguientes atributos.

- _id: Object Id
- Empresa:{
  - _id: Object Id de Empresa
  - _id: Nombre:String}
- Usuario:{
  - _id: Object Id de Usuario
  - _id: Nombre:String }
- DescripcionConsentimiento: String
- Data:[{
  - Tipo:String
  - Valor: String }]
- Permisos:[{
  - Tipo: String
  - Valor: Boolean
  - Descripcion: String
  - Data: [String] }]
- FechaFin:Date
- FechaCreacion:Date

La Figura 6.5 presenta el diagrama de la colección Consentimiento.

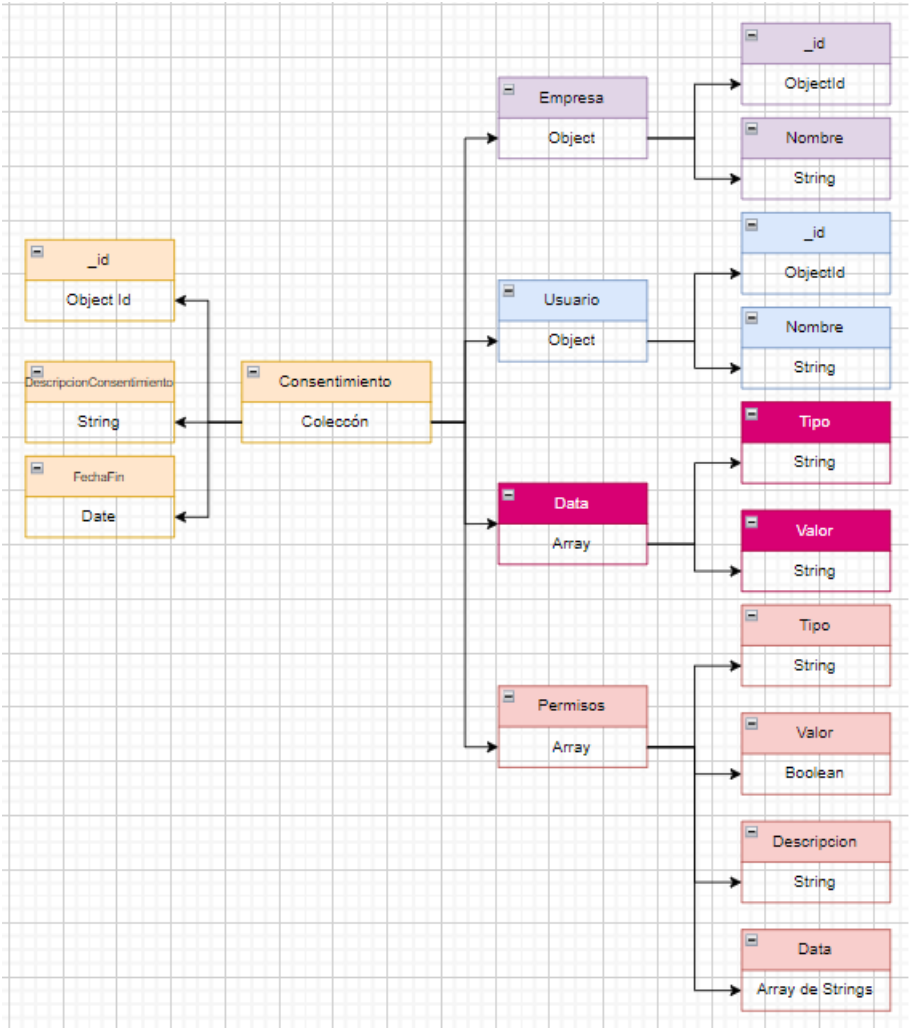


Figura 6.5: Colección Consentimeinto Fuente: Elaborada por el autor

La colección Blockchain contiene los siguientes atributos.

- ❒ _id: Object Id
- ❒ HashMain: String
- ❒ HashEnterprise: String
- ❒ PreviousHashMain: String
- ❒ PreviousHashEnterprise: String
- ❒ Heigh: Number
- ❒ HeighEnterprise: Number
- ❒ Body: String
- ❒ Body_Enterprise: String

- Data:[{
  - Tipo:String
  - Valor: String }]
- Permisos:[{
  - Tipo: String
  - Valor: Boolean
  - Descripcion: String
  - Data: [String] }]
- idUsuario:ObecjId de Usuario
- idEmpresa:ObecjId de Empresa
- FechaFin:Date
- FechaCreacion:Date

La Figura 6.6 presenta el diagrama de la colección Blockchain.

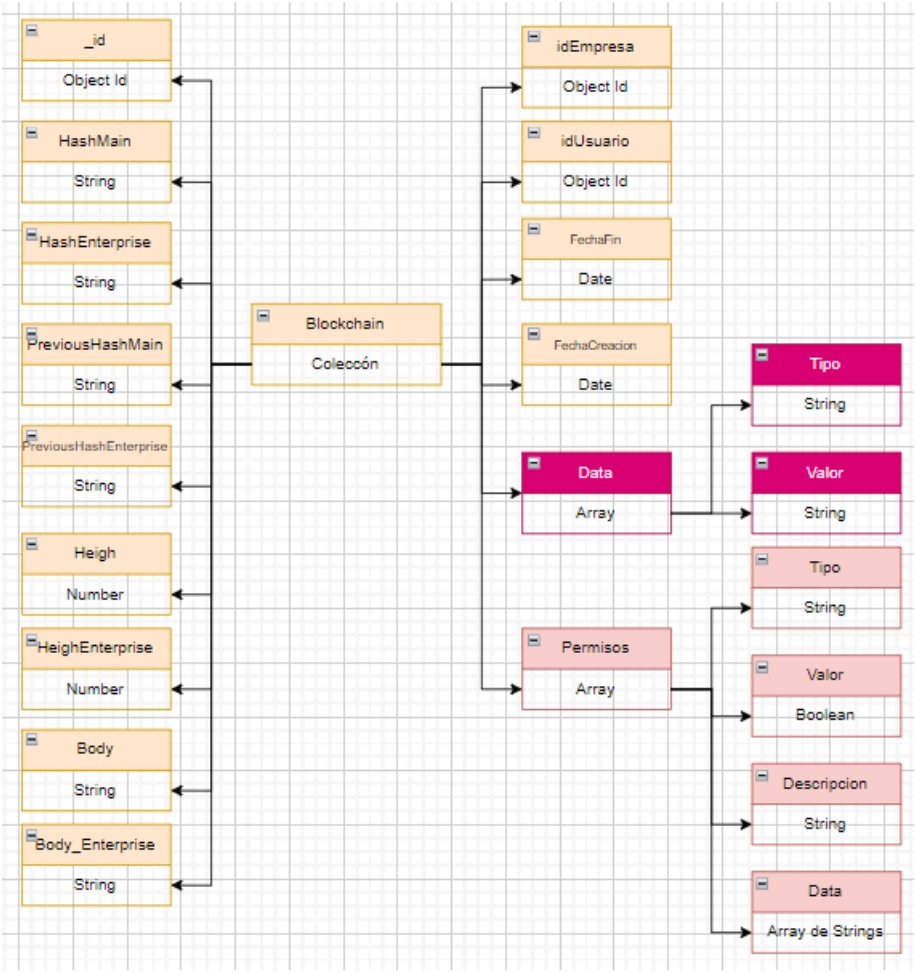


Figura 6.6: Colección Blockchain Fuente: Elaborada por el autor

6.2 DESARROLLO

Para el desarrollo se identificó que necesitaríamos de tres elementos principales, el frontend, el backend y la base de datos. Para el frontend se decidió hacer uso 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. Y 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 cualquier otro tipo de 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.

En la fase de diseño se realizó un listado de las tareas que se deben realizar para cumplir con la LODPD. 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 gestión de consentimiento y el control de acceso por parte del responsable de tratamiento. Es importante mencionar que debido a la interacción de dos usuarios, (titular y responsable del tratamiento de los datos) y otros requerimientos (gestión de consentimiento de los datos y control de acceso por parte del titular de los datos), la aplicación tiene más funcionalidades las cuales complementan el funcionamiento de toda la aplicación.

La base de la aplicación para cumplir los requerimientos de consentimiento y control de acceso es el blockchain debido a que de esta forma los datos de los usuarios estarían almacenados de tal forma que siempre se pudiera ver el historial de los datos y que el usuario pueda tener un control sobre los mismos, como saber que empresas están haciendo uso de sus datos, que datos tienen las empresas, poder tener la decisión en cualquier momento de actualizar sus datos o decidir si quieren que una empresa siga tratando mis datos, además con blockchain también garantizamos que la empresa este usando nuestros datos de la manera en la que nosotros lo autorizamos.
Como se sabe también existen múltiples formas de realizar un control de acceso y una correcta autenticación. De las conclusiones de la revisión sistemática de la literatura se obtuvo que hay un control de acceso que trabaja de forma centralizada, de acuerdo con Francis y Tina en [32] al trabajar con autenticación centralizada se tiene una autoridad de confianza que se encarga de manejar el control de acceso.

Si bien se sabe que una de las bases de blockchain es que su arquitectura se basa en ser descentralizada, para el 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 y la solución planteada en *“Privacy Issues and Tech- niques in E-Health Systems’* [32], tendríamos una autenticación centrali-

zada para controlar la gestión de acceso por parte del usuario, también usaremos el control de acceso basado en roles, no usaremos un control de acceso basado en atributos porque en este caso nos concentraremos únicamente en dos roles, estos son el titular de los datos y el responsable del tratamiento, ya que solo tenemos estos dos roles se optó por descartar el control de acceso basado en atributos, usaremos también el blockchain mencionado en *"Distributed access control solution for the IoT based on multi-endorsed attributes and smart contracts"* [20] 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 (titular) para ver que datos están siendo usados por la empresa, y por el lado de las empresas (responsables de tratamiento) para ver los datos del titular que pueden usar. El uso del blockchain nos ayudó en 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 de formato excel, que es el documento mas fácil de entender por una persona sin conocimientos en lenguajes de programación. También se puede exportar en formato csv dado que actualmente es un 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. Al titular se muestra de manera amigable que están haciendo los responsables de tratamiento con sus datos. Al responsable del tratamiento de igual forma se le presentan los datos y consentimientos de los titulares de una forma amigable. Como se menciono anteriormente, se uso el control de acceso basado en roles, los roles aplicados son titular y responsable del tratamiento.
En esta sección se encontrarán los flujos de la aplicación los cuales mostrarán su funcionamiento, también se describe el funcionamiento de nuestro blockchain el cual mediante un ejemplo, se mostrará su flujo. En el Anexo 3 se encuentra un video demostrativo de como funciona el aplicativo web, en el Anexo 4 se encuentra el código del frontend y finalmente en el Anexo 5 se encuentra el código del backend.

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.

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 sus datos principales los cuales se mostrarán en el flujo presentado a continuación, acompañado de una vista gráfica en la Figura 7.1.

1. Llenar formulario de registro.
    - ❒ El titular deberá llenar los siguientes datos:
        - ✧ Nombre.
        - ✧ Apellido.
        - ✧ Cédula.
        - ✧ Email.
        - ✧ Contraseña.
    - ❒ El responsable del tratamiento deberá llenar los siguientes datos:
        - ✧ Nombre.
        - ✧ Email.
        - ✧ 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.

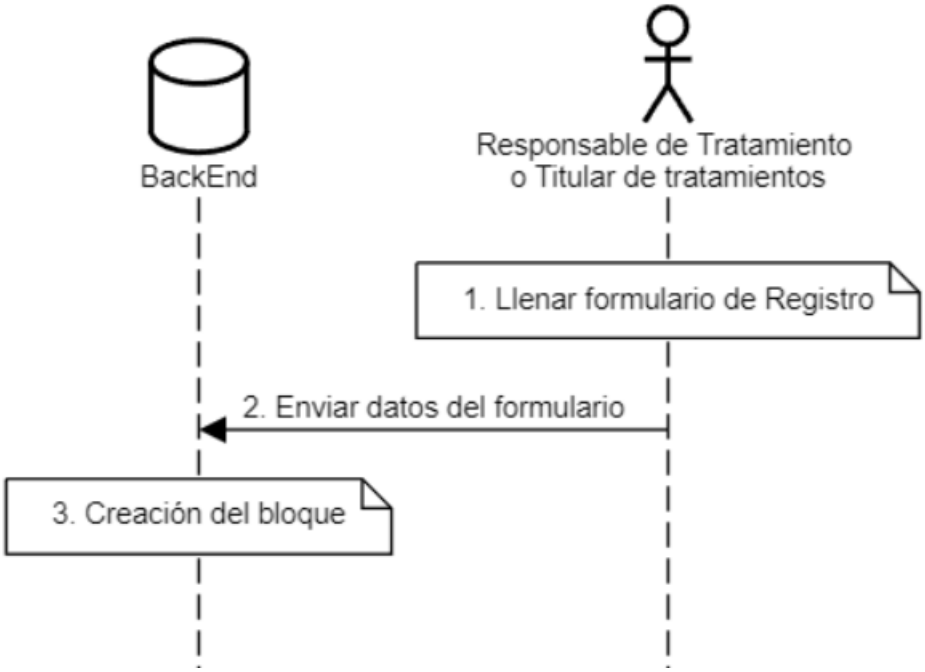


Figura 7.1: Diagrama de flujo de registro

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 gráfica en la Figura 7.2.

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

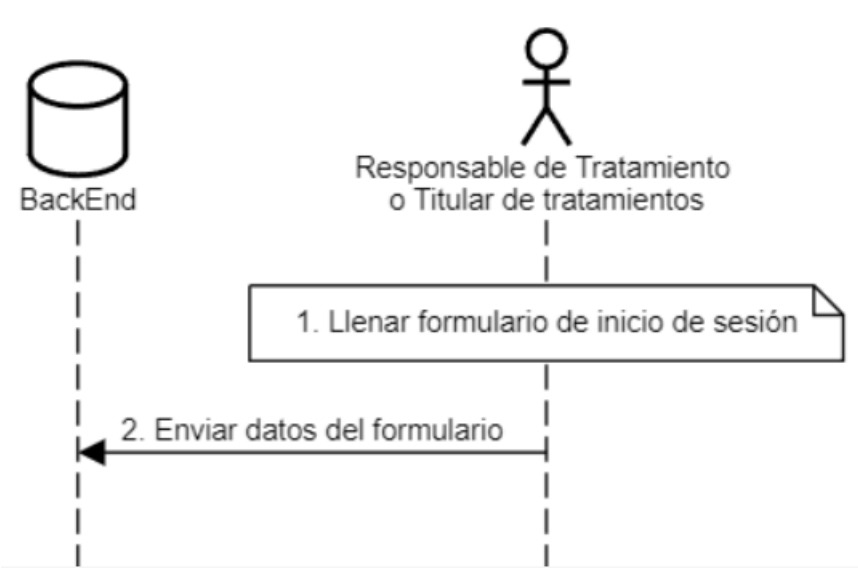


Figura 7.2: Diagrama de inicio de sesión

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 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 titular envía el tratamiento al backend.
3. El tratamiento es almacenado en la base de datos.
4. El titular 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 titular envía la solicitud
7. La solicitud es guardada en la base de datos por parte del backend

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.

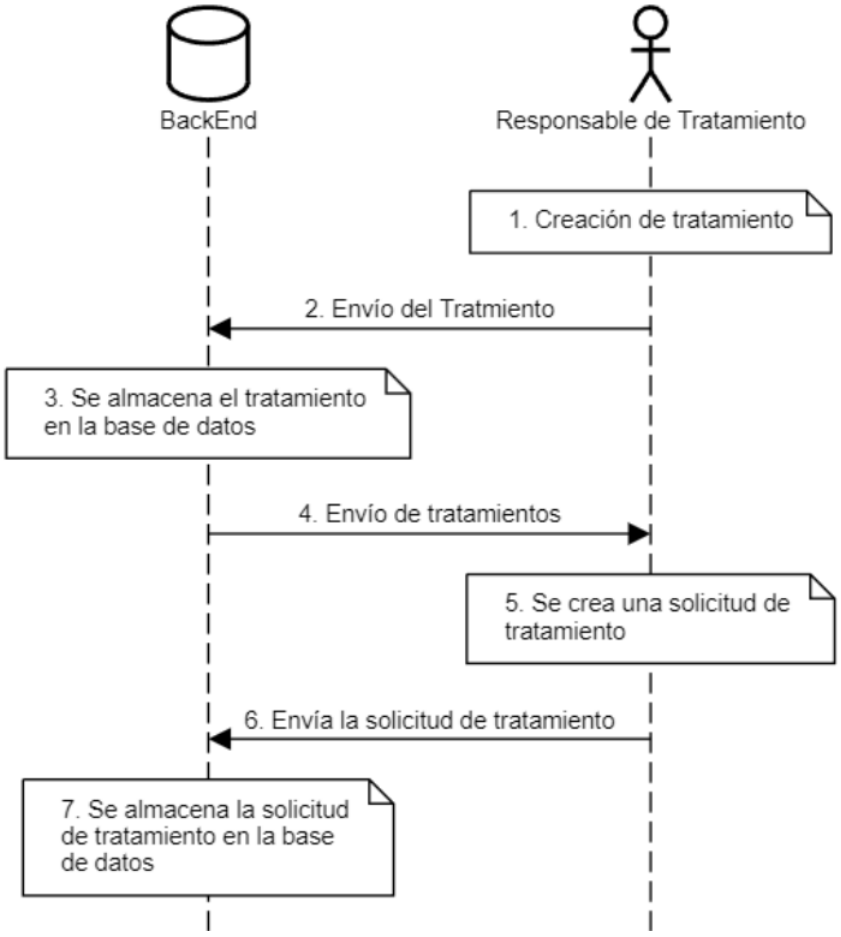


Figura 7.3: Diagrama de creación de solicitud de tratamiento

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 él quien acepte o rechace los tratamientos según su criterio, de igual forma será él quien pueda modificar la fecha fin para el tratamiento de sus datos. A continuación, se muestra el flujo del proceso, acompañado de una vista 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. Se 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 backend 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.

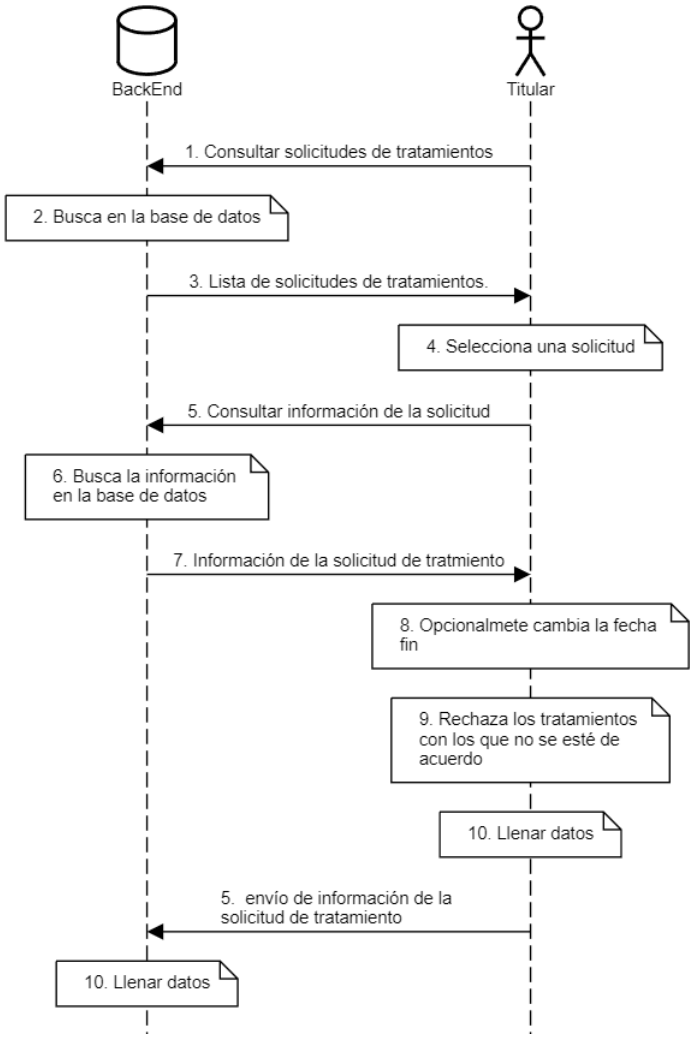


Figura 7.4: Diagrama de aceptación o rechazo para una solicitud de tratamiento

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

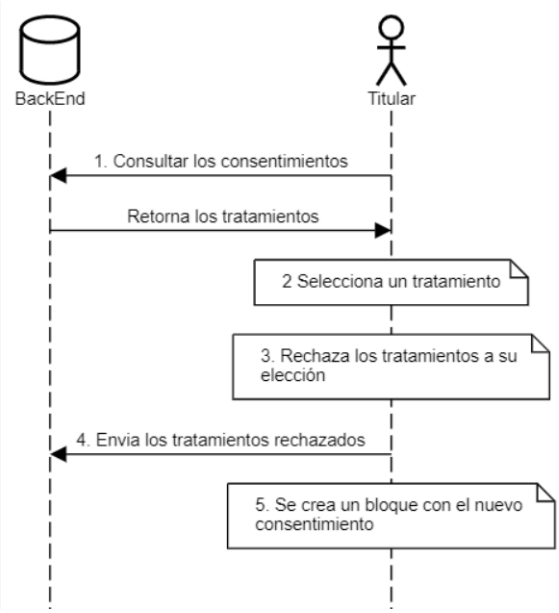


Figura 7.5: Diagrama de rechazo de tratamientos por parte del titular

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 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.

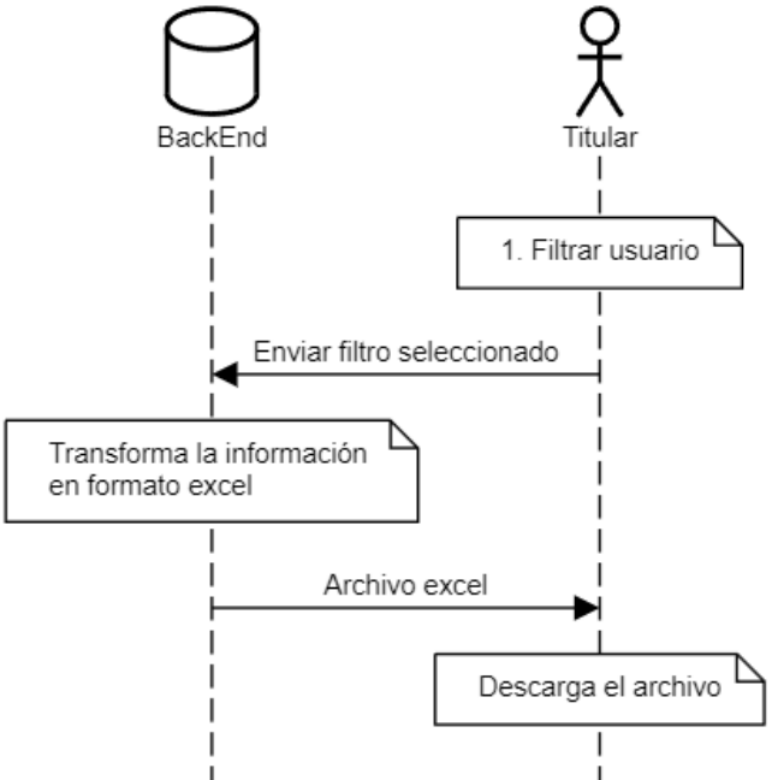


Figura 7.6: Diagrama de exportación de datos por parte del responsable de tratamiento

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 continuación, se muestra el flujo del proceso, acompañado de una vista 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.

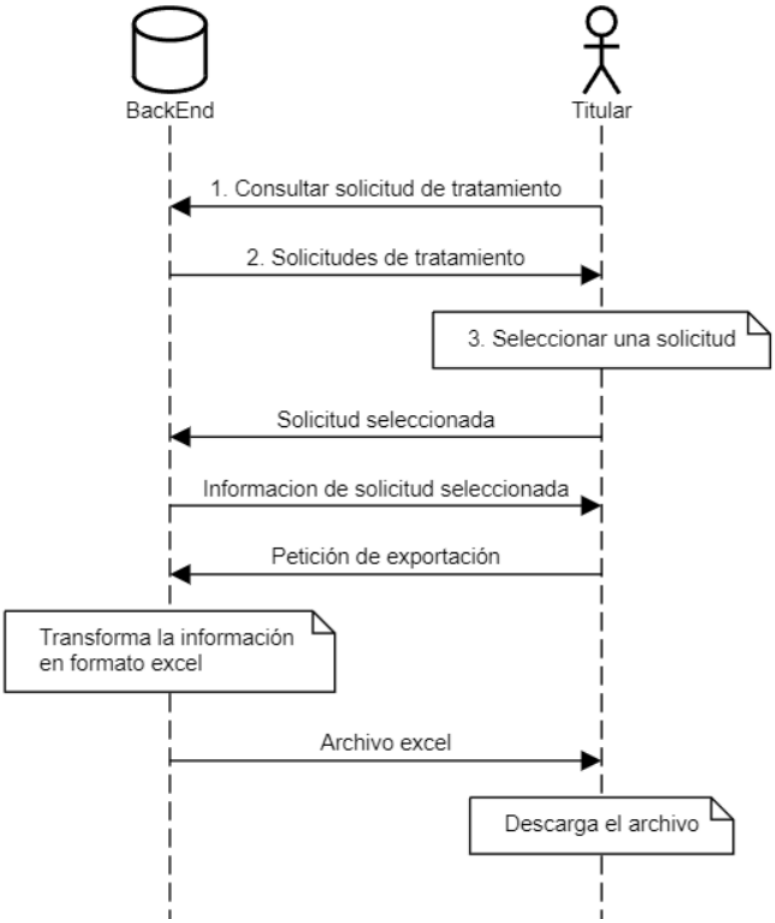


Figura 7.7: Diagrama de exportación de datos por parte del titular

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, acompañado de una vista 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.

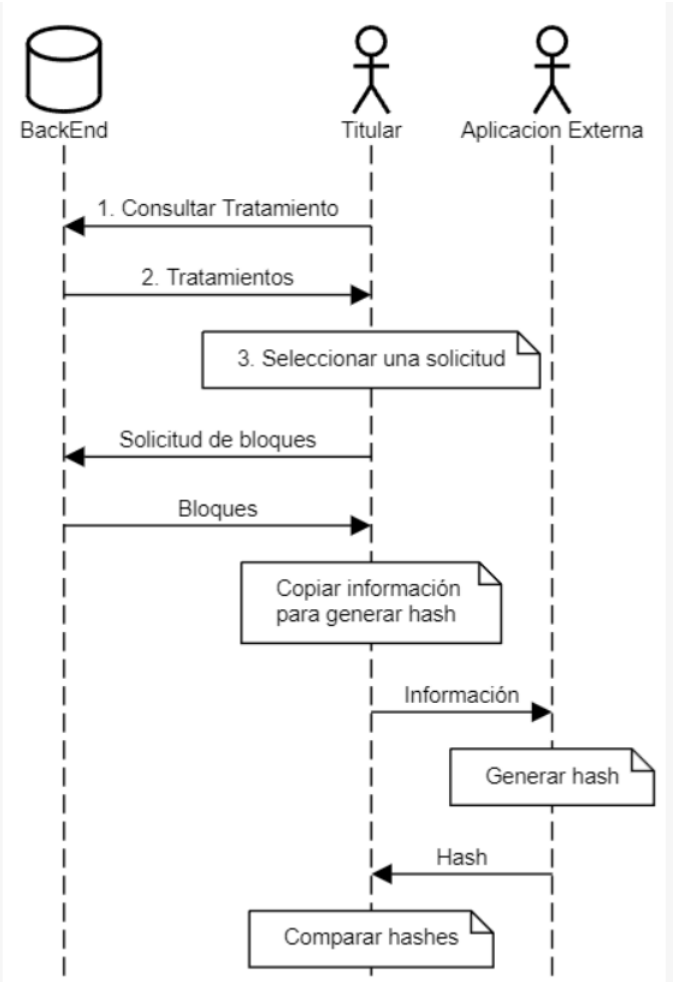


Figura 7.8: Diagrama de inmutabilidad en el historial de los datos y tratamientos

7.1.9 Eliminación automática del los datos del usuario cuando se cumple la fecha limite

A través del backend se implementó la lógica para que cada consentimiento se elimine a las 11 pm en su fecha límite, de esta manera el titular de sus datos no se debe preocupar porque un responsable de tratamiento use su datos después de la fecha limite establecida, en nuestra base de datos la fecha límite del consentimiento es representado por FechaFin. De igual manera el responsable de tratamiento no tiene que realizar ninguna actividad para borrar los datos de un titular, el sistema lo hará automáticamente.

7.2 FUNCIONAMIENTO DEL BLOCKCHAIN

En esta sección se describe brevemente la solución implementada para garantizar que el consentimiento del titular se cumpla. Como se menciono anteriormente MongoDB genera ids únicos por cada nuevo documento en una colección, en estos ejemplos los ids son colocamos con nombres fáciles por temas ilustrativos. Para comenzar debe haber un conjunto de titulares de datos registrados en el sistema, al igual que responsables del tratamiento. Para el ejemplo del funcionamiento del blockchain, asumimos que tenemos los siguientes 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

También asumimos que los siguientes responsables del tratamiento están registrados.

- ❒ **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**: Guayaquil
- ✧ **email**: usuario@guayaquil.com
- ✧ **ruc**: 0589455623
- ✧ **contraseña**: 123456

7.2.1 Creación del primer bloque

Para que se cree el primer bloque primero el usuario debe aceptar un tratamiento de datos, pero antes de eso un responsable del tratamiento debe enviar una solicitud de tratamiento a un titular, el titular debe aceptar los tratamientos sobre sus datos personales que él considere apropiados.
La solicitud de tratamiento es presentada en nuestra base de datos como la colección Email. Asumimos que el responsable del tratamiento 1 creará una solicitud de tratamiento (email), con los permisos de facturación electrónica y marketing. La estructura del email creado se presenta a continuación

❒ **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 él 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. De igual forma el Titular ha llenado los datos necesarios para los tratamientos, los cuales serán almacenados. Hay que recordar que el atributo heigh representa la longitud de la cadena, en este caso como es el primero, heigh es cero. El atributo heighEnterprise representa el tamaño de la cadena, pero para un responsable de tratamiento en específico, en otras palabras, si se añade un bloque y el id del responsable del tratamiento es nuevo, es decir es la primera

vez que el responsable del tratamiento se añade al blockchain, heighEnterprise será cero, heighEnterprise representa las veces que un responsable de tratamiento aparece en la cadena.

HashMain se genera a través de una función hash que contiene todo el bloque, el atributo body presenta todo el bloque y justamente es el contenido con el cual se genera el atributo hashMain, hashEnterprise es el hash del id del responsable del tratamiento concatenado con la hora en la que se creó que el bloque y también concatenado con el atributo body, este atributo es representado por body_enterprise que contiene el contenido con el que se genera el hash de la empresa es decir hashEnterprise.

Para este ejemplo, el hashMain y el hashEnterpise son colocados con nombres fáciles de recordar a manera ilustrativa, el atributo body también está remplazado por una cadena corta dado que su original es el bloque mismo, lo mismo se realiza con body_enterprise.

- ❒ **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

El responsable de tratamiento 2, envía una solicitud de tratamiento al titular 2, este contendrá el consentimiento para facturación electrónica y markenting, al igual que en el caso anterior. La estructura de la solicitud de tratamiento se encuentra a continuación, la cual es idéntica al email anterior, por lo cual en el siguiente ejemplo solo se colocan los cambios más representativos.

❒ **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 bloque 2, el cual es igual al bloque 1, por lo cual aquí únicamente se colocará los atributos más representativos,

en este caso hashMain, hashEnterprise, previousHasMain, previousHashEnterprise, heigh 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 tratamiento 1 “Pichincha” decide enviar una solicitud con el consentimiento de factura electrónica y marketing al titular 2, la estructura de la solicitud se presenta a continuación. Al igual que el ejemplo 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 acepta tanto permiso de facturación electrónica como el de marketing. 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 el 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 del responsable del tratamiento aparece, por otro lado, heigh es 2 dado que es tercer bloque de la cadena.

7.2.4 Creación del cuarto y quinto 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 la data del usuario ha cambiado, por ende se tiene que añadir un bloque por cada empresa que tenga el consentimiento del titular.
Como se puede observar en los bloques 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 demás atributos son iguales a los del primer bloque. Como se mencionó, en este caso se crearán bloques nuevos por cada responsable de tratamiento que estaba usando los datos del titular, dos responsables de tratamientos usaban los datos del titular por lo cual se crearán dos bloques nuevos.

❒ **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 cambió 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 presentan los atributos, hashMain, hashEnterprise, previousHash-Main, previousHashEnterprise, heigh y heighEnterprise en la Figura 7.9.

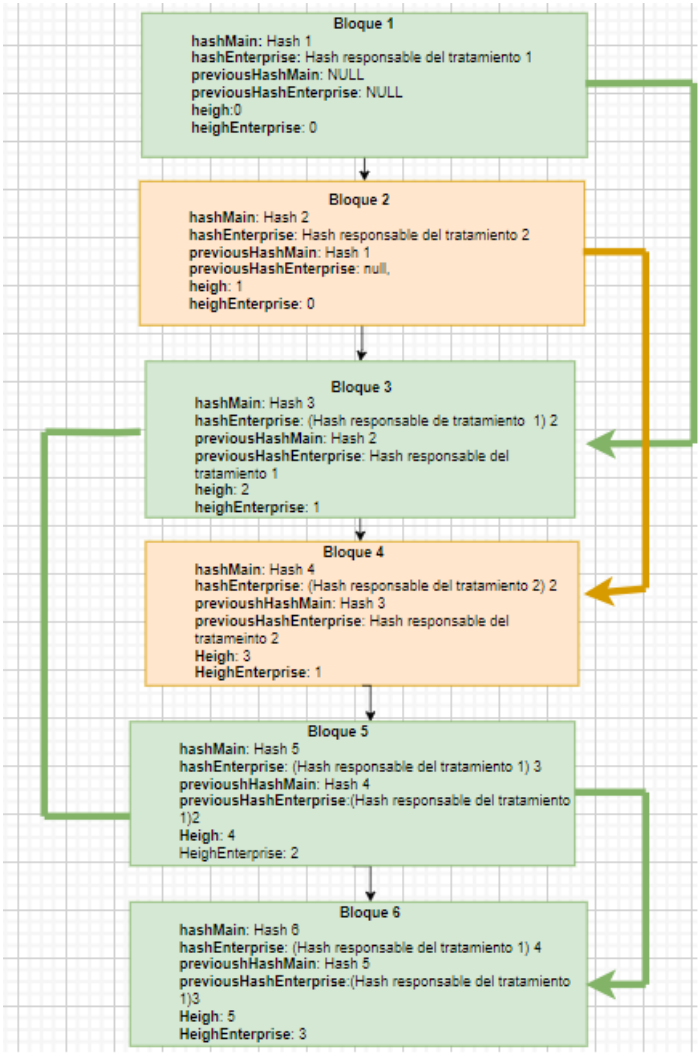


Figura 7.9: Diagrama de los 6 bloques mostrados en los ejemplos Fuente: Elaborado por el autor

8 ANÁLISIS DE RESULTADOS, CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

Habiendo terminado cada una de las fases anteriores, se procedió a realizar un análisis de los resultados del proyecto realizado. Una vez hecho el análisis de resultados, a partir de estos se obtuvo conclusiones, trabajo futuro que se puede realizar y finalmente recomendaciones.

8.1 ANÁLISIS DE RESULTADOS

Por medio del sistema realizado el titular de los datos puede comprobar que sus datos están siendo usados tal y como lo permitió al momento de aceptar una solicitud de tratamiento. También se puede comprobar que el encargado del tratamiento de datos está cumpliendo con lo que dijo en la solicitud de tratamiento. De esta forma se puede garantizar que el consentimiento del usuario se está cumpliendo. Si existe alguna violación al consentimiento del titular, el titular se puede dar cuenta de inmediato al momento de comprobar el hash de su respectiva solicitud de tratamiento de un responsable de tratamiento. Gracias a los artículos de la LOPDP pudimos construir un prototipo de software que cumple con los requerimientos planteados inicialmente.

8.2 CONCLUSIONES

- ❒ Gracias a la revisión sistemática de la literatura sobre el control de acceso y gestión de consentimiento, se evidencio que existen muchas formas para garantizar el control de acceso y la gestión de consentimiento, desde interfaces amigables hasta soluciones un poco más avanzada como la implementación de blockchain.

- ❒ El marco utilizado para el desarrollo de software resultó indispensable al momento del desarrollo del producto de software brindando retroalimentación por parte del Product Owner.

- ❒ Aplicar la tecnología blockchain para satisfacer la Ley Orgánica de Protección de Datos Personales es factible, y que la idea de que el usuario pueda garantizar la integridad y seguridad de sus datos a través de la confirmación del hash del bloque resulta ser una solución para el problema planteado en la fase inicial del proyecto.

- ❒ Los artículos de la LOPDP resultaron indispensables para la realización del presente proyecto, ya que a partir de sus artículos se obtuvo los requerimientos para la construcción del prototipo de software.

8.3 RECOMENDACIONES

- ❒ Escoger la metodología o marco adecuado resultó indispensable para el desarrollo del presente proyecto. Por lo cual recomendamos brindar una gran parte de su tiempo al momento de escoger la metodología o marco que se aplicará en las fases de su proyecto.

- ❒ MongoDB resultó indispensable para el desarrollo del prototipo de software, actualmente no es muy común encontrar una base de datos NoSQL, pero en nuestra experiencia manejando los dos tipos de bases tanto SQL como NoSQL, las bases de datos NoSQL resultan más intuitivas de manejar.

- ❒ LOPDP tiene muchas similitudes con GDPR, dado que la GDPR tiene más tiempo de existencia que la LOPDP existen ya soluciones tecnológicas, sin embargo, para que las empresa ecuatorianas se adapten de mejor manera, recomendamos leer la LOPDP ya que no es similar totalmente a la GDPR. De esta manera pueden encontrar soluciones mejores que no se basen en la GPDR.

8.4 TRABAJO FUTURO

- ❒ Como se mencionó anteriormente blockchain funciona de manera descentralizada, sin embargo, en el prototipo realizado, nuestro Blockchain no funciona así. Es convenien-

te realizar un análisis de como implementar redes descentralizadas en la tecnología backend implementada para el prototipo es decir Nodejs o encontrar nuevas tecnologías como Fastest de Ethereum que permite el desarrollo de aplicaciones blockchain.

- ❒ Las colecciones creadas para el prototipo de software se pueden mejorar, se sugiere realizar un análisis de las colecciones implementadas para reducirlas y de esta manera que sean más legibles y entendibles.

9 REFERENCIAS BIBLIOGRÁFICAS

[1] *Blockchain: Qué es y cómo funciona esta tecnología*, dic. de 2022. dirección: https://www.welivesecurity.com/la-es/2022/05/13/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/.

[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] Rae, *Definición de Privacidad - Diccionario Panhispánico del español jurídico - rae*. dirección: https://dpej.rae.es/lema/privacidad.

[6] P. Europeo, *Reglamento (UE) 2016/ 679 del parlamento europeo y del consejo - boe.es*. dirección: https://www.boe.es/doue/2016/119/L00001-00088.pdf.

[7] S. of California Department of Justice, *California Consumer Privacy Act CCPA*, mar. de 2022. dirección: https://oag.ca.gov/privacy/ccpa.

[8] A. Nacional, *Quinto Suplemento - Gob*. dirección: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf.

[9] telecomunicaciones.gob.e, *Gob*. dirección: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf.

[10] D. K. M. Solomon, *Fundamentals of Information Systems Security. Jones Bartlett Learning. pp. 144-. ISBN 978-0-7637-9025-7.* Nov. de 2010.

[11] IBM. dirección: https://www.ibm.com/docs/es/sva/10.0.5?topic=administration-access-control-policies.

[12] Cookiebot, *Home Page*. dirección: https://www.cookiebot.com/es/.

[13] 25IsoTools, *ISO 27001 - software ISO 27001 de Sistemas de Gestión*, jul. de 2022. dirección: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/.

[14] 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#/.

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

[16] 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.

[17] R. K. Jamra, B. Anggorojati, D. I. Sensuse, R. R. Suryono et al., «Systematic Review of Issues and Solutions for Security in E-commerce,» en *2020 International Conference on Electrical Engineering and Informatics (ICELTICs)*, IEEE, 2020, págs. 1-5.

[18] D. T. Dietz, L. A. Gorenstein, G. S. Veldman y K. D. Colby, «Shared Research Group Storage Solution with Integrated Access Management,» ACM, jul. de 2017, págs. 1-7, ISBN: 9781450352727. DOI: 10.1145/3093338.3093354.

[19] W. Shoukun, W. Kaigui y W. Changze, «Attribute-based solution with time restriction delegate for flexible and scalable access control in cloud storage,» ACM, dic. de 2016, págs. 392-397, ISBN: 9781450346160. DOI: 10.1145/2996890.3007851.

[20] S. Drame-Maigne, M. Laurent y L. Castillo, «Distributed access control solution for the IoT based on multi-endorsed attributes and smart contracts,» IEEE, jun. de 2019, págs. 1582-1587, ISBN: 978-1-5386-7747-6. DOI: 10.1109/IWCMC.2019.8766478.

[21] S. K. Khatri, Monica y V. R. Vadi, «Biometrie based authentication and access control techniques to secure mobile cloud computing,» IEEE, ago. de 2017, págs. 1-7, ISBN: 978-1-5090-6710-7. DOI: 10.1109/TEL-NET.2017.8343558.

[22] J. Galka, M. Masior y M. Salasa, «Voice authentication embedded solution for secured access control,» *IEEE Transactions on Consumer Electronics*, vol. 60, págs. 653-661, 4 nov. de 2014, ISSN: 0098-3063. DOI: 10.1109/TCE.2014.7027339.

[23] K. K. Kolluru, C. Paniagua, J. van Deventer, J. Eliasson, J. Delsing y R. J. DeLong, «An AAA solution for securing industrial IoT devices using next generation access control,» IEEE, mayo de 2018, págs. 737-742, ISBN: 978-1-5386-6531-2. DOI: 10.1109/ICPHYS.2018.8390799.

[24] P. S. W. Shieng, J. Jansen y S. Pemberton, «Fine-grained Access Control Framework for Igor, a Unified Access Solution to The Internet of Things,» *Procedia Computer Science*, vol. 134, págs. 385-392, 2018, ISSN: 18770509. DOI: 10.1016/j.procs.2018.07.194.

[25] Z. Zulkefli y M. M. Singh, «Sentient-based Access Control model: A mitigation technique for Advanced Persistent Threats in Smartphones,» *Journal of Information Security and Applications*, vol. 51, pág. 102 431, abr. de 2020, ISSN: 22142126. DOI: 10.1016/j.jisa.2019.102431.

[26] Z. Wan, J. Liu y R. H. Deng, «HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing,» *IEEE Transactions on Information Forensics and Security*, vol. 7, págs. 743-754, 2 abr. de 2012, ISSN: 1556-6013. DOI: 10.1109/TIFS.2011.2172209.

[27] D. Leibenger y C. Sorge, «A storage-efficient cryptography-based access control solution for subversion,» ACM Press, 2013, pág. 201, ISBN: 9781450319508. DOI: 10.1145/2462410.2462420.

[28] H. F. Atlam y G. B. Wills, «An efficient security risk estimation technique for Risk-based access control model for IoT,» *Internet of Things*, vol. 6, pág. 100 052, jun. de 2019, ISSN: 25426605. DOI: 10.1016/j.iot.2019.100052.

[29] K. C. Madathil, R. Koikkara, J. Obeid et al., «An investigation of the efficacy of electronic consenting interfaces of research permissions management system in a hospital setting,» *International Journal of Medical Informatics*, vol. 82, págs. 854-863, 9 sep. de 2013, ISSN: 13865056. DOI: 10.1016/j.ijmedinf.2013.04.008.

[30] M. Laurent, J. Leneutre, S. Chabridon e I. Laaouane, «Authenticated and Privacy-Preserving Consent Management in the Internet of Things,» *Procedia Computer*

Science, vol. 151, págs. 256-263, 2019, ISSN: 18770509. DOI: 10.1016/j.procs.2019.04.037.

[31] S. Nakamura, T. Enokido y M. Takizawa, «Information Flow Control Based on the CapBAC (Capability-Based Access Control) Model in the IoT,» *International Journal of Mobile Computing and Multimedia Communications*, vol. 10, págs. 13-25, 4 oct. de 2019, ISSN: 1937-9412. DOI: 10.4018/IJMCMC.2019100102.

[32] 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.

10 ANEXOS

1. Controles de la ISO 27001 que se relacionan con el control de acceso y gestión de consentimiento.
2. Controles de la NIST 800-53 que se relacionan con el control de acceso y gestión de consentimiento.
3. Video del aplicativo web.
4. Código frontend.
5. Código backend.