Facultad de Ingeniería

Escuela de Ingeniería en Tecnologías de la Información y la Comunicación

Proyecto de grado para optar por el título de:

Ingeniero en Tecnologías de la Información y la Comunicación

PROYECTO DE GRADO

Estrategia de Validación y Verificación de Documentos Estudiantiles para la Transformación Digital de la Administración Universitaria: Apoyo a través de la tecnología Blockchain

Sustentantes:

José Ediberto Germán Ray 18-0200

José Roberto Félix Ramírez 18-0677

Asesor:

Dr. Darwin Muñoz

25 de agosto de 2021

Santo Domingo, D.N.

República Dominicana

Dedicatoria

A mi familia, amigos y profesores, los cuales han estado conmigo durante todo este trayecto para convertirme en profesional. Dicho esto, quiero hacer una dedicatoria especial a mis padres, Angiolina Ray y José Germán, y a mi difunta abuela, Mercedes Santos, la persona de la que más he aprendido en toda mi vida, y la que me enseñó que el amor es la fuerza más poderosa de este mundo, a siempre ser humilde con las demás personas y, a entender que, ante Dios, todos somos iguales.

José Ediberto Germán Ray

Dedicatoria

A toda mi familia en especial a mis padres, Estela Ramírez y José Félix Mayib, por creer en mí, y enseñarme la importancia del amor y a valorar la empatía y la humildad. Quisiera darle una especial distinción a mi difunto padre que me mostró lo que es ser un profesional ejemplar y a valorar el trabajo arduo.

José Roberto Félix Ramírez

Agradecimientos

A Dios, nuestro Padre Eterno, porque sin él, nada de lo que he conseguido en mi vida sería posible, por haber llenado mi camino de personas buenas y por mostrarme que su amor no tiene límites.

A mis padres, por la gran formación que me han dado, su dedicación en mi crianza y por su apoyo durante todas las cosas que he hecho en mi vida, en especial por apoyarme en mi camino para convertirme en un profesional.

A mi querido tío Dr. Milton Ray Guevara, por su apoyo incondicional y por ser uno de mis modelos a seguir.

A mi hermana Yamel Germán Ray, por su gran apoyo durante toda esta etapa.

A mi compañero y amigo José Félix, una persona de la que he aprendido muchas cosas y que se ha convertido en un hermano para mí.

Al cuerpo docente de nuestra querida universidad, resaltando a los profesores Kaking Choi, Rina Familia, Francis Jáquez, Néstor Matos y Luis Bayonet, ya que más que servirnos como facilitadores en las diferentes asignaturas que hemos cursado con ellos, nos han dejado enseñanzas de vida, las cuales tendremos siempre presentes tanto en nuestra vida profesional como en nuestra vida personal.

José Ediberto Germán Ray

Agradecimientos

A Dios por ayudarme a seguir en el buen camino y a continuar adelante enfrentando las adversidades sin perder la esperanza ni fracasar.

A mi familia por estar conmigo y apoyarme incondicionalmente durante este viaje profesional.

A mi compañero de proyecto de grado, José Germán, por convertirse en uno de esos amigos a los que puedo llamar hermanos, y compartir el proceso de desarrollo de esta aspiración.

A mis profesores de nuestra querida universidad UNIBE, destacando a los profesores Kaking Choi, Luis Bayonet, Willis Polanco, Osiris Decena, Francis Jáquez, y Néstor Matos, por ser excelentes maestros que contribuyeron a forjar mi camino profesional con lecciones invaluables que marcarán mi vida profesional.

José Roberto Félix Ramírez

Abstract

One of the things that makes the vast majority of professionals feel proud is the entire journey they had to go through to achieve their goal (in many cases they consider it their dream) of becoming competent people in different areas of knowledge. Throughout history there have been many cases of falsification of degrees and university documents at all levels of education, which makes academic fraud a major threat to both the educational system and the reputation of the institutions that comprise it.

Our proposal is to use Blockchain technology to certify university administrative documents, like degrees and transcripts. This would allow employers to take only a few seconds to verify an applicant's documents and would provide students with a simpler way to prove that their documents are legitimate. The platform would initially be designed for use at UNIBE, however, we believe that it can be implemented in the vast majority of higher education institutions and could even be implemented in our country's elementary and middle school system.

These implementations, in addition to giving a strong blow to the dark business of academic fraud, would make our nation a benchmark in the Caribbean region, so it would be a great investment for both universities and our government if they decide to adopt this technology to certify their documents.

Keywords: Blockchain, Documents, Certification, Fraud, Programming, Universities, Security.

Resumen

Una de las cosas que hacen sentir orgullosos a la gran mayoría de profesionales es todo el trayecto que tuvieron que recorrer para lograr su meta (en muchos casos lo consideran su sueño) de convertirse en personas competentes en las diferentes áreas del saber. A lo largo de la historia, ha habido muchos casos de falsificación de títulos y documentos en todos los niveles de la educación, lo que hace que el fraude académico constituya una gran amenaza tanto para el sistema educativo como para la reputación de las instituciones que lo integran.

Nuestra propuesta consiste en utilizar la tecnología del Blockchain (Cadena de bloques) para certificar documentos administrativos universitarios, como por ejemplo títulos de grado y récord de notas. Esto permitiría que los empleadores duren solo unos segundos para verificar los documentos de un aplicante, y de paso, les proveería a los estudiantes una manera más simple de probar que sus documentos son legítimos. La plataforma en principio sería diseñada para usarse en UNIBE, sin embargo, pensamos que se puede implementar en la gran mayoría de instituciones de educación superior y que incluso se podría implementar en el sistema de educación básica y media de nuestro país.

Estas implementaciones además de darle un fuerte golpe al negocio oscuro del fraude académico, convertirían a nuestra nación en un referente en la región del Caribe, por lo que resultaría una gran inversión tanto para las universidades como para nuestro gobierno si deciden adoptar esta tecnología para certificar sus documentos.

Palabras Clave: Blockchain, Documentos, Certificación, Fraude, Programación, Universidades, Seguridad.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Capítulo 1: Introducción e Información General

1.0 Introducción

El fraude es un elemento de riesgo presente en casi todas las áreas de nuestra sociedad. Lo hemos visto en elecciones, en compra y venta de terrenos, en falsificaciones de identidad y en el tema del que vamos a hablar en cuestión, la falsificación de documentos universitarios. Históricamente siempre ha estado presente y es nuestra responsabilidad ética utilizar todos los recursos que nos permitan disminuir el número de casos de fraude que se dan en el mundo de las TIC.

En el ámbito universitario, el fraude académico constituye una grave problemática, ya que se mancha el nombre de una universidad y de paso, se pisotea a aquellas personas que sí se esforzaron y lograron completar su programa de estudios de manera legítima.

Nuestra motivación para llevar a cabo este proyecto no es más que contribuir a disminuir la cantidad de fraudes académicos y proporcionar una herramienta para proteger la integridad y el nombre de nuestra universidad, y de todas aquellas instituciones que quieran implementar esta tecnología para llevar a cabo la certificación de sus documentos.

Hemos identificado que la mejor opción para dar una solución a este problema es a través de la tecnología de Blockchain (Cadena de bloques), el cual es un sistema que garantiza la integridad de la información almacenada en el mismo y que a su vez, ha tenido casos de uso bastante exitosos, como su uso en las criptomonedas.

Creemos que esto puede tener un gran impacto, y que puede iniciar una tendencia para que certificar los documentos utilizando la tecnología de Blockchain se vuelva un estándar y que nuestro país se vuelva un referente en la región del Caribe en cuanto a metodologías y herramientas utilizadas para certificar documentos y evitar posibles fraudes.

1.1 Planteamiento del Problema

En la República Dominicana se han visto múltiples casos de falsificación de títulos universitarios. Incluso, en 2014 la empresa reclutadora de personal Business Solutions Group denunció que al menos el 70% de los títulos y/o certificados de bachiller que recibieron por parte de personas interesadas en ser contratadas por alguna empresa eran falsos o habían sido alterados. (Periódico Hoy, 2014).

Otro caso bastante recordado, ocurrió en el 2017, cuando se desmanteló un laboratorio que falsificaba títulos universitarios y otros documentos. Este operativo fue llevado a cabo por la Dirección Regional de Santo Domingo Oriental de la Policía Nacional, la cual se presentó a este laboratorio clandestino que operaba en el sector de Villa Carmen, donde se falsificaban cédulas, cartas bancarias, matrículas para vehículos, títulos universitarios y otros documentos. (Pichardo, 2017).

Así como los casos anteriormente mencionados, suceden muchos otros que no llegan a la prensa o a la opinión pública. Esto representa una grave problemática y significa un cáncer para nuestra sociedad. Este problema debe cortarse de raíz, y nosotros como futuros ingenieros en el área de las TIC tenemos la responsabilidad ética de destinar esfuerzos para evitar que estos fraudes se sigan dando.

1.2 Situación Actual

En la actualidad, en nuestro país no muchas instituciones tienen mecanismos para proteger sus documentos de la posibilidad de ser falsificados. Incluso, pocas instituciones emiten sus documentos de forma digital. Una de ellas es nuestra universidad, esa emisión tiene cierto nivel de protección, pero no al nivel que ofrece la tecnología del Blockchain (esta parte es detallada en el acápite de aplicaciones similares).

Resulta preocupante que las demás universidades no se hayan preocupado por hacer esta inversión para empezar a emitir sus certificados de manera digital, ya que además de

mostrar su compromiso con estar a la vanguardia con las soluciones tecnológicas que se van creando en el mercado, representaría una gran ayuda para sus egresados, ya que los departamentos de recursos humanos de las empresas donde apliquen tendrían la facilidad de comprobar la validez de sus documentos en tan solo unos segundos utilizando la tecnología de Blockchain.

En los países desarrollados la situación es un poco distinta. Por ejemplo, en España desde el año 2018 los egresados de la Universidad Carlos III, la Universidad Internacional de la Rioja (UNIR) y el Instituto Superior para el Desarrollo de Internet (ISDI) tienen la opción de recibir sus títulos validados con la tecnología de Blockchain, los cuales pueden compartirse con empresas reclutadoras y plataformas de redes sociales tales como LinkedIn, garantizando así la inviolabilidad del documento. (Criptonoticias, 2018).

Otro caso que data del año 2019 es el de la Universidad Provincial del Sudoeste de la Provincia de Buenos Aires (UPSO) en Argentina, la cual se convirtió en la primera universidad argentina en implementar Blockchain para comenzar a emitir sus documentos de manera digital. (Universia, 2019).

En México, el Tecnológico de Monterrey ha sido el pionero en la emisión de títulos utilizando Blockchain. Desde el año 2019 les dan a sus egresados la posibilidad de tener sus títulos en formato digital y avalados por la tecnología de cadena de bloques, sentando un precedente en ese país. (Expansión, 2021).

Otras instituciones de educación superior que emiten sus diplomas usando Blockchain son el Instituto Tecnológico de Massachusetts (MIT), la Universidad Harvard, la Universidad de California en Berkeley y la Universidad de California, de Estados Unidos; la Universidad Técnica de Múnich y la Universidad de Potsdam, de Alemania; la Universidad Tecnológica de Delft, en Países Bajos; y la Universidad de Toronto, en el país de Canadá. (Expansión, 2021).

1.3 Justificación de la investigación

La falsificación de un título universitario representa una amenaza no solo para el sistema de educación superior, sino para todo el sistema educativo en general. El hecho de poder falsificar un diploma de alguna universidad y aplicar para conseguir un trabajo sin tener que estudiar constituye una fuerte tentación y puede hacer que un gran número de estudiantes pierdan el interés en estudiar y que simplemente quieran pasar por encima de las reglas, pisoteando a aquellos que sí han dedicado mucho esfuerzo y tiempo para convertirse en profesionales.

Otro de los motivos principales por los cuales decidimos hacer esta investigación, es por la gran cantidad de casos que se han visto en nuestro país y en la región del Caribe. Resulta alarmante ver cómo las autoridades encuentran personas que se dedican a esto y que incluso van más allá de títulos universitarios, pueden hasta englobar falsificaciones de identidad, las cuales hasta son utilizadas en crímenes de diversa índole.

Si bien existen implementaciones de esta tecnología en diferentes partes del mundo, nosotros queremos ofrecer una solución dominicana a las diferentes instituciones que quieran implementar esta tecnología, para demostrar que en nuestro país tenemos profesionales altamente capacitados y que se debe invertir aún más en educación, especialmente en el área de las TIC, que es un área que todos los días va evolucionando y presentando cosas nuevas.

La implementación de este proyecto puede elevar aún más el estado de referente que tiene nuestra universidad, e incluso puede impulsar que el propio gobierno considere implementar la tecnología de Blockchain para comenzar a emitir documentos de forma digital, con lo cual además de impulsar una transformación digital en la administración universitaria, estaríamos impulsando una transformación digital en la administración pública.

1.4 Importancia e interés del tema

Tener medidas de prevención contra el fraude resulta bastante beneficioso en varios aspectos, se puede hablar de beneficios en materia social, educativa e incluso en la lucha contra el crimen, ya que la implementación de esta tecnología les daría un duro golpe a las personas y/o grupos que se dedican a la falsificación o alteración de documentos.

Sería interesante tanto para universidades como para estudiantes, ya que les permitiría certificar y proteger sus documentos, y ponerse a la vanguardia en cuanto a tecnologías de protección contra fraude.

1.5 Limitaciones

Este proyecto contará con las siguientes limitaciones:

- En principio solo será aplicado a UNIBE.
- No se va a contar con la totalidad de documentos que ofrece la universidad.

1.6 Hipótesis Preliminar

El uso de la tecnología de Blockchain (cadena de bloques) aplicado a la emisión de documentos digitales aumenta los niveles de seguridad en el proceso de validación de su autenticidad, dificulta la realización de un fraude, y permite aumentar los niveles de confianza que tienen las personas en los servicios que involucran esta tecnología.

1.7 Objetivos

1.7.1 Objetivo General

El objetivo principal de nuestro proyecto es brindar una herramienta que transforme la manera en la que son emitidos los documentos universitarios, dándole mucha más seguridad a la emisión digital de los mismos y contribuyendo a facilitar el proceso tanto para la universidad como para el estudiante.

1.7.2 Objetivos Específicos

- Desarrollar e implementar una plataforma de validación de documentos utilizando Blockchain.
- Ayudar a combatir la falsificación de documentos.
- Facilitar la emisión de documentos digitales.
- Aumentar el nivel de confianza en los documentos digitales.

Capítulo 2: Marco Teórico y Estado del Arte

A nivel global, la tecnología del Blockchain ha representado una revolución que recuerda a lo ocurrido con el nacimiento de la Internet. Esta serie de cambios se ha visto especialmente en la economía, donde las llamadas criptomonedas se han convertido en uno de los fenómenos más grandes del siglo XXI, siendo la llamada Bitcoin (BTC) la criptomoneda más famosa del mundo, llegando a costar la unidad unos $64,863.10 en su pico más alto. (BBC News Mundo, 2019).

En cuanto a nuestro tema en cuestión (usar Blockchain para validar documentos) tanto en los Estados Unidos, en algunas partes de América Latina como Argentina y México, y en muchos países de Europa ya se usa esta tecnología para certificar y proteger sus documentos. Debido a la importancia (e incluso en estos tiempos se le puede llamar necesidad) de un registro confiable de la información, Blockchain ha representado un gran mecanismo para poder asegurar la integridad de los datos desde su origen, proporcionado una forma de evitar los fraudes y de salvaguardar el valor de la honestidad.

2.1 Antecedentes y referencias

Si nos ponemos a buscar algún antecedente o referencia en cuanto a investigaciones sobre la utilización del Blockchain es imposible quedarnos cortos. En este sentido, podemos mencionar los siguientes:

- **Uso de Blockchain en la administración pública:** este proyecto fue presentado en el año 2019 por Eduardo Mereles y Juan Ortellado, estudiantes de la Universidad de la República en el país de Uruguay. El tema central de este proyecto, tal y como su título lo indica, fueron las posibles aplicaciones que podría tener la tecnología de Blockchain en la administración pública de su país. El objetivo de este proyecto fue investigar la tecnología en general, así como herramientas que permitan trabajar con Blockchain y a través de ellas evaluar su aplicabilidad a un caso de uso en la

administración pública. Los resultados finales fueron satisfactorios, ya que pudieron comprobar su hipótesis preliminar. Estos resultados anteriormente mencionados les dejaron con la siguiente conclusión. “Un aspecto importante que se saca como conclusión y se considera se debe mejorar es lo relacionado con la aplicabilidad de Blockchain. El uso de la tecnología de Blockchain es altamente recomendable en escenarios donde sea necesario contar con coordinación, confiabilidad y seguridad de datos entre múltiples actores sin intermediarios”. (Mereles & Ortellado, 2019).

- **Revisión sistemática del uso de Blockchain en datos clínicos y su aplicación en Colombia**: este proyecto fue llevado a cabo en el año 2018 por Diego Oliveros, estudiante de la Universidad Católica de Colombia. El tema central de este proyecto es cómo utilizar la tecnología de Blockchain en la gestión de los datos clínicos en Colombia. El objetivo principal era realizar una revisión sistemática de la aplicación de Blockchain para entender cómo sería su aplicación en los servicios de salud en el contexto colombiano. Esto para que, por medio de estudios y síntesis de los datos extraídos y analizados, se den métodos y soluciones para aplicar en los procesos de entidades de salud. Sus resultados comprobaron que la gestión de datos clínicos en Colombia se podía clasificar como deficiente. Por lo que, en sus recomendaciones, establece que “en trabajos futuros, se recomienda la integración de tecnología Blockchain para dar solución a falencias en el cuidado de la salud, sin descuidar la privacidad de los datos, además de respaldarse en desarrolladores, lenguajes y estructuras que aportan y facilitan la implementación de esta tecnología, por otro lado, visualizar los avances tecnológicos futuros para estar un paso adelante a lo que vulneración de sistemas se refiere”. (Oliveros, 2018).

2.1.1 Aplicaciones Similares

Una aplicación similar a nuestra propuesta es “eTítulo” desarrollada por la empresa española SIGNE. Consiste en una copia electrónica auténtica, en formato pdf, del título universitario, el cual se encuentra firmado electrónicamente. Contiene un código BIDi, el cual permite la verificación de los datos del emisor y cuenta con un Código Seguro de Verificación (CSV). (Universidad Iberoamericana, 2019).

Nuestra propia universidad usa esta aplicación, sin embargo, solo se encuentra aplicada a los títulos universitarios. Nuestro objetivo es aplicar la tecnología de Blockchain a todos los documentos que emite la universidad.

Blockcerts es otro sistema similar. Fue desarrollado por la compañía estadounidense PixelPlex y es una plataforma basada en la tecnología de Blockchain para crear, ver y auditar documentos digitales en el ecosistema inteligente de Ethereum. (PixelPlex, s. f.).

Otra iniciativa es la de Certifaction, la cual es un API desarrollada por un grupo de desarrolladores suizos para certificar documentos utilizando la tecnología de la cadena de bloques. Además del Blockchain, esta empresa ofrece servicios de firmas inteligentes y el llamado “gemelo digital”, que consiste en una copia digital del documento, la cual se encuentra encriptada y consta de un código QR para su posterior acceso. (Certifaction, s. f.).

Otro caso bastante particular es el de Japón. El gobierno japonés se encuentra desarrollando proyectos sobre usos de la cadena de bloques para registrar propiedades y para todos los trámites relacionados con bienes raíces. Esto convierte al país del sol naciente en uno de los que mayor adaptación pública y privada están haciendo de la cadena de bloques. Según fuentes locales, la intención es identificar y unificar todos los datos sobre propiedades vacías o sin dueño, tierras y espacios improductivos,

> propietarios desconocidos e inquilinos o usuarios sin identificar ante los organismos. La consolidación de estos datos y su disponibilidad ante todos los organismos competentes mediante el Blockchain permitirá garantizar la inviolabilidad de la información y asegurar que no se cometa ningún tipo de fraude. (Alcaide, 2019).

2.2 Base teórica

2.2.1 Blockchain

Blockchain o cadena de bloques (traducido al español), es un sistema mediante el cual se pueden realizar transacciones de forma segura entre personas de todo el mundo sin necesidad de intermediarios. (Fernández, 2020).

Nació debido a la necesidad de eliminar intermediarios como los bancos (cuando se habla de operaciones financieras). Tradicionalmente, estas entidades han sido necesarias para poder hacer transacciones de mucho valor, ya que ellas son las encargadas de certificar que los participantes en la transacción son quienes dicen ser. A cambio de este servicio que consiste básicamente en servir como garante, las entidades bancarias y/o plataformas electrónicas como Paypal se quedan con los datos de los usuarios y comercian con ellos. Esto obviamente limita la privacidad de los participantes en las transacciones y, por ende, condiciona su libertad a la hora de realizarlas. (Fernández, 2020).

2.2.2 Componentes fundamentales de Blockchain

En primer lugar, tenemos que entender que no todas las cadenas de bloques son iguales. A nivel general, se pueden clasificar los diferentes tipos de Blockchain en cuatro categorías: públicos, privados, federados y “Blockchain como un servicio”. Sus diferencias fundamentales son el modelo de administración que utilizan y el nivel de descentralización y/o el grado de transparencia que presentan. El tipo de cadena más utilizado para desarrollar soluciones con valor de impacto social son las redes federadas, las cuales permiten a las

empresas y a las instituciones gubernamentales usar el Blockchain para generar confianza y aumentar la seguridad. (López, 2019).

Es cierto que existen diferentes tipos de cadenas de bloques, sin embargo, existen ciertos componentes que prácticamente todos los Blockchain tienen en común por defecto, los cuales son los nodos, los bloques y las transacciones. (López, 2019).

Transacciones

En la cadena de bloques, una transacción es definida como un mensaje firmado digitalmente que autoriza alguna acción en particular asociada a la cadena. El uso más conocido es el de las criptomonedas, donde el tipo de transacción más común es el que involucra al menos a dos partes y está asociado al intercambio de bienes o servicios a cambio del capital correspondiente. (Mereles & Ortellado, 2019).

Bloques

Los bloques son un conjunto de registros que representan la información del Blockchain. Un bloque se encuentra formado por un conjunto de transacciones que han sido confirmadas y la información adicional que se ha incluido en la cadena. Del mismo modo que sucede con las transacciones, dependiendo de la plataforma sobre la cual se esté trabajando, puede variar la información que lleva el bloque, pero en líneas generales algunos de estos campos se mantienen en la estructura de cualquier bloque (a excepción del bloque generatriz, el cual inicia la cadena). (Mereles & Ortellado, 2019).

Estos campos son:

- Un hash que cumple la función de enlazar con el bloque anterior.
- El conjunto de transacciones que incluye.
- La marca de tiempo de la generación del bloque.
- Otro hash que cumplirá la función de enlazar con el bloque siguiente.

Una cadena de bloques en construcción se vería de la siguiente manera:

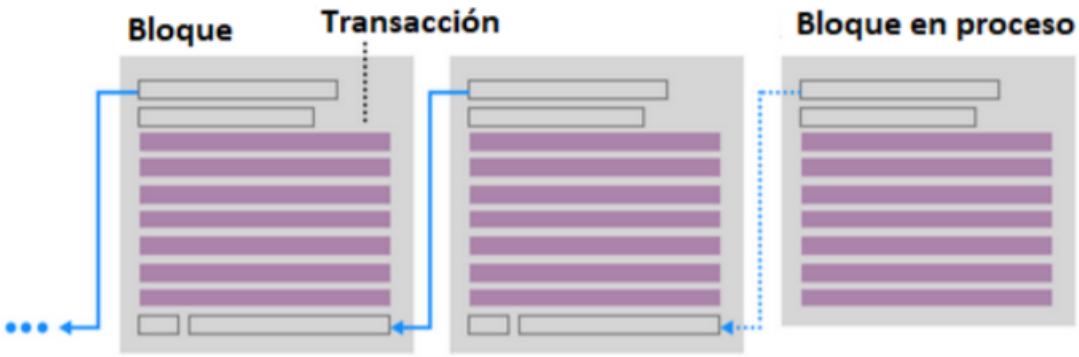

Figura 2.1. Cadena de bloques en construcción (Mereles & Orellado, 2019).

Nodos

Un nodo se define como un ordenador conectado a la red de la cadena de bloques que utiliza un software que almacena y distribuye una copia de la información de la cadena en tiempo real. De manera conceptual, este nodo puede estar representando una organización o una entidad, tales como una empresa o alguna entidad gubernamental. (Mereles & Ortellado, 2019).

Dependiendo del tipo de cadena de bloques y los privilegios que tenga un nodo en cuestión, este nodo tendrá la facultad para validar bloques y transacciones, agregar transacciones a un bloque y añadir bloques a la propia cadena. Cada vez que un bloque es confirmado y se añade a la cadena, esta acción es comunicada a todos los nodos miembros del Blockchain y todos añaden la transacción a la copia de seguridad que cada uno almacena. Cada nodo representa un seguro de vida para la cadena, por tanto, mientras más nodos haya en la cadena, muchas más copias habrá y, por ende, la información almacenada estará más segura. (Mereles & Ortellado, 2019).

Un ejemplo donde se vieran a los tres componentes de la cadena de bloques en acción podría ser representar la cadena como un libro de cuentas donde los bloques se corresponden a hojas del libro anteriormente mencionado, las transacciones corresponden a párrafos de

cada hoja del libro y los nodos corresponden a cada lugar del mundo donde existe una copia de ese libro. La ilustración se vería de la siguiente manera:

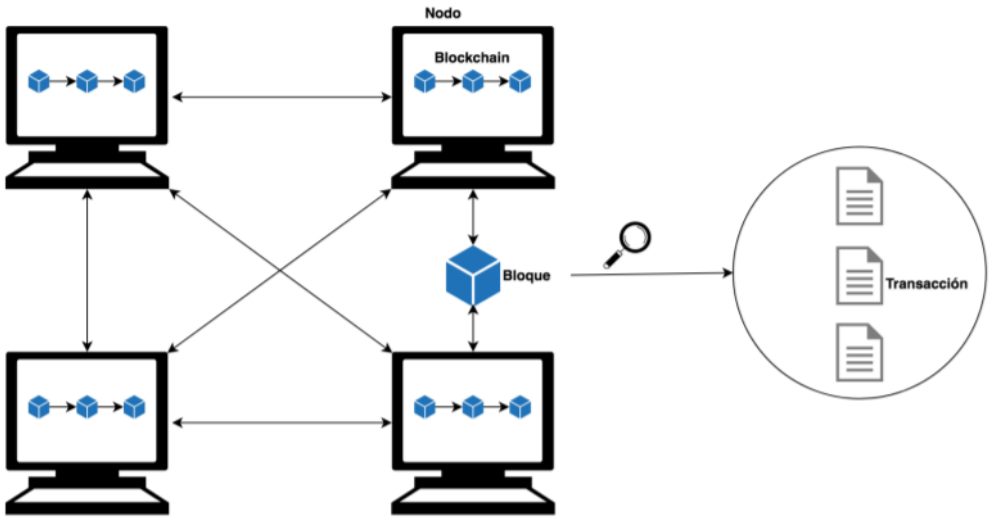

Figura 2.2. Ilustración de cada componente de la cadena de bloques. (Elaboración Propia).

2.2.3 Tipos de Blockchain

Como mencionamos anteriormente, existen diferentes tipos de cadenas de bloques. Estas pueden aplicarse dependiendo del caso de uso donde se va a aplicar, ya que se pueden presentar distintos requerimientos dentro del Blockchain.

Blockchain pública

Tal y como su nombre lo indica, se encuentran abiertas al mundo, por lo que cualquier interesado que desee, puede unirse. Además, todos tienen la facultad para copiar los datos de la cadena, leer o proceder a escribir nuevas transacciones y comenzar a participar en el proceso de validación de las transacciones. (Mereles & Ortellado, 2019).

Blockchain federada

Por otro lado, las cadenas de bloques federadas funcionan bajo el control de un grupo. Estas no tienen permitido que todos los miembros de la red participen del proceso de validación. Dado que en estas cadenas los nodos que validan las transacciones son un conjunto que está definido e identificado, generalmente usan certificados para firmar sus transacciones, razón por la cual el ingreso de una transacción se hace de forma ágil. (Mereles & Ortellado, 2019).

Blockchain privada

Son aquellas cadenas que pertenecen a una entidad única, donde todos los participantes de la red están plenamente identificados. La diferencia con las anteriores es que el derecho a leer de la cadena es restringido únicamente a los participantes. Este tipo de cadena de bloques es ideal para el manejo de los procesos internos de las empresas. Si comparamos, la privada y la federada son similares. (Mereles & Ortellado, 2019).

Tabla 2.1.

Comparación entre los tipos de Blockchain.

Categoría	**Pública**	**Privada**	**Federada**
Acceso	Lectura / Escritura Libre	Lectura / Escritura libre (para los miembros de la red)	Lectura / Escritura solo para los nodos autorizados. El resto de los participantes solo posee permisos de lectura
Velocidad	Lenta	Rápida	Rápida
Seguridad	Proof of Work, Proof of Stake y otros mecanismos de consenso	Participantes autorizados	Participantes autorizados
Identidad	Anónimos y Pseudo - anónimos	Identidades conocidas	Identidades conocidas

Nota. Fuente: Elaboración Propia.

2.2.4 Integridad de la Información

Este es uno de los conceptos sobre los cuales basamos todo el sentido de nuestro proyecto, ya que ese es uno de los objetivos fundamentales de cualquier aplicación de la tecnología de cadena de bloques. Al implementar Blockchain, existen diferentes mecanismos para garantizar la integridad de los datos. A continuación, procedemos a definir los más utilizados.

Proof of work

También llamada prueba de trabajo, es el mecanismo utilizado por Bitcoin y otras criptomonedas. Hace referencia a la generación de un hash que sea muy difícil de generar, pero que sea fácil de verificar. Esto implica que se genera un hash de un valor, o una transacción en este caso, con un determinado algoritmo. El objetivo es que el generador de ese hash tenga que dedicar una gran parte de sus recursos para generarlo, satisfaciendo la prueba de trabajo y de paso, asegurando que la generación de uno de esos hashes no sea fácil de reproducir o modificar. (Mereles & Ortellado, 2019).

Proof of stake

También llamada prueba de participación, este mecanismo de seguridad nació como alternativa a la prueba de trabajo, específicamente para solucionar el problema de costos que esta presenta. Proof of stake es usado por Ethereum, Credits y otras criptomonedas. A diferencia de la prueba de trabajo donde los nodos generadores pueden generar la cantidad de bloques que deseen, en la prueba de participación es necesario el uso de criptomonedas, dado que cada nodo puede generar bloques en proporción a la cantidad de criptomonedas que posea el mismo. Por ejemplo, si un nodo posee un 5% de la cantidad total de criptomonedas de la cadena de bloques, el mismo nodo sólo podrá generar un 5% de los bloques. (Mereles & Ortellado, 2019).

Proof of authority

Traducida como prueba de autoridad, este mecanismo se basa en tener un conjunto de nodos validadores, los cuales cumplen con la función de validar todas las transacciones que ocurren en el sistema. Este conjunto generalmente se mantiene reducido para asegurar que la eficiencia y la seguridad sean manejables. Es usado por Hyperledger, Corda, VeChainThor, entre otros. (Mereles & Ortellado, 2019).

Estrategia de Transacciones

Para mantener la seguridad de las transacciones, existen múltiples métodos. Vamos a tomar un ejemplo de Ethereum, la cual es una de las cadenas de bloques más grandes de todo el mundo. Este método se denomina “Separación de firma y transmisión”, también llamado firma sin conexión. (GitBook, s. f.).

Una vez que se firma una transacción, está lista para transmitirse a la red Ethereum. Los tres pasos para crear, firmar y difundir una transacción normalmente ocurren como una sola operación, por ejemplo, usando web3.eth.sendTransaction. Sin embargo, se puede crear y firmar la transacción en dos pasos separados. Una vez se tenga una transacción firmada, puede transmitirse usando web3.eth.sendSignedTransaction, que toma una transacción firmada y codificada en hexadecimal y la transmite en la red Ethereum. (GitBook, s. f.).

¿Para qué querríamos separar la firma y la transmisión de transacciones? La razón más común es la seguridad. La computadora que firma una transacción debe tener claves privadas desbloqueadas cargadas en la memoria. La computadora que realiza la transmisión debe estar conectada a Internet (y ejecutar un cliente Ethereum). Si estas dos funciones están en una computadora, entonces tiene claves privadas en un sistema en línea, lo cual es bastante peligroso. Separar las funciones de firmar y transmitir y realizarlas en diferentes máquinas (en un dispositivo fuera de línea y en línea, respectivamente) se denomina firma fuera de línea y es una práctica de seguridad común. (GitBook, s. f.).

El proceso sería de la siguiente manera:

- Se crea una transacción sin firmar en la computadora en línea donde se pueda recuperar el estado actual de la cuenta, especialmente el nonce actual y los fondos disponibles. (GitBook, s. f.).
- Se transfiere la transacción sin firmar a un dispositivo fuera de línea "con espacio de aire" para la firma de la transacción, por ejemplo, a través de un código QR o una unidad flash USB. (GitBook, s. f.).
- Se transmite la transacción firmada (de regreso) a un dispositivo en línea para su transmisión en la cadena de bloques Ethereum, por ejemplo, a través de un código QR o una unidad flash USB. (GitBook, s. f.).

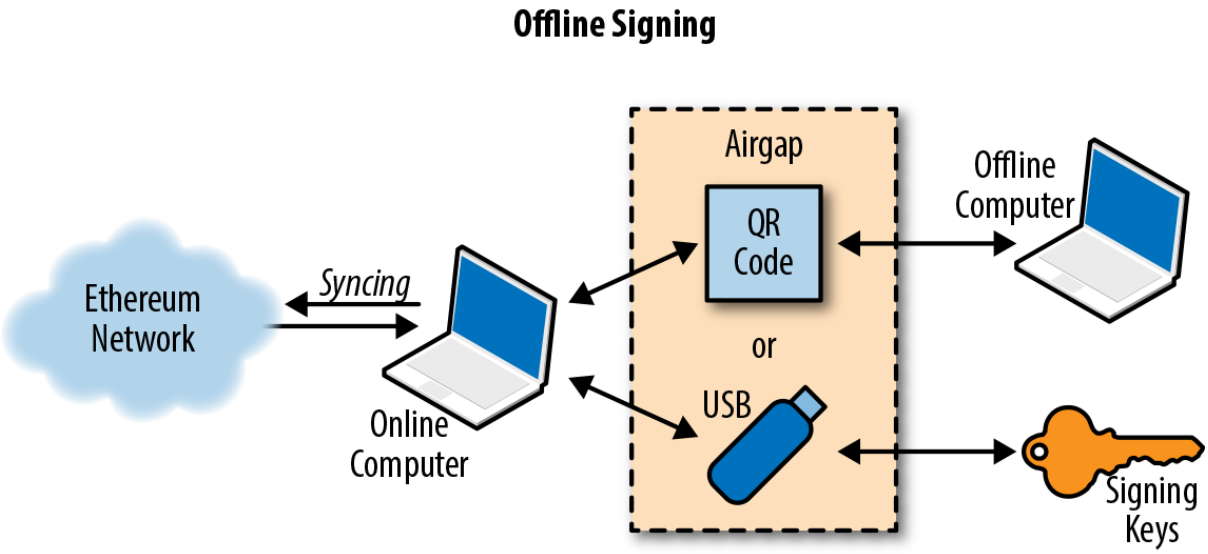

Figura 2.3. Ilustración del método de firma sin conexión. (Ethereum).

Dependiendo del nivel de seguridad que se necesite, la computadora de "firma sin conexión" puede tener diversos grados de separación de la computadora en línea, que van desde una subred aislada y con cortafuegos (en línea pero segregada) hasta un sistema completamente fuera de línea conocido como sistema con espacio de aire. En un sistema con espacio de aire no hay conectividad de red en absoluto: la computadora está separada del entorno en línea por un espacio de "aire". Para firmar transacciones, las transfiere hacia y

desde la computadora con espacio de aire utilizando medios de almacenamiento de datos o (mejor) una cámara web y un código QR. Por supuesto, esto significa que se deben transferir manualmente todas las transacciones que se desea que sean firmadas, y esto no aumenta. (GitBook, s. f.).

Si bien no muchos entornos pueden utilizar un sistema completamente con espacio de aire, incluso un pequeño grado de aislamiento tiene importantes beneficios de seguridad. Por ejemplo, una subred aislada con un cortafuegos que sólo permite un protocolo de cola de mensajes puede ofrecer una superficie de ataque mucho más reducida y una seguridad mucho más alta que iniciar sesión en el sistema en línea. Muchas empresas utilizan un protocolo como ZeroMQ (0MQ) para este propósito. (GitBook, s. f.).

Con una configuración como esa, las transacciones se serializan y se ponen en cola para su firma. El protocolo de cola transmite el mensaje serializado, de forma similar a un socket TCP, al equipo de firma. La computadora de firma lee las transacciones serializadas de la cola (cuidadosamente), aplica una firma con la clave apropiada y las coloca en una cola de salida. La cola de salida transmite las transacciones firmadas a una computadora con un cliente Ethereum que las quita de la cola y las transmite. (GitBook, s. f.).

2.3 Base legal

Si examinamos las leyes de nuestro país, podemos encontrar una ley que nos sirve de base legal para nuestro proyecto. Esta es la Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología, la cual tiene como objeto “la protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido, así como la prevención y sanción de los delitos cometidos contra éstos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas física o morales, en los términos previstos en esta ley. La integridad de los sistemas de información y sus componentes, la información o los datos, que se almacenan o transmiten a través de éstos, las

transacciones y acuerdos comerciales o de cualquiera otra índole que se llevan a cabo por su medio y la confidencialidad de éstos, son todos bienes jurídicos protegidos". (Congreso Nacional, 2007).

Del mismo modo, podemos basarnos en la Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales, del 14 de agosto de 2002, y su Reglamento de Aplicación (Decreto No. 335-03). Esta ley define los conceptos de Firma Digital, Certificado Digital y de Documento Digital. (Viafirma, 2019).

En cuanto a firma digital, establece su definición como: "El valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y el texto del mensaje, y que el mensaje inicial no ha sido modificado después de efectuada la transmisión". (Viafirma, 2019).

Del mismo modo, define el Certificado Digital como: "Es el documento digital emitido y firmado digitalmente por una entidad de certificación, que identifica unívocamente a un suscriptor durante el período de vigencia del certificado, y que se constituye en prueba de que dicho suscriptor es fuente u originador del contenido de un documento digital o mensaje de datos que incorpore su certificado asociado". (Viafirma, 2019).

El artículo 6 equipara el documento administrativo físico que requiere firma al documento digital: "Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, se entenderá satisfecho dicho requerimiento en relación con un Documento Digital o un Mensaje de Datos, si éste ha sido firmado digitalmente y la firma digital cumple con los requisitos de validez establecidos en la presente ley". (Viafirma, 2019).

Al mismo tiempo, equipara la Firma Digital a la firma manuscrita siempre que cumpla con todos los requisitos establecidos por el artículo 31 de la ley, es decir:

- Sea única a la persona que la usa. (Viafirma, 2019).
- Esté bajo el control exclusivo de la persona que la usa. (Viafirma, 2019).
- Esté ligada a la información, documento digital o mensaje, de tal manera que, si estos son cambiados, la firma digital es invalidada, y esté conforme a las reglamentaciones adoptadas por el Poder Ejecutivo. (Viafirma, 2019).

El Decreto No. 335-03, reglamento de Aplicación de la Ley, diferencia la Firma Digital de la Firma Electrónica que define como: "Conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, que por acuerdo entre las partes se utilice como medio de identificación entre el emisor y el destinatario de un mensaje de datos o un documento digital y que carece de alguno de los requisitos legales para ser considerado firma digital". (Viafirma, 2019).

Otra base legal que podríamos tomar es la Ley. No 153-98, también conocida como Ley General de Telecomunicaciones, la cual contempla algunos aspectos sobre este tema. (Viafirma, 2019).

2.3.1 Resoluciones destacadas vinculadas al tema

- **Resolución No. 041-13** (6 de junio de 2013): Uso de Mensajes de Datos, Documentos y Firmas Digitales en los Medios de Pagos Electrónicos. (Viafirma, 2019).
- **Resolución No. 025-11** (31 de marzo de 2011): Firmas Digitales, No. 126-02, a los procedimientos aduaneros. (Viafirma, 2019).
- **Resolución No. 135-09** (21 de diciembre de 2009): Norma complementaria a la ley sobre Comercio Electrónico, Documentos y Firmas Digitales, No. 126-

02, para la Integración de la Jurisdicción Inmobiliaria en la Infraestructura de Firma Digital Nacional. (Viafirma, 2019).

- **Resolución No. 033-07** (28 de febrero de 2007): Norma complementaria de la Ley no. 126-02 sobre el Uso de Mensajes de Datos, Documentos y Firmas Digitales en los Medios de Pagos Electrónicos. (Viafirma, 2019).
- **Resolución No. 142-06** (3 de agosto de 2006): Norma complementaria de la ley 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales, relativa a La Protección de los Derechos de los Consumidores y Usuarios. (Viafirma, 2019).
- **Resolución No. 026-06:** Norma Complementaria de la Ley No. 126-02 sobre Comercio Electrónico, Documentos Y Firmas Digitales, relativa a la determinación de la hora en medios electrónicos e internet. (Viafirma, 2019).

2.3.2 Smart Contracts

Antes de hablar de los Smart Contracts o contratos inteligentes, resulta útil definir un contrato: “Un contrato es un pacto o convenio, oral o escrito, entre partes que se obligan sobre una materia o cosa determinada, y a cuyo cumplimiento pueden ser compelidas”. Visto esto, los Smart Contracts son código escrito en un lenguaje de programación determinado, siendo los términos del contrato sentencias y comandos en el código que lo forma, evitando la interpretación al no ser verbal o escrito en el lenguaje que hablamos. (Mereles & Ortellado, 2019).

En el contexto de las cadenas de bloques, los contratos inteligentes son usados para eliminar a los intermediarios, implementando los controles y acciones realizadas por estos. Los Smart Contracts se encuentran almacenados y distribuidos entre los participantes de la cadena de bloques, evitando que exista un único punto de falla y que no sean modificados. Estas características permiten la simplificación de los procesos que intervienen en una

transacción, con el objetivo de ahorrar costos asociados a estos procesos. Un contrato inteligente es creado por uno o más nodos de la red de la cadena de bloques de acuerdo a los términos de uso y condiciones de ejecución, y una vez codificado es almacenado en la misma cadena de bloques. (Bit2Me Academy, 2021).

Como ejemplo, un contrato inteligente puede ser usado para modelar la venta de un bien físico. Vamos a suponer que José es un participante en la cadena de bloques y tiene registrado un vehículo. Roberto es otro participante de la cadena y decide comprar ese vehículo. Se puede generar un contrato inteligente, de modo que cuando se genere una transacción indicando que Roberto le transfiere el dinero correspondiente a José, el contrato puede generar una transacción indicando que la posesión del vehículo pasa de José a Roberto, y para su realización no se estará usando ningún agente de control externo o mediador.

Si luego de la venta, José intenta vender nuevamente su vehículo a otro participante, la acción será rechazada por los participantes de la cadena de bloques, ya que allí mismo el vehículo figura como posesión de Roberto.

Capítulo 3: Marco Metodológico

En este capítulo de nuestro proyecto estaremos abordando el tipo de investigación que realizaremos, los instrumentos y las técnicas de recolección de los diferentes datos que debemos recopilar. En el mismo sentido, definiremos la forma en que procesaremos y presentaremos los datos, detallando las técnicas y herramientas utilizadas para analizar e interpretar los resultados obtenidos.

3.0 Tipo de investigación (metodología)

En base a la problemática que hemos planteado, consideramos que nuestro proyecto entra dentro del tipo de metodología conocida como “investigación aplicada”. Se trata de un tipo de investigación centrada en encontrar mecanismos o estrategias que permitan lograr un objetivo concreto, que en este caso es proteger los documentos emitidos de forma digital. En esta investigación el ámbito en que se aplica es bien específico y bien delimitado, ya que estamos tratando de abordar un problema específico.

Debemos de cumplir con lo anteriormente planteado, por tanto, se deben tomar en consideración los datos que vamos a recolectar, cómo recolectarlos y cómo analizarlos. Dicho esto, y partiendo de nuestros objetivos, es fundamental elegir una metodología de investigación adecuada para cumplir con esos requisitos. Para esto, lo ideal sería elegir una metodología de investigación mixta, es decir, combinar la posibilidad de obtener la percepción u opinión de un grupo de personas utilizando la metodología cualitativa, con la posibilidad de obtener datos estadísticos concretos usando la metodología cuantitativa. Eso nos va a proporcionar una imagen más rica de los datos obtenidos, con lo cual les podremos sacar mucha más utilidad.

Habiendo sentado esa línea de investigación, podremos obtener en nuestra encuesta datos estadísticos sobre el número de casos de fraude de los que tiene conocimiento nuestra muestra encuestada, y, al mismo tiempo, obtener su opinión acerca del valor de nuestra

implementación y si la consideran una mejora respecto a la emisión de documentos en formato físico.

3.1 Método

Tenemos claro que debemos realizar una investigación cuantitativa de casos de falsificación de documentos, para poder clasificar los casos dependiendo del tipo de documento, de la magnitud de la falsificación y de otros factores que serán analizados posteriormente.

De igual manera, debemos de realizar una investigación cualitativa para poder obtener datos descriptivos sobre los procesos que vamos a estar investigando y cambiando. También debemos investigar sobre las formas en las que vamos a implementar nuestra plataforma y buscar los mejores mecanismos para que el cliente (en este caso, nuestra universidad), pueda implementarla sin inconvenientes y que pueda sacar grandes beneficios de nuestra plataforma.

3.2 Investigación Preliminar

Teniendo ya claro el tipo de metodología que estaremos aplicando a nuestro proyecto, debemos dividir nuestra investigación en las partes correspondientes. Debemos comenzar con una parte exploratoria, donde ya hemos visto de forma superficial los conceptos básicos de la tecnología de cadena de bloques, su funcionamiento y las diferentes aplicaciones o usos que se le han dado a esta tecnología. En esta parte exploratoria debemos investigar sobre los casos y las formas en la que se han falsificado documentos en nuestro país, y sobre los desenlaces finales de esos casos.

Luego en la parte descriptiva debemos describir el funcionamiento de los diferentes componentes de la tecnología, para que sirven y la importancia que tiene cada uno dentro del esquema de la cadena de bloques. Para culminar, en la parte explicativa de la investigación

preliminar debemos explicar el funcionamiento básico de nuestra plataforma y la manera en la que se realizaría la implementación.

3.3 Delimitación del problema

3.3.1 Área geográfica

Este proyecto está pensado para implementarse inicialmente en la Universidad Iberoamericana, por lo que el área geográfica estaría limitada al Distrito Nacional.

3.3.2 Tiempo

Entre el final del seminario de investigación y la entrega del proyecto de grado disponemos de alrededor de 4 meses para realizar la entrega de nuestro proyecto.

3.3.3 Población y muestra

Uno de los objetivos principales de la investigación es determinar la cantidad de casos de fraude de los que haya oído nuestra población. Del mismo modo queremos saber su opinión acerca del valor y la mejora que supondría nuestra plataforma a comparación con los documentos físicos. Dicho esto, la población para este estudio sería una mezcla entre estudiantes universitarios y personas que ya terminaron sus estudios universitarios o que trabajen en alguna universidad.

La fórmula para calcular el tamaño de la muestra es la siguiente:

$$n = \frac{Z^2 . p . q . N}{NE^2 + Z^2 \ p . q .}$$

Z=Nivel de confianza
N=Población-Censo
p= Probabilidad a favor
q= Probabilidad en contra
e= error de estimación
n= Tamaño de la muestra

Figura 3.1. Ilustración de la fórmula para calcular el tamaño de la muestra (Kenfield, 2018)

Nuestros valores serían los siguientes:

Margen de error: 5%

Nivel de confianza: 90%

Población: 340, no tomaremos en cuenta los 5000 estudiantes activos de UNIBE, ya que no todos solicitan documentos constantemente. Tomaremos un número de 340 como un promedio de solicitudes cada cuatrimestre entre estudiantes y egresados.

El tamaño de la muestra (n) es calculado de acuerdo con la fórmula: $n = [z2 * p * (1 - p) / e^2]$ / $[1 + (z^2 * p * (1 - p) / (e^2 * N))]$

Donde: z = 1.645 para un nivel de confianza (α) de 90%, p = proporción (expresado como decimal), N = tamaño de la población y e = margen de error.

z = 1.645, p = 0.5, N = 340, e = 0.05

n = [1.6452 * 0.5 * (1 - 0.5) / 0.052] / [1 + (1.6452 * 0.5 * (1 - 0.5) / (0.052 * 340))]

n = 270.6025 / 1.7959 = 150.679

n ≈ 151

El tamaño de la muestra es igual a **151** personas.

3.3.4 Técnicas e instrumentos

Para realizar la recolección de datos en nuestra investigación preliminar, además de las fuentes de datos, tendremos que realizar encuestas destinadas al público en general para ver cuantas personas han oído o saben de un caso similar.

3.3.5 Técnicas de procesamiento y análisis de datos

Ya que los datos cuantitativos (respuestas de las encuestas) serán obtenidos a través de herramientas como Google Forms, podremos tener los datos con un formato ya definido, por lo que su análisis será mucho más fácil de realizar. Para analizar los datos podríamos utilizar ciertos componentes de lenguajes de programación como Python o R, y en el mismo sentido, combinar estos componentes con herramientas visualizadoras de datos como Power

BI o Tableau, donde se pueden presentar los datos de una forma sencilla y en la que cualquier persona que vea los datos podrá entender de qué se está hablando.

3.3.6 Fuentes de datos

Como fuente de datos principal, utilizaremos artículos y publicaciones alojadas en la web, lo cual combinado con noticias detalladas sobre los casos de falsificación y los conceptos fundamentales del Blockchain nos servirán como un gran apoyo para la realización de nuestro proyecto, ya que nos van a proporcionar toda la información que necesitamos para llevar a cabo los diferentes análisis que necesitaremos tanto para establecer los fundamentos de la plataforma como para definir todos los aspectos o módulos que han de ser tomados en cuenta en la implementación.

Otra fuente de datos será la propia encuesta, la cual nos dará datos estadísticos sobre la dimensión de la problemática que tenemos como objetivo resolver. Además, nos dará información cualitativa sobre la opinión de los encuestados acerca de la migración de los documentos físicos a los documentos digitales verificados por Blockchain y del valor que le dan a la implementación de nuestra plataforma.

Del mismo modo, la Universidad Iberoamericana nos servirá como fuente de datos, ya que debemos replicar la estructura de algunos de los documentos que emite e integrarlas en nuestra plataforma. También hemos identificado la oportunidad de utilizar las documentaciones de las aplicaciones similares que mencionamos en el capítulo 2, tomando de ellas todos los aspectos positivos que puedan integrarse a nuestro proyecto, contribuyendo así a evitar cometer algún error en el desarrollo del prototipo.

UNIBE también nos va a proporcionar datos sobre el proceso actual de emisión de documentos, lo cual nos va a servir para poder entender a fondo las diferentes fases que se agotan en el proceso y para poder ofrecer ventajas comparativas con nuestra plataforma.

Capítulo 4: Plan de mercadeo y Análisis del entorno

4.1 Benchmarking

Para realizar el Benchmarking de nuestra plataforma, la cual para los fines del prototipo hemos llamado “DocBlock”, procederemos a comparar las funcionalidades que tendrá con las funcionalidades de eTítulo, aplicación anteriormente mencionada y que fue desarrollada por la empresa española SIGNE.

Tabla 4.1.

Benchmarking entre DocBlock y eTítulo.

Funcionalidades	**DocBlock**	**eTítulo**
Tracking de las solicitudes realizadas	✓	x
Red propia a la que la Universidad tiene acceso	✓	x
Firma digital	✓	✓
Historial de documentos solicitados	✓	x

Nota. Fuente: Elaboración Propia.

4.2 Mecanismo para poblar de información al sistema

Para alimentar de datos a nuestra plataforma utilizaremos las bases de datos de las propias universidades en las que estaremos implementando DocBlock. Al momento de la presentación de nuestro proyecto estaremos utilizando una simulación de la base de datos de UNIBE, con tablas como Estudiantes y Asignaturas.

Además de esto se propone crear una nueva tabla en la base de datos, donde se puedan procesar las solicitudes que entran a la plataforma, de modo que se puedan visualizar además de en la plataforma, en herramientas de análisis de datos o de inteligencia de negocios como Power BI o la herramienta Tableau. Además de la información, tomaremos de UNIBE las plantillas y diseños de los documentos que emite la administración universitaria,

para así poder replicarlos en nuestra plataforma de la manera más parecida posible a como se emiten en la actualidad en el formato físico.

4.3 Modelo de negocio (Método Canvas)

Tabla 4.2.

Modelo de negocio usando el Método Canvas.

<table>
<tr><td rowspan="2">Socios Claves

En principio para nuestra tesis, nuestro principal socio sería nuestra Universidad Iberoamericana (UNIBE).</td><td>Actividades claves

Recepción de solicitudes de documentos universitarios.

Posterior emisión y certificación de los documentos.</td><td rowspan="2">Propuesta de valor

Emisión de documentos universitarios certificados utilizando la tecnología Blockchain.</td><td>Relación con el cliente

Tendremos una relación directa con los usuarios a través de la plataforma.</td><td rowspan="2">Segmento de clientes

Estudiantes universitarios que quieran obtener documentos certificados y validados por Blockchain.</td></tr>
<tr><td>Recursos claves
Una computadora, o un dispositivo inteligente (celulares o tabletas) con acceso a Internet.</td><td>Canales
Plataforma web.</td></tr>
<tr><td colspan="3">Estructura de coste
Una vez desarrollada e implementada la plataforma, el principal coste sería el posterior mantenimiento y las distintas actualizaciones que tendrían que hacerse en nuestra plataforma.</td><td colspan="2">Fuente de ingreso
Si la administración de UNIBE decide implementar nuestro proyecto de grado, ellos serían el principal apoyo y fuente de ingreso para la consecución de la implementación.</td></tr>
</table>

Nota. Fuente: Elaboración Propia.

4.4 Presupuesto

Tabla 4.3.

Presupuesto del proyecto.

	Tarea	Horas de trabajo	Costo total	A facturar
Partida	**Tarea**	**Horas**	**RD$**	**Total**
Investigación	Acercamiento inicial al personal UNIBE	**2.00**	760.00	896.80
	Entrevistas y encuestas	**10.00**	3,800.00	4,484.00
Análisis	Análisis funcional	**16.00**	18,560.00	21,900.80
	Diagrama de flujo	**8.00**	9280.00	10,950.40
	Diseño base de datos	**12.00**	13,920.00	16,425.60
	Diseño de políticas de acceso	**20.00**	23,200.00	27,376.00

	Especificaciones generales de infraestructura y programa	**6.00**	6,960.00	8,212.80
Desarrollo	Desarrollo de Front-End Web	**60.00**	69,600.00	82,128.00
	Desarrollo Front-End Mobile	**20.00**	23,200.00	27,376.00
	Desarrollo Back-end API	**40.00**	46,400.00	54,752.00
	Configuración de infraestructura	**20.00**	23,200.00	27,376.00
	Desarrollo de contratos inteligentes	**40.00**	46,400.00	54,752.00
	Integración de infraestructura con API y Front-End	**20.00**	23,200.00	27,376.00
Costos de operación	Registro Dominio/Hosting Privado/Licencia de Mantenimiento	**Mensual**	40,000.00	47,200.00
Subtotal		**274 horas**	317,840.00	375,051.20
Honorarios	Gastos administrativos	**18% ITBIS**	57,211.20	67,509.22
Total				442,560.42

Nota. Fuente: Elaboración Propia.

4.5 Retorno de la inversión

Asumimos que la inversión sería retornada en alrededor de 1 año ya que la verificación por Blockchain se volvería un estándar, y casi todos los estudiantes querrán tener sus documentos verificados. Además, las instituciones, especialmente UNIBE, podrán reducir los costes de papel y de energía eléctrica, y la productividad del personal aumentará en gran medida al no tener que dedicar tiempo a la verificación y manipulación de los documentos emitidos por la institución.

En el caso de la implementación en otras instituciones, puede variar el precio de la instalación. Dado que las instituciones tienen sus propios procesos y necesidades, cualquier actualización del Blockchain requerirá amplias pruebas y validaciones entre las entidades.

En el caso particular de la implementación en UNIBE, si estuviéramos cobrando estimamos una inversión inicial de $7,902.86 USD, con una ganancia aproximada de $20,000.00 USD. Por tanto, utilizando la fórmula del retorno de la inversión, tendríamos lo siguiente:

ROI = (Ganancia - Inversión) / Inversión

ROI = (20000 - 7902.86) / 7902.86

ROI = 1.53

Habiendo calculado con la fórmula, el retorno esperado de la inversión (ROI) es de aproximadamente 153.09%. Se prevé que nuestras ganancias sean de $20,000.00 USD con una inversión de $7,902.86 USD.

Capítulo 5: Análisis, presentación de resultados y Conclusiones

5.1 Encuestas

Resulta de vital importancia realizar una encuesta para determinar el impacto que ha llegado a tener la problemática que estamos tratando en nuestro proyecto de grado. Esta serie de preguntas estuvieron destinadas al público en general, pero hemos puesto especial atención a personas que laboren o estudien en alguna universidad, para así poder identificar el grado de ocurrencia que ha tenido la falsificación de documentos universitarios. Luego de tener la aprobación del Comité de Ética de Investigación (CEI), procedimos a poner en circulación la siguiente encuesta:

5.1.1 ¿Es usted estudiante universitario? Con esta pregunta buscamos identificar el lugar que ubica el encuestado en el mundo universitario.

5.1.2 En caso de no ser estudiante, ¿trabaja usted en alguna universidad? Se persigue el mismo objetivo que con la primera pregunta.

5.1.3 ¿Es usted egresado de una institución de educación superior? Se busca lo mismo que en las dos primeras preguntas.

5.1.4 ¿Considera que el proceso de emitir documentos académicos es burocrático (tarda mucho tiempo)? Buscamos obtener la opinión de los encuestados en cuanto al nivel de burocracia para obtener los documentos universitarios.

5.1.5 ¿Ha sido testigo de un caso de falsificación de documentos universitarios? Buscamos saber si el encuestado ha sido testigo directo de un caso de esta índole.

5.1.6 En caso negativo, ¿Ha escuchado de algún caso similar? Se busca ver si el encuestado ha oído de algún caso de este tipo.

5.1.7 ¿Sabes si había personas a lo interno de la institución involucradas en el hecho? Queremos ver si hubo complicidad dentro de la entidad donde ocurrió el hecho.

5.1.8 ¿El documento falsificado fue digital o físico? Queremos saber a través de qué medio se cometió el fraude.

5.1.9 ¿Hubo algún tipo de sanción? Buscamos saber si hubo consecuencias.

5.1.10 ¿Sabes cómo se descubrió la falsificación? Queremos saber la forma en la que descubrió el hecho.

5.1.11 ¿Sabes si han tomado medidas en el lugar del hecho para prevenir que suceda otra vez? Esta pregunta es fundamental para nosotros, ya que dependiendo si han implementado o no medidas de prevención, nuestro proyecto podría ser una gran solución.

5.1.12 ¿Cuál considera que es más vulnerable a la falsificación, el documento digital (cifrado) o el documento físico? Esta pregunta trata de determinar hasta qué punto los usuarios consideran que los documentos digitales son vulnerables en comparación con los físicos.

5.1.13 En caso de haber seleccionado el digital (cifrado), si existiera un método más seguro para emitir documentos de esta manera, ¿optaría por este medio? Queremos saber si el usuario utilizará los documentos digitales en lugar de los físicos si lo considera más seguro.

5.1.14 Independientemente de su vulnerabilidad, ¿cuál es más conveniente? Queremos saber qué es lo que la mayoría de los usuarios considera más conveniente para sus vidas.

5.1.15 ¿Cree que los documentos digitales son beneficiosos para el medio ambiente? Dado que el cambio climático es un tema importante en esta época, queremos saber si tienen un conocimiento previo de los beneficios de los documentos digitales para el clima.

5.1.16 ¿Cree que tener los documentos en formato digital(cifrados) es más eficiente que tenerlos en formato físico? Queremos conocer la opinión del encuestado respecto a la eficiencia de los documentos digitales frente a los físicos.

5.1.17 Sugerencias del encuestado. Buscamos conocer cualquier tipo de sugerencia que tenga el encuestado respecto a la implementación de nuestro proyecto.

5.2 Verificación y Evaluación de Objetivos

5.2.1 Verificación de Objetivo General

El objetivo principal de nuestro proyecto es brindar una herramienta que transforme la manera en la que son emitidos los documentos universitarios, dándole mucha más seguridad a la emisión digital de los mismos y contribuyendo a facilitar el proceso tanto para la universidad como para el estudiante. Al realizar la encuesta y analizar los resultados, encontramos que un 59.6% de los encuestados entiende que los documentos físicos son más vulnerables a la falsificación que los digitales. Además, un 72.3% estaría dispuesto a utilizar exclusivamente documentos digitales si estos tuvieran mecanismos de protección de la información tales como la firma digital y el estar respaldados por la cadena de bloques.

Apoyándonos en estos datos, procedimos a desarrollar nuestro prototipo, el cual es una plataforma que permite la emisión y posterior validación de documentos universitarios utilizando la tecnología de la cadena de bloques. Para ver los detalles del cumplimiento de este objetivo, se debe verificar el capítulo 6.

De resultar exitosa nuestra implementación, comprobaremos que nuestro objetivo general estaría cumplido, ya que la mayoría de los estudiantes optarían por realizar la transición de los documentos físicos a los documentos digitales. Por tanto, estaríamos logrando impulsar una transformación en el proceso de emisión de documentos universitarios y en la administración universitaria en general.

5.2.2 Verificación de Objetivos Específicos

Objetivo 1. **Desarrollar e implementar una plataforma de validación de documentos utilizando Blockchain.** Este objetivo se cumplió totalmente, ya que desarrollamos nuestro prototipo siendo fieles a que el fundamento de la plataforma fuera el Blockchain. Para ver los detalles, se debe leer el capítulo 6.

Objetivo 2. **Ayudar a combatir la falsificación de documentos.** Una de las características principales de DocBlock es que hace casi imposible que se falsifique un documento emitido por esta plataforma. Para ver los detalles de los mecanismos utilizados, se debe leer el capítulo 6.

Objetivo 3. **Facilitar la emisión de documentos digitales.** A través de nuestra plataforma, el usuario solicitante obtiene sus documentos directamente en su correo electrónico en menos de 2 minutos, por lo que el proceso resulta bastante fácil. Para ver el funcionamiento, se debe verificar el capítulo 6.

Objetivo 4. **Aumentar el nivel de confianza en los documentos digitales.** Cuando los usuarios conozcan y entiendan el funcionamiento de la cadena de bloques verán que es uno de los métodos más seguros para asegurar la información. Esto se puede ver en la parte de validación de documentos de nuestra plataforma, donde se verifica la autenticidad del documento a través de la firma digital y del hash identificador en el Blockchain. Esto se puede ver a profundidad en el capítulo 6.

5.3 Conclusiones

A través de esta investigación validamos que el uso del Blockchain aplicado a la emisión de documentos digitales aumenta los niveles de seguridad de la información que contienen y proporciona un gran mecanismo para poder confirmar la autenticidad de los mismos. En base a estos grandes beneficios y al análisis de los resultados de nuestra encuesta, podemos concluir que nuestra propuesta puede implementarse de manera satisfactoria y que sería vista con buenos ojos por la mayoría de la población estudiantil.

5.4 Líneas futuras de investigación

Todo producto o solución, especialmente en el área de la tecnología es siempre mejorable, por lo que resulta fundamental mantenerlo actualizado con las nuevas tecnologías que van surgiendo, esto con el fin de poder satisfacer las nuevas necesidades que puedan tener los usuarios de nuestra plataforma.

Dicho esto, hemos identificado ciertas áreas en las cuales podemos investigar para mejorar y enriquecer su funcionamiento. Entre esas líneas de investigación, pudimos identificar las siguientes:

- **Interoperabilidad entre instituciones.** Se refiere a la capacidad del contrato inteligente de compartir datos y utilizar datos anteriores entre los contratos de otras instituciones. Esto mejora la programabilidad y abre la posibilidad de coordinar acciones inteligentes basadas en la validez de los documentos en la cadena de bloques.
- **Permitir las firmas múltiples.** Permite que los decanos, el personal académico y otras autoridades firmen conjuntamente los contratos y garanticen la verificación del contrato entre departamentos.
- **Identidad digital de los estudiantes en la cadena de bloques.** Incluir la identificación de los estudiantes en la cadena de bloques aumenta la seguridad, ya que la suplantación de identidad será casi imposible. Los estudiantes pueden utilizarla para garantizar su identidad sea dentro del programa o en físico, abriendo un sinnúmero de beneficios como la digitalización de los procesos académicos.

Capítulo 6: Análisis y Diseño del Prototipo

6.1 Narrativa General

6.1.1 Objetivos de la Institución, Empresa o Sector al que está dirigido el Proyecto

Este prototipo en concreto va dirigido a la Universidad Iberoamericana, la cual tiene dentro de sus objetivos ser una institución de educación superior innovadora, que sea inclusiva y que está en constante desarrollo, que anticipa y actúa frente a las cambiantes necesidades educativas, y propicia un impacto positivo en la sociedad.

6.1.2 Breve descripción del sistema propuesto

Nuestra plataforma de verificación de documentos (DocBlock) consiste en una solución web para certificar los documentos universitarios utilizando la tecnología de la cadena de bloques.

6.1.3 Objetivos del sistema

El objetivo principal de nuestro proyecto es ofrecer una solución web a nuestra universidad para que los estudiantes puedan solicitar y obtener cualquier documento universitario que requieran de forma digital y certificado utilizando la tecnología de Blockchain. De este modo los estudiantes podrán obtener versiones digitales de sus documentos estando estos certificados utilizando la tecnología de la cadena de bloques, y al mismo tiempo, en caso de que un egresado esté aplicando a un empleo, el departamento de recursos humanos de la empresa en la que aplique, podrá validar la autenticidad de un título universitario a través de nuestra plataforma.

6.1.4 Innovaciones del sistema propuesto

Sería el primer sistema en universidades del país en ofrecer la validación de la totalidad de sus documentos a través del Blockchain. Además, se van a utilizar múltiples tecnologías relativamente nuevas, las cuales son detalladas en el apartado de tecnologías a usarse.

6.1.5 Ventajas / Beneficios

- La plataforma permitirá eficientizar el tiempo de respuesta con el que se responden las solicitudes de los estudiantes.
- Aumenta la facilidad para la obtención de los documentos.
- Protege los documentos de posibles falsificaciones.
- La plataforma tendrá un módulo dedicado a que personas externas (como el departamento de recursos humanos de una empresa) puedan verificar la autenticidad de los documentos.

6.2 Análisis FODA del Sistema Propuesto

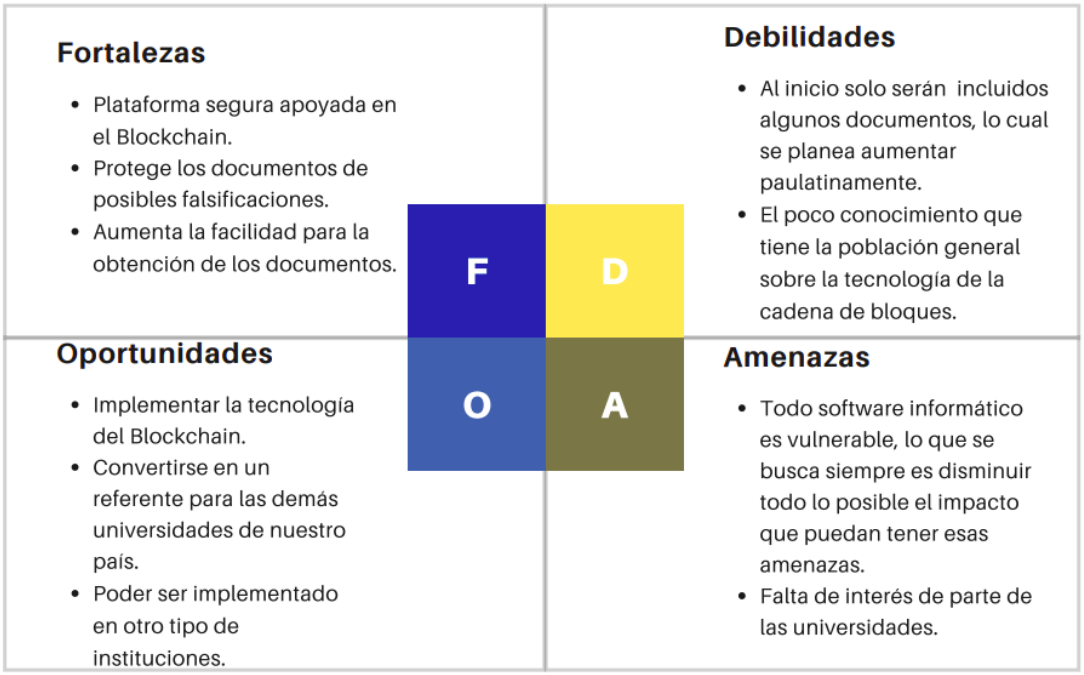

Figura 6.1. Análisis FODA de DocBlock. (Elaboración Propia).

6.3 Análisis funcional del sistema

Dependiendo del tipo de usuario, nuestra plataforma contiene las siguientes funcionalidades:

- Para los usuarios con el rol de administrador, se cuenta con un back - office, el cual contiene las siguientes funcionalidades:
    - Dashboard que contiene datos estadísticos sobre el número de estudiantes registrados, las solicitudes recibidas, los documentos emitidos, los documentos fallidos y el tiempo promedio para emitir documentos dentro de la plataforma.
    - A este Dashboard se le puede aplicar un filtro donde se indica el rango de fecha deseado.
    - Del mismo modo se cuenta con el módulo de “Usuarios”, el cual permite añadir usuarios dentro de la plataforma. Además, permite editar datos de los usuarios luego de que han sido creados.
- Para los usuarios con el rol de estudiante, se cuenta con las siguientes funcionalidades:
    - Contamos con el módulo de pago de servicios, desde donde se solicitan los documentos a ser emitidos por la plataforma. Desde ahí se puede elegir entre los diferentes documentos que se ofrezcan dentro de la plataforma. Para este prototipo solo se está ofreciendo el récord de notas.
    - Una simulación del pago del servicio, donde el estudiante inserta su método de pago y culmina el proceso para solicitar el documento.
    - Una vez validado el pago, el estudiante podrá ver el estado de su documento en el apartado de “Mis Documentos”. Una vez emitido, el estado de la solicitud cambiará a “Enviado al correo”, y efectivamente el usuario recibirá el

documento solicitado directamente a su correo electrónico. Este apartado guardará el historial de solicitudes que haga el estudiante.

- Del mismo modo se cuenta con el módulo de “Verificar Documentos”, desde donde el usuario puede verificar la validez del documento recibido. A este módulo también pueden acceder personas externas que no tengan usuario dentro de la plataforma, esto con el objetivo de que empresas puedan comprobar la autenticidad de un documento presentado por un estudiante de UNIBE.
- En caso de que se tenga el documento impreso, se puede confirmar su autenticidad escaneando el código QR, el cual lleva al módulo de verificación y muestra una copia digital del mismo documento.

6.4 Diagramas de flujo de los procesos

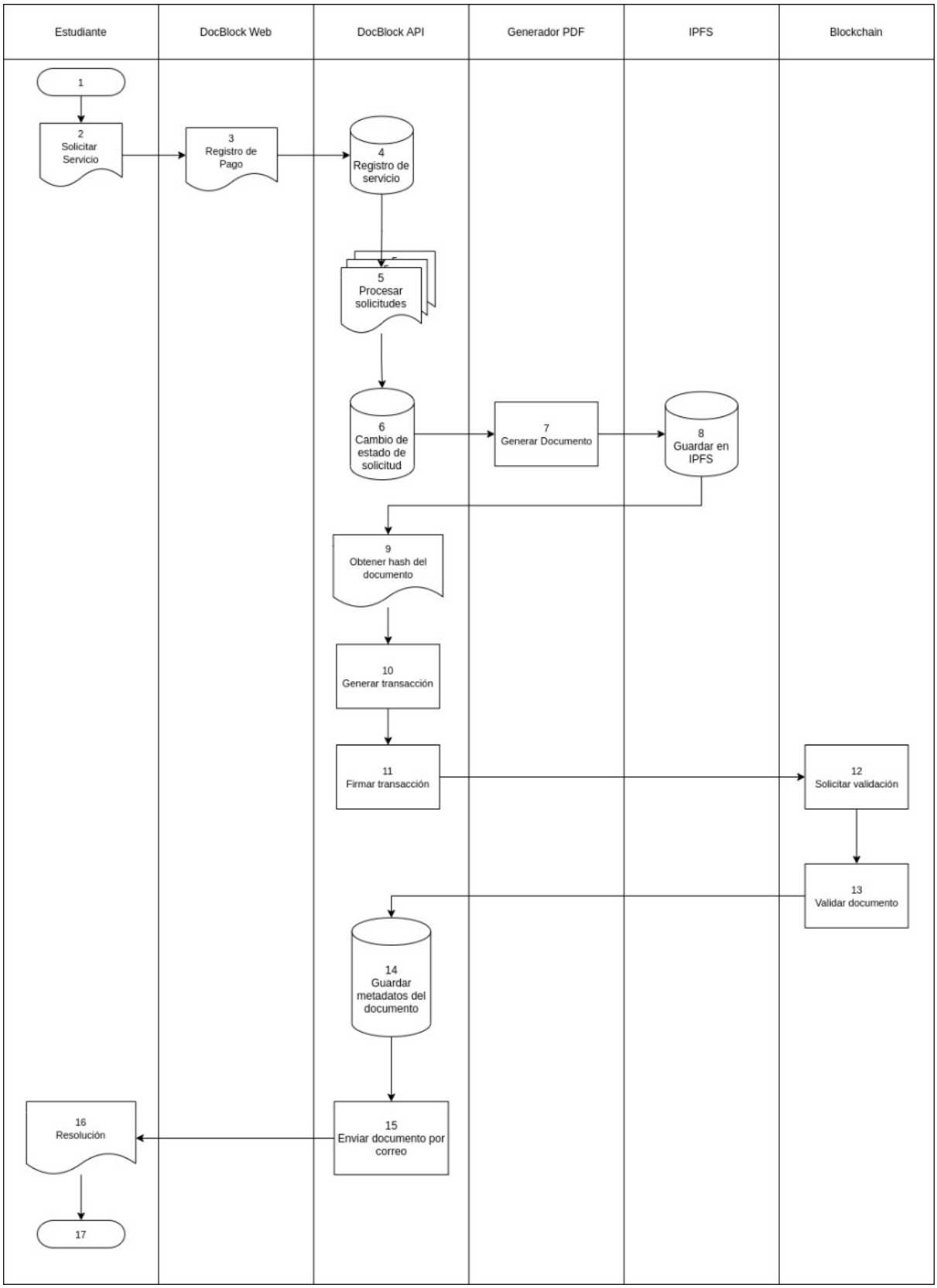

Figura 6.2. Diagrama de flujo del proceso para emitir un documento. (Elaboración Propia).

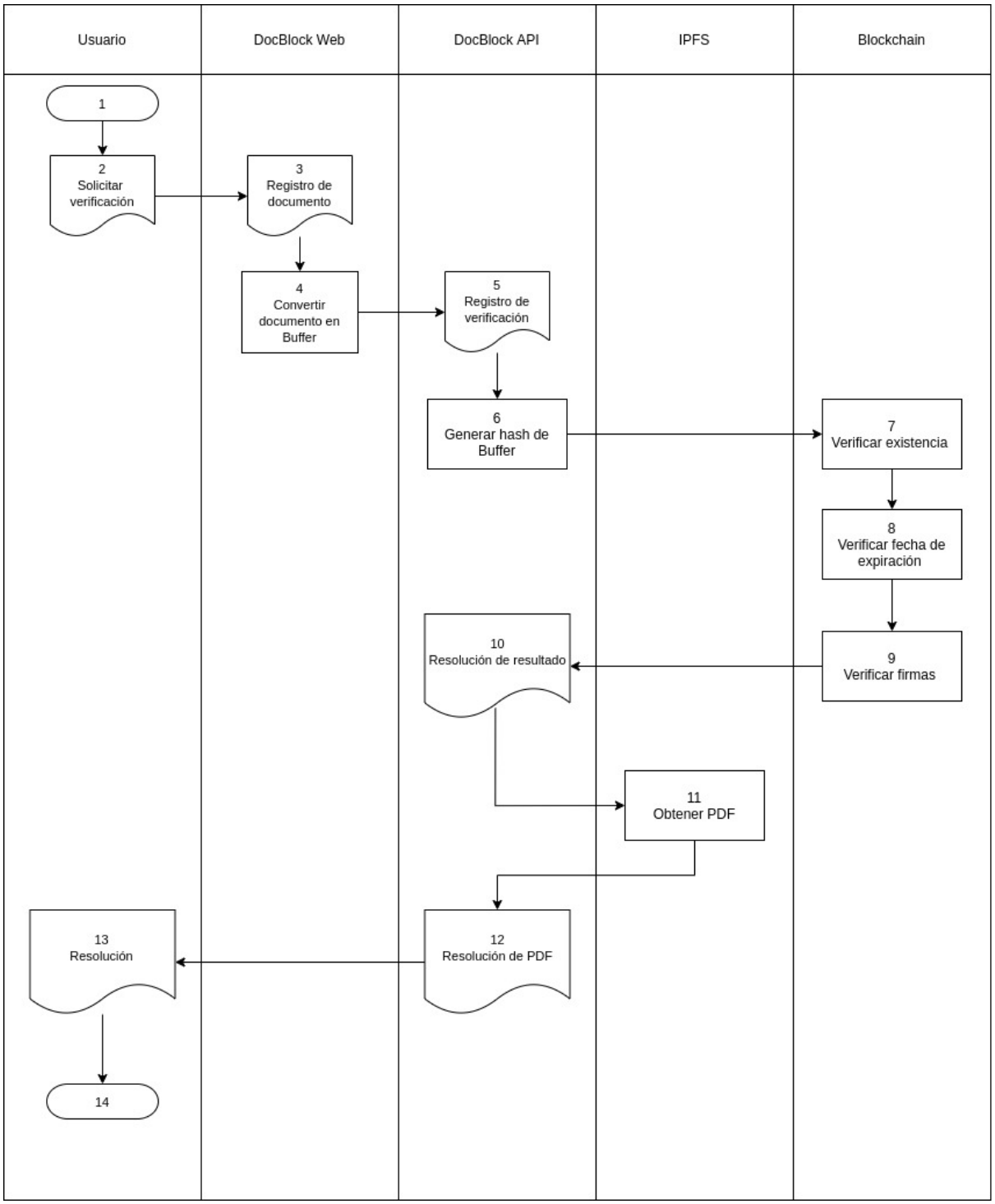

Figura 6.2.1 Diagrama de flujo del proceso para verificar un documento.

(Elaboración Propia).

6.5 Diagrama de Flujo de Datos (DFD) del sistema propuesto

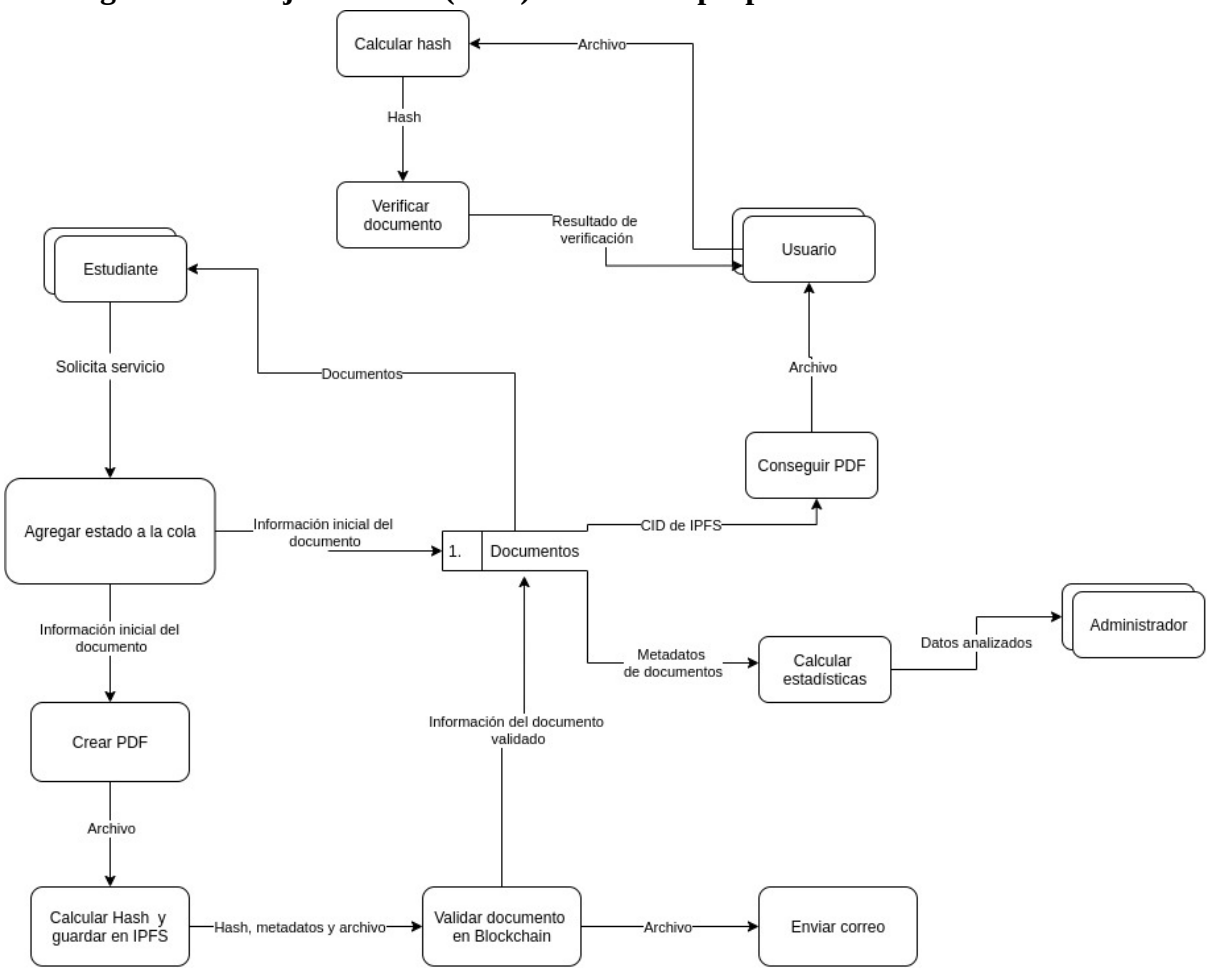

Figura 6.3. Diagrama de flujo de datos del sistema. (Elaboración Propia).

6.6 Diseño de la Base de Datos

6.6.1 Esquema de la base de datos

En este apartado colocaremos los scripts, ya que en el diagrama entidad - relación, también se puede apreciar el esquema de la base de datos.

```
-- CreateEnum
CREATE TYPE "Role" AS ENUM ('User', 'Admin');

-- CreateEnum
CREATE TYPE "DocumentStatus" AS ENUM ('Preparing', 'InProgress', 'Ready', 'Failed');

-- CreateEnum
CREATE TYPE "DocumentType" AS ENUM ('NoteRecord');

-- CreateTable
CREATE TABLE "User" (
    "id" SERIAL NOT NULL,
    "username" TEXT NOT NULL,
    "email" TEXT NOT NULL,
    "role" "Role" NOT NULL,
    "createdAt" TIMESTAMP(3) NOT NULL DEFAULT CURRENT_TIMESTAMP,
    "updatedAt" TIMESTAMP(3) NOT NULL,

    PRIMARY KEY ("id")
);

-- CreateTable
CREATE TABLE "Login" (
    "id" SERIAL NOT NULL,
    "userId" INTEGER NOT NULL,
    "hash" TEXT NOT NULL,

    PRIMARY KEY ("id")
);
```

Figura 6.4. Script usado para la creación de las tablas en la base de datos.

(Elaboración Propia).

```sql
-- CreateTable
CREATE TABLE "Profile" (
    "id" SERIAL NOT NULL,
    "firstName" TEXT NOT NULL,
    "lastName" TEXT NOT NULL,
    "faculty" TEXT NOT NULL,
    "identification" TEXT NOT NULL,
    "countryOfBirth" TEXT NOT NULL,
    "cityOfBirth" TEXT NOT NULL,
    "birthDate" TIMESTAMP(3) NOT NULL,
    "userId" INTEGER NOT NULL,

    PRIMARY KEY ("id")
);

-- CreateTable
CREATE TABLE "Student" (
    "id" SERIAL NOT NULL,
    "code" TEXT NOT NULL,
    "course" TEXT NOT NULL,
    "school" TEXT NOT NULL,
    "admissionDate" TIMESTAMP(3) NOT NULL,
    "userId" INTEGER NOT NULL,

    PRIMARY KEY ("id")
);
```

Figura 6.5. Script usado para la creación de las tablas en la base de datos.

(Elaboración Propia).

```sql
-- CreateTable
CREATE TABLE "Document" (
    "id" SERIAL NOT NULL,
    "userId" INTEGER,
    "status" "DocumentStatus" NOT NULL,
    "type" "DocumentType" NOT NULL,
    "createdAt" TIMESTAMP(3) NOT NULL DEFAULT CURRENT_TIMESTAMP,
    "updatedAt" TIMESTAMP(3) NOT NULL,
    "emissionDate" TIMESTAMP(3),
    "dataHash" TEXT,
    "hash" TEXT,
    "expiryDate" INTEGER,
    "validators" TEXT[],
    "creator" TEXT,
    "transactionHash" TEXT,
    "cid" TEXT,

    PRIMARY KEY ("id")
);

-- CreateIndex
CREATE UNIQUE INDEX "User.username_unique" ON "User"("username");

-- CreateIndex
CREATE UNIQUE INDEX "Login_userId_unique" ON "Login"("userId");

-- CreateIndex
CREATE UNIQUE INDEX "Profile_userId_unique" ON "Profile"("userId");

-- CreateIndex
CREATE UNIQUE INDEX "Student.code_unique" ON "Student"("code");

-- CreateIndex
CREATE UNIQUE INDEX "Student_userId_unique" ON "Student"("userId");
```

Figura 6.6. Script usado para la creación de las tablas en la base de datos.

(Elaboración Propia).

```
94   CREATE UNIQUE INDEX "Document.dataHash_unique" ON "Document"("dataHash");
95
96   -- CreateIndex
97   CREATE UNIQUE INDEX "Document.hash_unique" ON "Document"("hash");
98
99   -- AddForeignKey
100  ALTER TABLE "Login" ADD FOREIGN KEY ("userId") REFERENCES "User"("id") ON DELETE RESTRICT ON UPDATE CASCADE;
101
102  -- AddForeignKey
103  ALTER TABLE "Profile" ADD FOREIGN KEY ("userId") REFERENCES "User"("id") ON DELETE RESTRICT ON UPDATE CASCADE;
104
105  -- AddForeignKey
106  ALTER TABLE "Student" ADD FOREIGN KEY ("userId") REFERENCES "User"("id") ON DELETE RESTRICT ON UPDATE CASCADE;
107
108  -- AddForeignKey
109  ALTER TABLE "Document" ADD FOREIGN KEY ("userId") REFERENCES "User"("id") ON DELETE SET NULL ON UPDATE CASCADE;
110
```

Figura 6.7. Script usado para la creación de las tablas en la base de datos.

(Elaboración Propia).

6.6.2 Diagrama Entidad - Relación

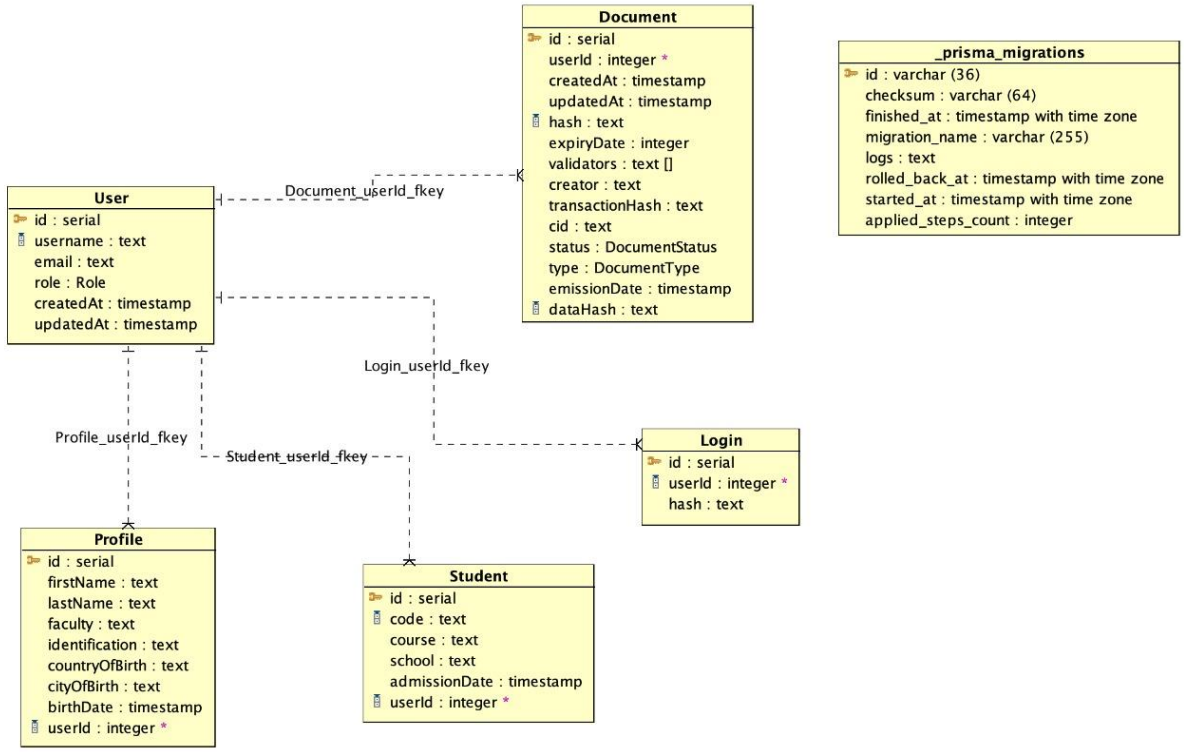

Figura 6.8. Diagrama de Entidad - Relación de DocBlock. (Elaboración Propia).

6.6.3 Diccionario de datos del sistema

El diccionario de datos del sistema es fundamental para poder entender su funcionamiento. Para definirlo, mencionaremos todos los campos de las tablas y no repetiremos campos que son comunes. Este apartado debemos comenzarlo con la tabla de Documentos, la cual guarda todos los documentos emitidos dentro de nuestra plataforma. Consta de los siguientes campos:

- id: representa el número identificador del documento que ha sido emitido.
- userId: representa el número identificador del usuario que solicitó el documento.
- createdAt: representa la fecha en la que se creó el documento.
- updatedAt: representa la fecha en la que se actualizó el documento.
- hash: representa el hash identificador del documento dentro de la cadena de bloques.
- transactionHash: representa el hash identificador de la transacción.
- status: representa el estado del documento.
- type: representa el tipo de documento.
- emissionDate: representa la fecha de emisión del documento.
- creator: representa la persona que inició la emisión del documento en el Blockchain. Normalmente es la universidad o institución.
- validators: representa las firmas de las entidades que emiten documentos.
- cid: representa un id especial para encontrar el documento en el IPFS.

Tabla 6.1.

Tabla de Documentos.

	Key	#	Name	Title	Data type	References	Nullable
	🔑	1	id		integer		☐
		2	userId		integer	User	☑
		5	createdAt		timestamp(3) without time zone)		☐
		6	updatedAt		timestamp(3) without time zone)		☐
		7	hash		text		☑
		8	expiryDate		integer		☑
		9	validators		text[]		☑
		10	creator		text		☑
		11	transactionHash		text		☑
		12	cid		text		☑
		13	status		"DocumentStatus"		☐
		14	type		"DocumentType"		☐
		15	emissionDate		timestamp(3) without time zone)		☑
		16	dataHash		text		☑

Nota. Fuente: Elaboración Propia.

Siguiendo con la construcción del diccionario de datos, pasamos a la tabla del Login, la cual guarda los datos necesarios para ingresar a la plataforma. Consta de los siguientes elementos:

- id: representa el número identificador del login.
- userId: el id del usuario que ha iniciado sesión.

Tabla 6.2.

Tabla de Login.

	Key	#	Name	Title	Data type	References	Nullable
	🔑	1	id		integer		☐
		2	userId		integer	User	☐
		3	hash		text		☐

Nota. Fuente: Elaboración Propia.

Continuando, tenemos la tabla de perfiles, la cual contiene el perfil de los usuarios de la plataforma. Consta de los siguientes campos:

- firstName: indica el nombre del usuario.
- lastName: indica el apellido del usuario.
- faculty: indica la facultad a la que pertenece el usuario.
- identification: indica la cédula del usuario.
- countryOfBirth: indica el país de nacimiento del usuario.
- cityOfBirth: indica la ciudad de nacimiento del usuario.
- birthDate: indica la fecha de nacimiento del usuario.

Tabla 6.3.

Tabla de Perfiles.

	Key	#	Name	Title	Data type	References	Nullable
	🔑	1	id		integer		☐
		2	firstName		text		☐
		3	lastName		text		☐
		4	faculty		text		☐
		6	identification		text		☐
		7	countryOfBirth		text		☐
		8	cityOfBirth		text		☐
		9	birthDate		timestamp(3) without time zone)		☐
		10	userId		integer	User	☐

Nota. Fuente: Elaboración Propia.

Seguimos con la tabla de estudiantes, la cual contiene los datos de los estudiantes registrados en la plataforma. Consta de los siguientes campos:

- code: indica la matrícula del estudiante.
- course: indica la carrera del estudiante.
- school: indica la escuela a la que pertenece el estudiante.
- admissionDate: indica la fecha de admisión del estudiante.

Tabla 6.4.

Tabla de Estudiantes.

	Key	#	Name	Title	Data type	References	Nullable
	🔑	1	id		integer		☐
		2	code		text		☐
		3	course		text		☐
		4	school		text		☐
		5	admissionDate		timestamp(3) without time zone)		☐
		6	userId		integer	User	☐

Nota. Fuente: Elaboración Propia.

Para culminar con el diccionario, pasamos a la tabla de usuarios, la cual contiene los datos de los usuarios registrados en la plataforma. Consta de los siguientes campos:

- username: indica el nombre de usuario.
- email: indica el correo electrónico.
- role: indica el rol que tiene el usuario dentro de la plataforma, ya sea de estudiante o de administrador.

Tabla 6.5.

Tabla de Usuarios.

	Key	#	Name	Title	Data type	References	Nullable
	🔑	1	id		integer		☐
		2	username		text		☐
		3	email		text		☐
		4	role		"Role"		☐
		5	createdAt		timestamp(3) without time zone)		☐
		6	updatedAt		timestamp(3) without time zone)		☐

Nota. Fuente: Elaboración Propia.

6.7 Formato de pantallas para las E/S de datos del sistema

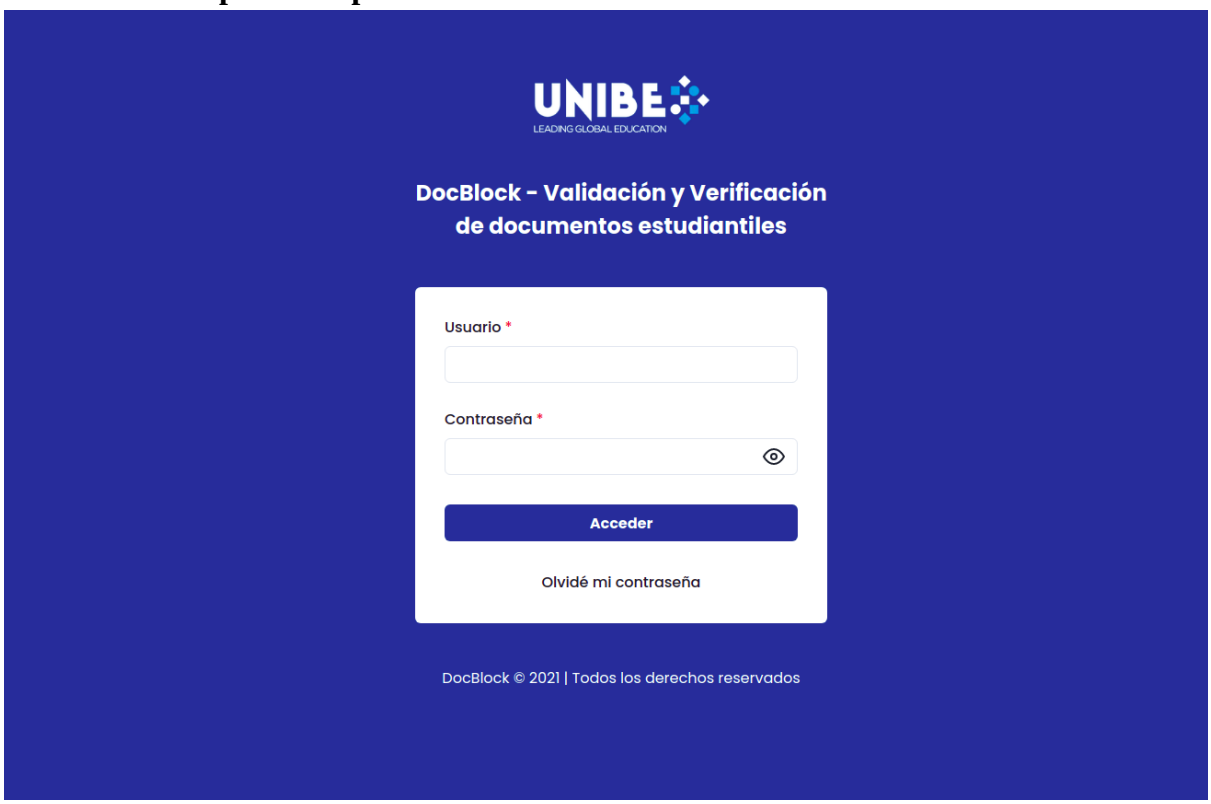

Figura 6.9. Pantalla de Login de DocBlock. (Elaboración Propia).

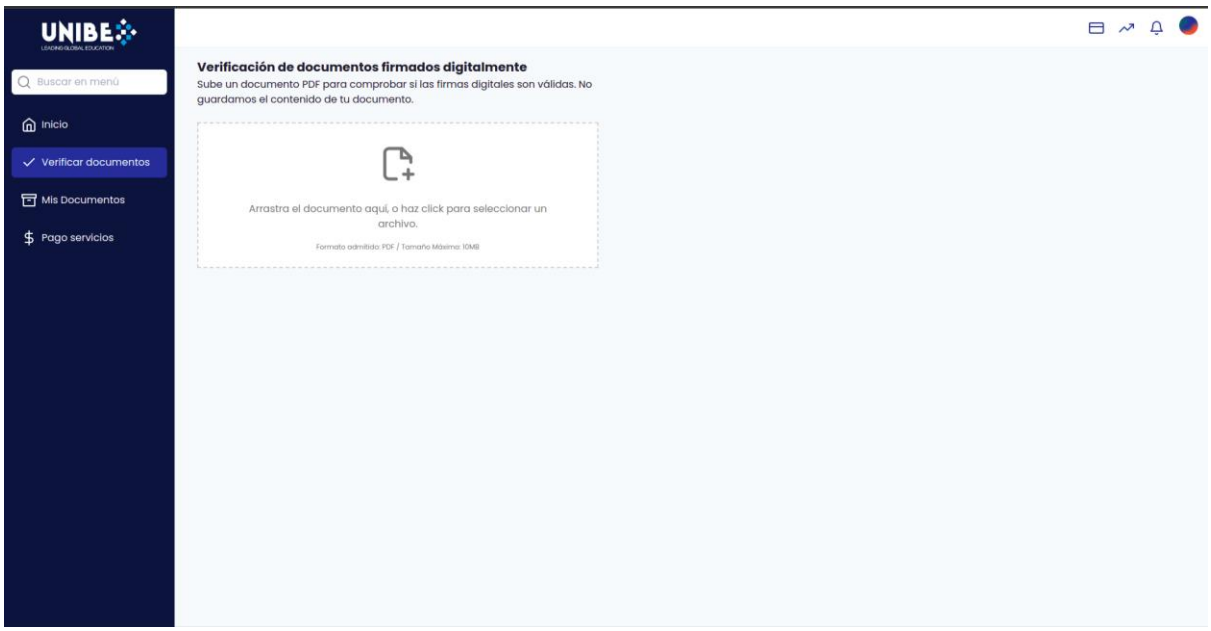

Figura 6.10. Pantalla para insertar documentos a ser verificados. (Elaboración Propia).

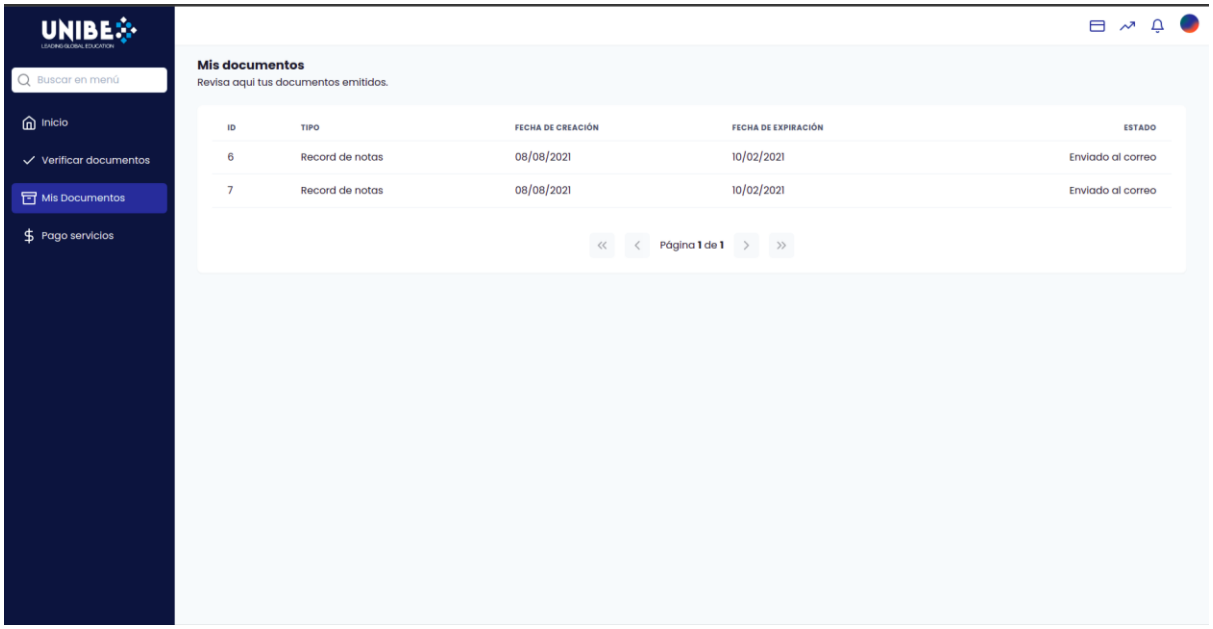

Figura 6.11. Historial de documentos solicitados. (Elaboración Propia).

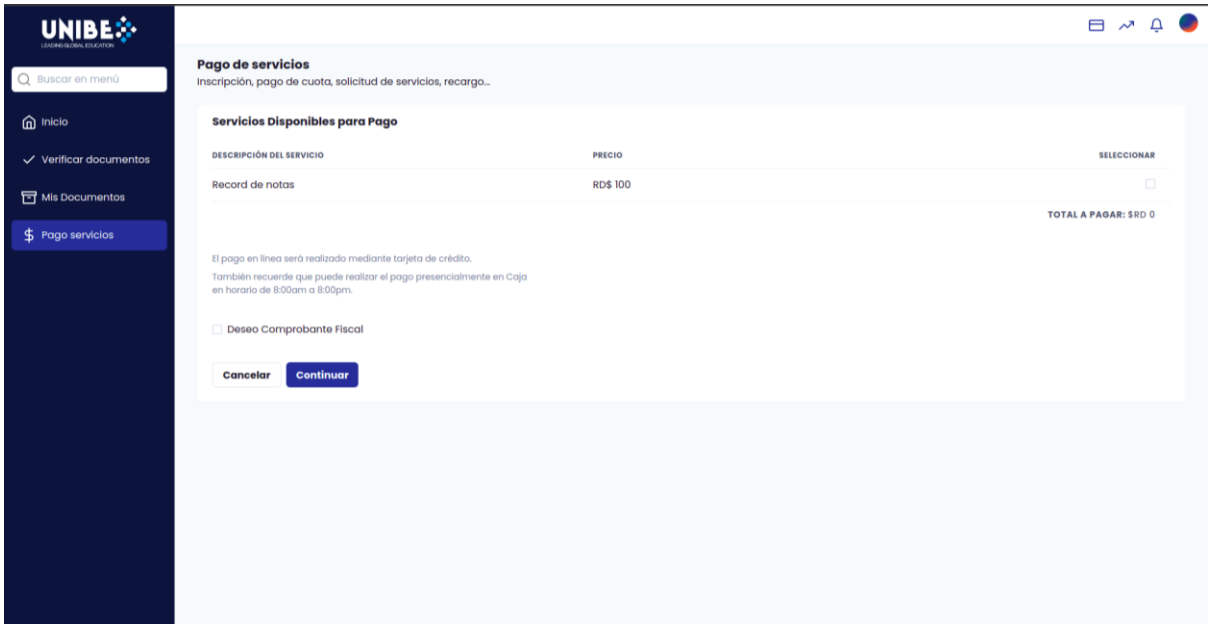

Figura 6.12. Pantalla inicial del módulo de pago de servicios. (Elaboración Propia).

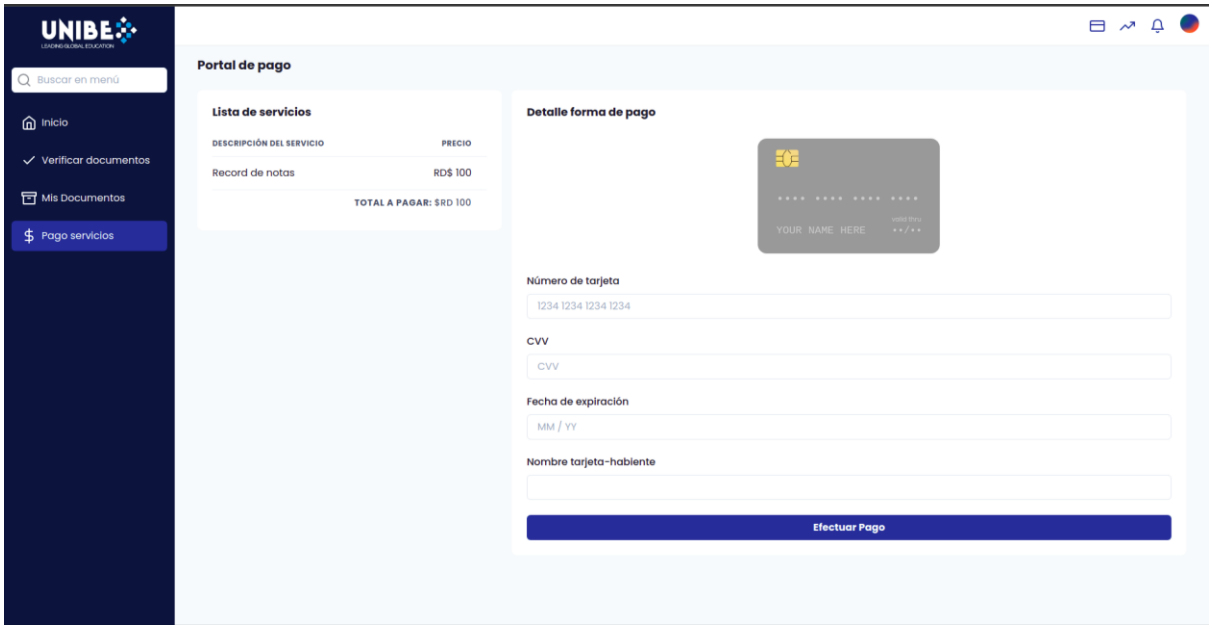

Figura 6.13. Pantalla para insertar el método de pago. (Elaboración Propia).

Figura 6.14. Pantalla de inicio de un usuario con rol de administrador. (Elaboración Propia).

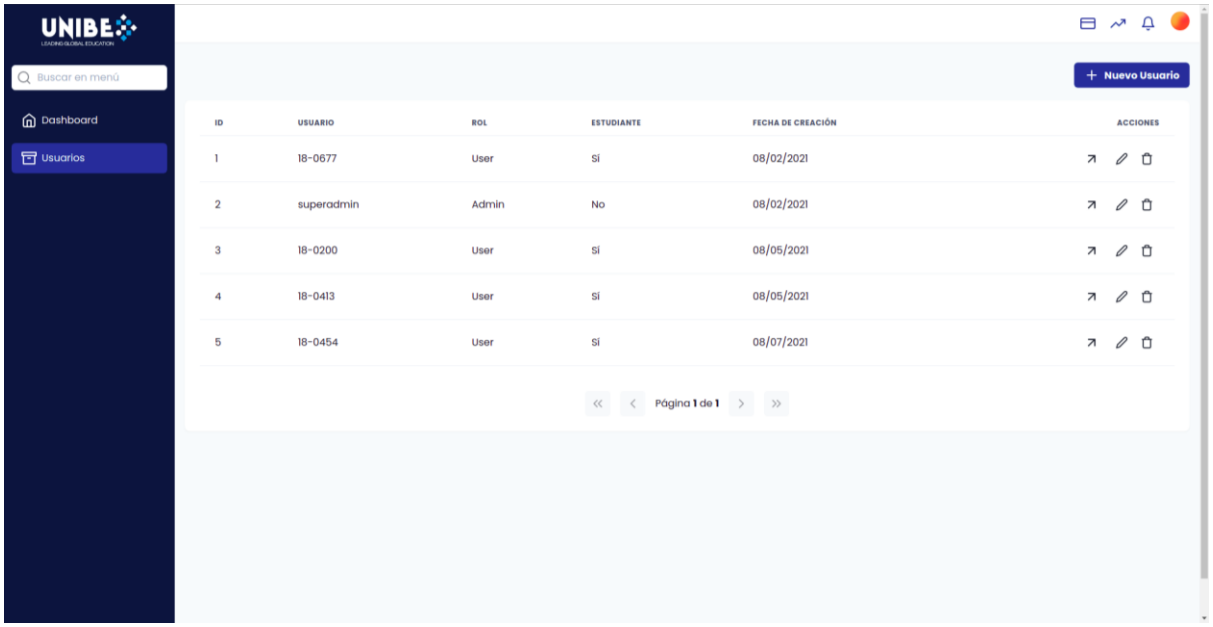

Figura 6.15. Listado de usuarios. (Elaboración Propia).

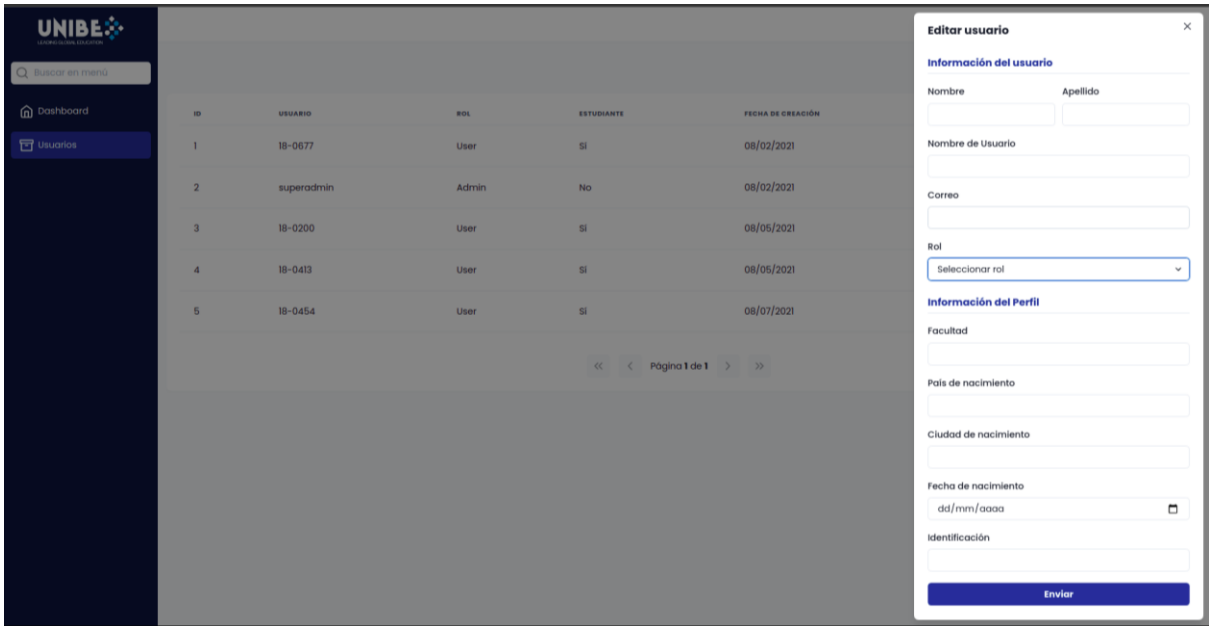

Figura 6.16. Formulario para agregar un usuario. (Elaboración Propia).

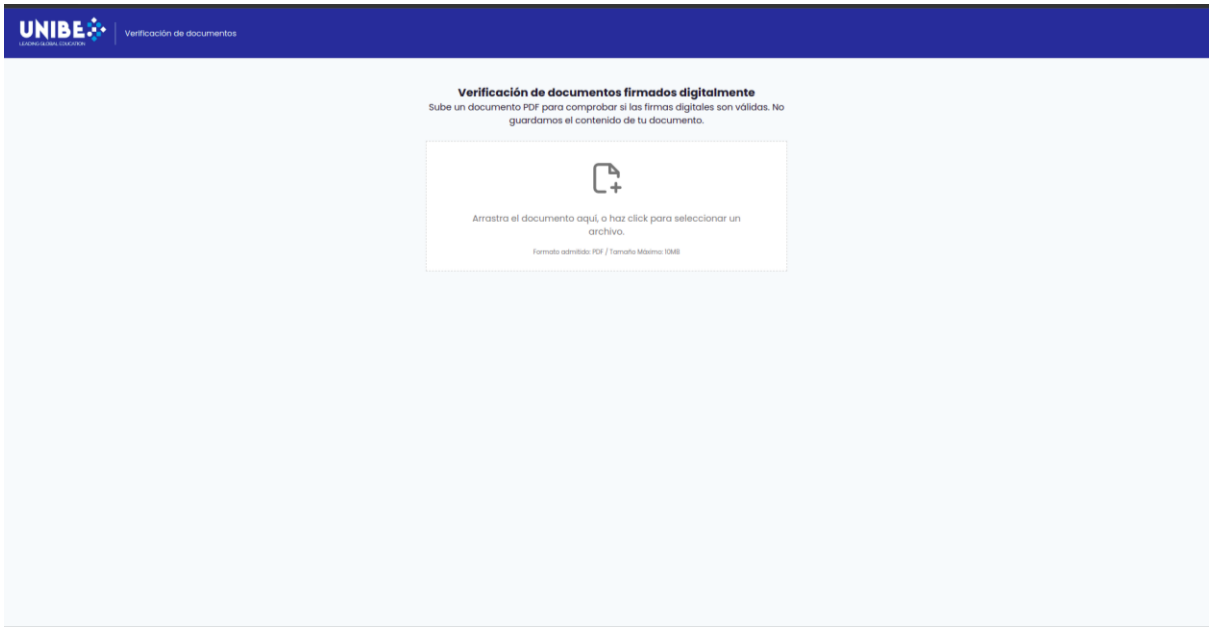

Figura 6.17. Pantalla para verificar documentos sin ser usuario de DocBlock. (Elaboración Propia).

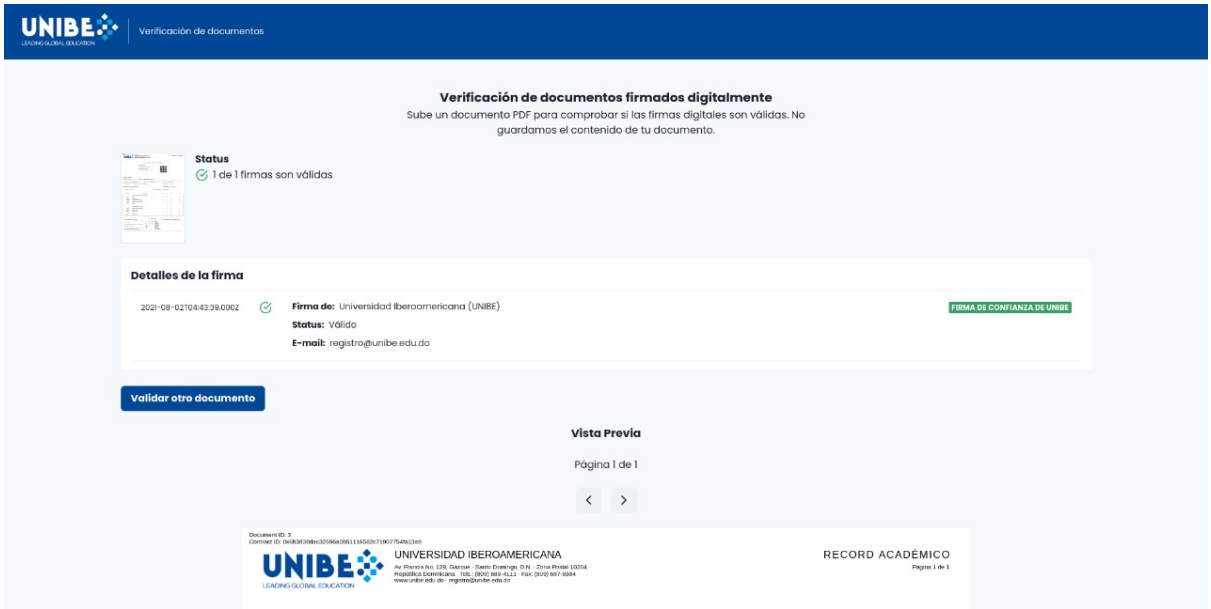

Figura 6.18. Documento siendo verificado en DocBlock. (Elaboración Propia).

6.8 Diagrama jerárquico de programas y/o menús principales

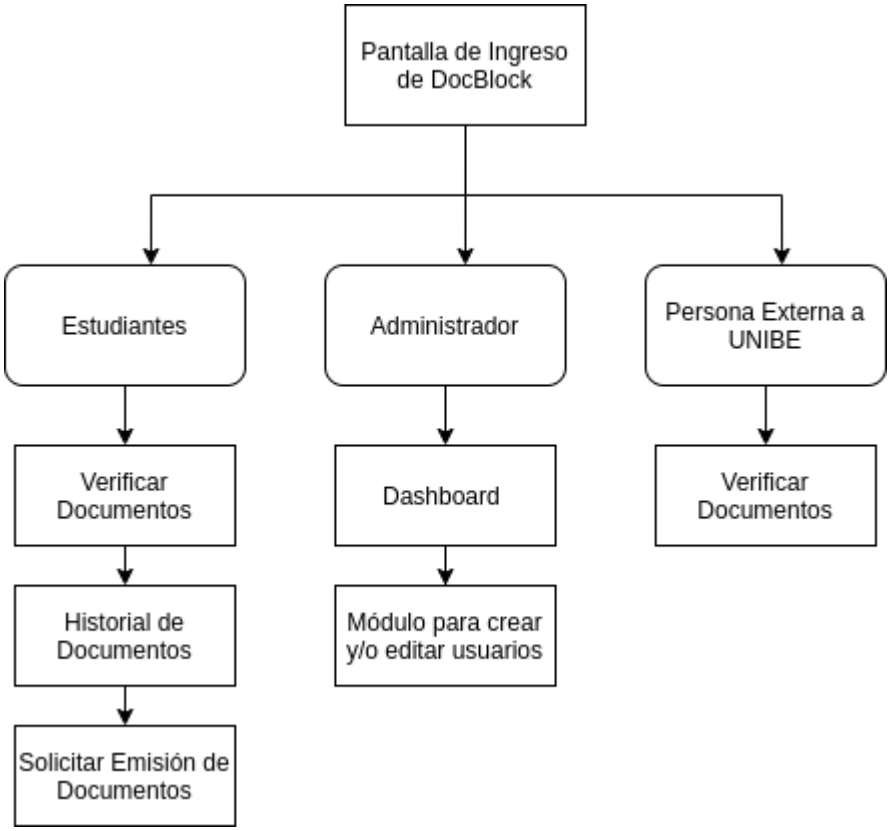

Figura 6.19. Diagrama jerárquico de menús. (Elaboración Propia).

6.9 Seguridad y Control

La plataforma aprovecha técnicas comunes de autenticación y autorización para garantizar su seguridad y control. Para la autorización, utiliza tokens web JSON (JWT) que son un estándar de la industria para representar reclamaciones entre partes. JWT requiere que el usuario utilice un algoritmo criptográfico subyacente para garantizar la validez de la sesión. DocBlock aprovecha el algoritmo de cifrado asíncrono RSA 256 para codificar sus tokens. Esto permite que diferentes servidores verifiquen la validez del token con sólo una clave pública. Dada la naturaleza desacoplada de estos tokens, se generan estrictamente en el Front-End con una clave privada, y el back-end se asegura de comprobar su validez a través de la clave pública.

Para la autorización, la plataforma tiene dos roles: usuario y administrador. El rol de usuario permite que el usuario sólo utilice operaciones que no sean de administrador, como la solicitud y verificación de documentos. El rol de administrador es mucho más permisivo, ya que permite el acceso al panel de control del administrador, que incluye las estadísticas de los documentos y la creación, eliminación y actualización de los usuarios. Estos roles se imponen en el back-end. El front-end hace una comprobación superficial y se asegura de que el usuario y el administrador están dentro de sus rutas correspondientes.

Dentro de la infraestructura, el Blockchain contiene una característica de seguridad esencial: la inmutabilidad. La inmutabilidad de los contratos inteligentes garantiza que una vez emitido un documento no puede ser revocado o modificado de ninguna manera, aumentando la confianza y la validez de los documentos firmados digitalmente. Aunque la inmutabilidad es importante, un gran grado de seguridad dependerá de su algoritmo de consenso (Proof of Work, Proof of Stake, o Proof of Authority; ver sección 2.2.4) y del número de nodos validadores en la red. El número mínimo de validadores varía según el consenso. Sin embargo, se recomienda tener al menos 7 nodos para adquirir el mínimo de Tolerancia a Fallos Bizantinos entre todos los consensos.

Dado que DocBlock utiliza Solidity Smart Contracts, se requiere que el Blockchain contenga la EVM (Ethereum Virtual Machine) que se encarga de ejecutar el contrato inteligente y comprometer su resultado en la cadena de bloques. Existen Blockchains públicas (Mainnet, Moonbeam, ...) y privadas (Consensys Quorum, Hyperledger Burrow, Go Ethereum, ...) que satisfacen este requisito. Se recomienda utilizar cadenas de bloques públicas por el beneficio añadido de la seguridad globalizada proveniente de miles de nodos. No obstante, una Blockchain privada puede ser útil y recomendable si hay un requisito estricto de privacidad de datos o la institución tiene su propio hardware y desea evitar las tasas de transacción y la latencia. Sin embargo, DocBlock está preparado para ser desplegado

tanto en Blockchain pública como privada, por lo que la decisión dependerá de los requisitos no funcionales de la institución.

6.10 Especificaciones generales de la solución

Debemos destacar el uso del Blockchain (especificada dentro de las tecnologías de desarrollo a utilizar) y de la firma digital, la cual está presente en todos los documentos emitidos en la plataforma.

DocBlock permite a los usuarios realizar diferentes funciones dependiendo de su rol en la plataforma:

- **Estudiantes:** la plataforma les permite solicitar todos los documentos que estén disponibles y tener un historial de los documentos que han solicitado. Estos documentos son enviados directamente al correo electrónico del estudiante y pueden ser compartidos con terceros para que comprueben su autenticidad a través de DocBlock.
- **Administradores:** la plataforma les permite crear y editar usuarios, además de llevar un control de los datos estadísticos de las solicitudes recibidas. Este dashboard se actualiza en tiempo real y permite ver los detalles de las solicitudes recibidas.
- **Personas externas:** la plataforma les permite verificar un documento sin necesidad de tener un usuario dentro de DocBlock. Sirve para autenticar la firma digital y para confirmar que el hash pertenece a la cadena de bloques. En caso de que tengan el documento impreso, también pueden utilizar el código QR del documento para validar su autenticidad.

6.11 Descripción de programas

6.11.1 Tecnologías de desarrollo a utilizar

La plataforma consta de cuatro partes: Front-End, Back-End, generador PDF, e Infraestructura. El Front-End utilizará React.js con el framework Next.js. Su sistema de diseño y estilización se realizará a través de Chakra UI, una librería de componentes de React.js. Además, el Back-End será un servidor Express con el framework Nest.js. Se comunicará y gestionará las migraciones de bases de datos con Prisma. El generador de PDF utiliza la librería React PDF Renderer para construir un PDF electrónicamente de acuerdo a una plantilla. Por último, la infraestructura será la base de datos y el blockchain. Para la base de datos, se utilizará PostgreSQL para los datos dinámicos como los detalles de los usuarios; también, se utilizará el protocolo InterPlanetary File System (IPFS) para almacenar datos estáticos como imágenes y documentos. El Blockchain principal será una implementación privada de Ethereum que utilizará la solución Consensys Quórum.

6.12 Cronograma de actividades para el desarrollo del sistema

DocBlock

Export & Share ▾ Baselines ▾ Options ▾ Columns ▾

		ASSIGNEE	EH	START	DUE	%
	Primera Etapa (Definición):		90h	16/Feb	11/Apr	100%
1	Definición del tema para el proyecto de grado	JG, JF	20h	16/Feb	11/Mar	100%
2	Conceptualización de la plataforma	JF, JG	24h	12/Mar	19/Mar	100%
3	Elección de las tecnologías a utilizar	JF, JG	16h	21/Mar	27/Mar	100%
4	Elaboración del documento teórico	JG, JF	30h	22/Mar	11/Apr	100%
	+ Add task + Add section					
	Segunda Etapa (Desarrollo):		228h	05/May	21/Jul	100%
7	Investigar formas para validar contratos inteligentes	JF, JG	10h	05/May	07/May	100%
8	Creación del contrato inteligente 'Document'	José Félix	6h	07/May	14/May	100%
9	Creación del Front-End en Node.js	José Félix	8h	07/May	11/May	100%
10	Creación del login	JF, JG	16h	12/May	16/May	100%
11	[QA] Realizar pruebas para contrato inteligente `Document`	José Germán Ray	2h	17/May	18/May	100%
12	Creación del contrato inteligente 'Document Track'	José Félix	10h	17/May	20/May	100%
13	[QA] Realizar pruebas para contrato inteligente `DocumentTrack``	José Germán Ray	8h	20/May	23/May	100%
14	[Back-End] Crear base de datos PostgreSQL	JF, JG	8h	24/May	25/May	100%
15	[Back-End] Implementar sistema de autorización	JF, JG	10h	25/May	26/May	100%
16	Permitir iniciar sesión a través del Backend	JF, JG	9h	26/May	28/May	100%
17	[Front-End] Crear pantalla de inicio	José Félix	10h	27/May	30/May	100%
18	[Front-End] Crear pantalla de pago de servicios	JF, JG	12h	31/May	03/Jun	100%
19	[Back-End] Crear cola para manejar solicitudes de servicios	José Félix	8h	04/Jun	07/Jun	100%
20	[Back-End] Crear transacción para validar documento en el Blockchain	José Félix	16h	09/Jun	16/Jun	100%
21	[Front-End] Crear pantalla de mis documentos	José Félix	6h	14/Jun	15/Jun	100%
22	[IPFS] Agregar PDF	JG, JF	8h	15/Jun	17/Jun	100%
23	[INFRASTRUCTURA] Crear nodo de IPFS	JF, JG	4h	15/Jun	16/Jun	100%
24	[INFRASTRUCTURA] Crear nodo de blockchain	José Félix	8h	18/Jun	19/Jun	100%
25	[Front-End] Crear pantalla de verificación de documento	José Félix	9h	21/Jun	24/Jun	100%
26	[Back-End] Verificar documento a través del blockchain	JF, JG	12h	25/Jun	02/Jul	100%
27	[Front-End] Crear roles y pantalla de administración	José Félix	24h	01/Jul	09/Jul	100%
28	[Front-End] Crear CRUD de usuarios	JF, JG	8h	10/Jul	12/Jul	100%
29	[Back-End] Crear endpoints CRUD para usuarios	JF, JG	8h	12/Jul	16/Jul	100%
30	[INFRASTRUCTURA] Crear servidor fron-end y back-end	JF, JG	8h	17/Jul	21/Jul	100%

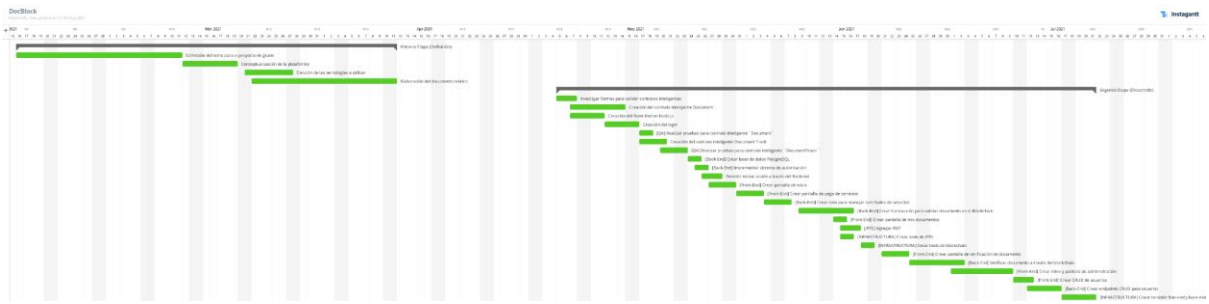

Figura 6.20. Cronograma y Diagrama de Gantt de DocBlock. (Elaboración Propia).

Conclusiones

El fraude o la falsificación de documentos es un problema que siempre ha estado presente y, a decir verdad, es probable que siempre lo esté. Hemos visto falsificaciones de cédulas, pasaportes, títulos de propiedad e incluso de documentos universitarios. El caso concreto de los títulos universitarios fue el que despertó nuestro interés y motivó la creación de nuestra plataforma.

Al realizar la investigación nos encontramos con más casos de fraude de los que habíamos imaginado, lo cual nos hizo ver que estamos frente a una problemática real y que debíamos buscar una solución eficiente y eficaz. Identificamos que la mejor manera de hacerlo era a través de la tecnología de la cadena de bloques.

Nuestra plataforma aplica la tecnología de Blockchain a la emisión de documentos digitales, lo cual aumenta los niveles de seguridad en el proceso de validación de su autenticidad, dificulta la realización de un fraude, y permite aumentar los niveles de confianza que tienen las personas en los servicios que involucran esta tecnología. DocBlock es un proyecto cuya implementación puede resultar muy beneficiosa para todas las partes involucradas. Las instituciones que adopten nuestra plataforma obtendrían una solución innovadora para emitir sus documentos de manera digital, y los estudiantes, obtendrían una alternativa rápida y segura al proceso actual de emisión de documentos físicos.

Realizar este proyecto ha sido bastante enriquecedor, ya que hemos aplicado todos los conocimientos adquiridos en la universidad e incluso hemos ido un poco más allá. Tenemos la firme convicción de que esta implementación puede resultar totalmente exitosa y que incluso puede ir más allá de documentos universitarios, llegando incluso a aplicarse en todos los niveles educativos de nuestro país e incluso en documentos oficiales emitidos por el Estado Dominicano.

Referencias

Referencias web

Alcaide, J. (2019, 29 mayo). Blockchain para registro de la propiedad: países pioneros en su uso. Recuperado 5 de julio de 2021, de https://blog.enzymeadvisinggroup.com/blockchain-registro-propiedad

BBC News Mundo. (6 de julio de 2019). *Blockchain: Qué es esta tecnología y por qué dicen que cambiará el mundo tanto como internet.* Recuperado el 25 de marzo de 2021, de https://www.bbc.com/mundo/noticias-48829091

Bit2Me Academy. (01 de febrero de 2021). *Smart Contracts: ¿Qué son, cómo funcionan y qué aportan?* Recuperado el 26 de marzo de 2021, de https://academy.bit2me.com/que-son-los-smart-contracts/

Certifaction. (s. f.). Certifaction.io | *Blockchain Certification.* Recuperado el 10 de junio de 2021, de https://certifaction.io/blockchain-certification/

Congreso Nacional. (23 de abril de 2007). L*ey No. 53–07 sobre Crímenes y Delitos de Alta Tecnología.* Recuperado el 26 de marzo de 2021, de https://www.oas.org/juridico/PDFs/repdom_ley5307.pdf

Criptonoticias. (12 de septiembre de 2018). *Universidades españolas emiten títulos académicos certificados en redes de blockchain.* Recuperado el 05 de julio de 2021, de https://www.criptonoticias.com/comunidad/adopcion/universidades-espanolas-emiten-titulos-academicos-certificados-redes-blockchain/

Expansión. (02 de junio de 2021). *En el futuro cercano, los títulos universitarios necesitarán del blockchain.* Recuperado el 05 de julio de 2021, de https://expansion.mx/tecnologia/2021/06/02/en-el-futuro-cercano-los-titulos-universitarios-necesitaran-del-blockchain

Fernández, H. (05 de junio de 2020). *¿Qué es Blockchain? La tecnología que cambiará la economía global*. Recuperado el 25 de marzo de 2021, de https://economiatic.com/blockchain/

GitBook. (s. f.). GitBook. *Chapter 6: Transactions* Recuperado el 12 de junio de 2021, de https://cypherpunks-core.github.io/ethereumbook/06transactions.html

López, M. A. (01 de junio de 2019). *Aprende los tres elementos clave de blockchain con este ejemplo práctico*. Recuperado el 25 de marzo de 2021, de https://blogs.iadb.org/conocimiento-abierto/es/elementos-clave-de-blockchain/

Mereles, E., & Ortellado, J. (2019). *Uso de blockchain en la administración pública.* Recuperado el 25 de marzo de 2021, de https://www.colibri.udelar.edu.uy/jspui/bitstream/20.500.12008/20646/1/tg-mereles-ortellado.pdf

Oliveros, D. (2018). *Revisión sistemática del uso de Blockchain en datos clínicos y su aplicación en Colombia*. Recuperado el 25 de marzo de 2021, de https://repository.ucatolica.edu.co/bitstream/10983/22426/1/REVISI%C3%93N%20SISTEM%C3%81TICA%20DEL%20USO%20DE%20BLOCKCHAINS%20EN%20DATOS%20CL%C3%8DNICOS%20Y%20SU%20APLICACI%C3%93N%20EN%20COLOMBIA_624906_2018_11_18.pdf

Periódico Hoy. (14 de octubre de 2014). *Empresa reclutadora denuncia 70% de títulos que recibe son falsificados*. Recuperado el 19 de marzo de 2021, de https://hoy.com.do/empresa-reclutadora-denuncia-70-de-titulos-que-recibe-son-falsificados/

Pichardo, C. (25 de mayo de 2017). *Desmantelan laboratorio falsificaba títulos universitarios y otros documentos*. Recuperado 19 de marzo de 2021, de https://ntelemicro.com/desmantelan-laboratorio-falsificaba-titulos-universitarios-y-otros-documentos/

PixelPlex. (s. f.). Blockcerts - *Blockchain-Based Digital Document Verification System*. Recuperado el 25 de marzo de 2021, de https://pixelplex.io/work/blockchain-based-digital-document-verification-system/

Kenfield, Y. (2018). AC*TITUDES LINGÜÍSTICAS DE ESTUDIANTES UNIVERSITARIOS HACIA EL QUECHUA EN CUSCO*. Recuperado el 16 de julio de 2021, de https://www.redalyc.org/jatsRepo/4676/467655911001/html/index.html

Universia. (27 de febrero de 2019). *Red de Portales News Detail Page.* Recuperado el 05 de julio de 2021, de https://www.universia.net/ar/actualidad/orientacion-academica/certificacion-documentos-blockchain-llega-universidades-argentinas-1164020.html

Universidad Iberoamericana. (25 de julio de 2019). *eTítulo.* Recuperado el 25 de marzo de 2021, de https://www.unibe.edu.do/sobre-unibe/registro/etitulo/

Viafirma. (17 de mayo de 2019). *Firma electrónica en República Dominicana.* Recuperado 18 de mayo de 2021, de https://www.viafirma.do/firma-electronica-en-republica-dominicana-legal/

Apéndice A (Encuesta realizada a través de Google Forms)

UNIBE
ESCUELA DE
INGENIERÍA EN TECNOLOGÍAS
DE LA INFORMACIÓN
Y LA COMUNICACIÓN

DocBlock - Estrategia de Validación y Verificación de Documentos Estudiantiles a través del Blockchain para la Transformación Digital de la Administración Universitaria

Hola! Muchas gracias por abrir el enlace.

Nuestro proyecto de grado consiste en una plataforma para realizar la verificación de los documentos univesitarios a través del blockchain y la firma digital, contribuyendo así a evitar la falsificación de documentos y a que la universidad pueda emitir todos sus documentos de forma digital.

El único objetivo de esta encuesta es recopilar datos estadísticos para utilizarlos en nuestro proyecto de grado. Todos los datos recopilados serán totalmente anónimos y están protegidos por el mecanismo de Google Forms.

De antemano muchas gracias por colaborar con nuestro proyecto de grado!

José Félix y José Germán.

*Obligatorio

¿Es usted estudiante universitario? *

- ◯ Sí
- ◯ No

En caso de no ser estudiante, ¿trabaja usted en alguna universidad? (Si es estudiante puede obviar esta pregunta)

- ◯ Sí
- ◯ No

¿Es usted egresado de una institución de educación superior? (En caso de estar estudiando, puede obviar esta pregunta)

- ◯ Sí
- ◯ No

¿Considera que el proceso de emitir documentos académicos es burocrático(tarda mucho tiempo)? *

- ◯ Sí
- ◯ No

¿Ha sido testigo de un caso de falsificación de documentos universitarios? *

- ◯ Sí
- ◯ No

En caso negativo, ¿Ha escuchado de algún caso similar? (En caso negativo obviar las siguientes 5 preguntas)

- ◯ Sí
- ◯ No

¿Sabes si había personas a lo interno de la institución involucradas en el hecho?

- ◯ No lo sé
- ◯ Si

¿El documento falsificado fue digital o físico?

- ◯ Digital
- ◯ Físico
- ◯ No lo sé

¿Hubo algún tipo de sanción?

- ◯ Si
- ◯ No
- ◯ No lo sé

¿Sabes cómo se descubrió la falsificación?

Tu respuesta

¿Sabes si han tomado medidas en el lugar del hecho para prevenir que suceda otra vez?

- ◯ Sí
- ◯ No
- ◯ No lo sé

¿Cuál considera que es más vulnerable a la falsificación, el documento digital (cifrado) o el documento físico? *

- ◯ Digital
- ◯ Físico

En caso de haber seleccionado el digital (cifrado), si existiera un método más seguro para emitir documentos de esta manera, ¿optaría por este medio?

- ◯ Sí
- ◯ No
- ◯ Tal vez

¿Independientemente de su vulnerabilidad, cuál es más conveniente? *

- ◯ Digital
- ◯ Físico

¿Cree que los documentos digitales son beneficiosos para el medio ambiente? *

- ◯ Sí
- ◯ No
- ◯ Tal vez

¿Cree que tener los documentos en formato digital(cifrados) es más eficiente que tenerlos en formato físico? *

- ◯ Sí
- ◯ No
- ◯ Tal vez

Tiene alguna sugerencia para nuestro proyecto?

Tu respuesta

Apéndice B (Resultados de la Encuesta)

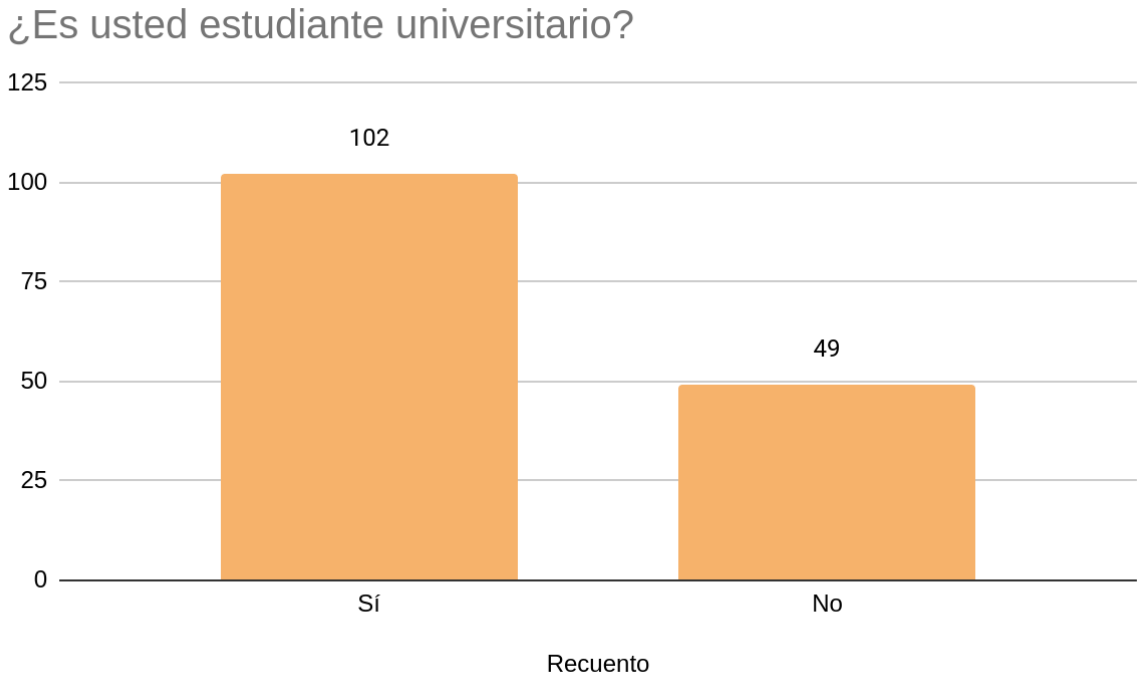

Figura A-1. Respuestas a la primera pregunta.

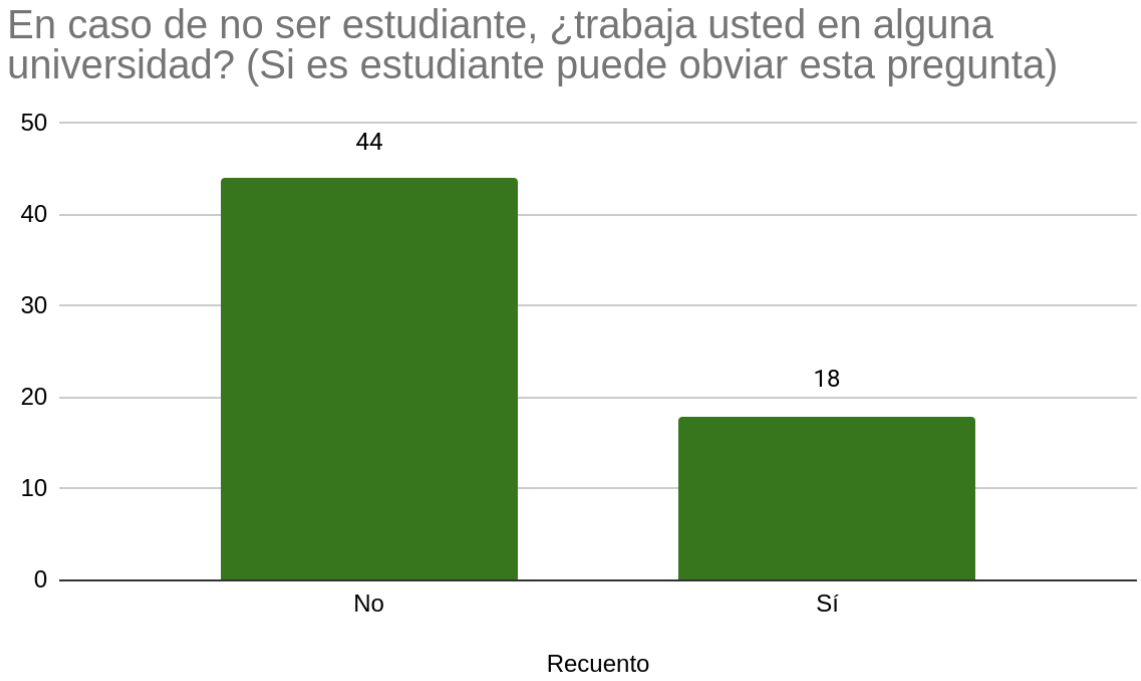

Figura A-2. Respuestas a la segunda pregunta.

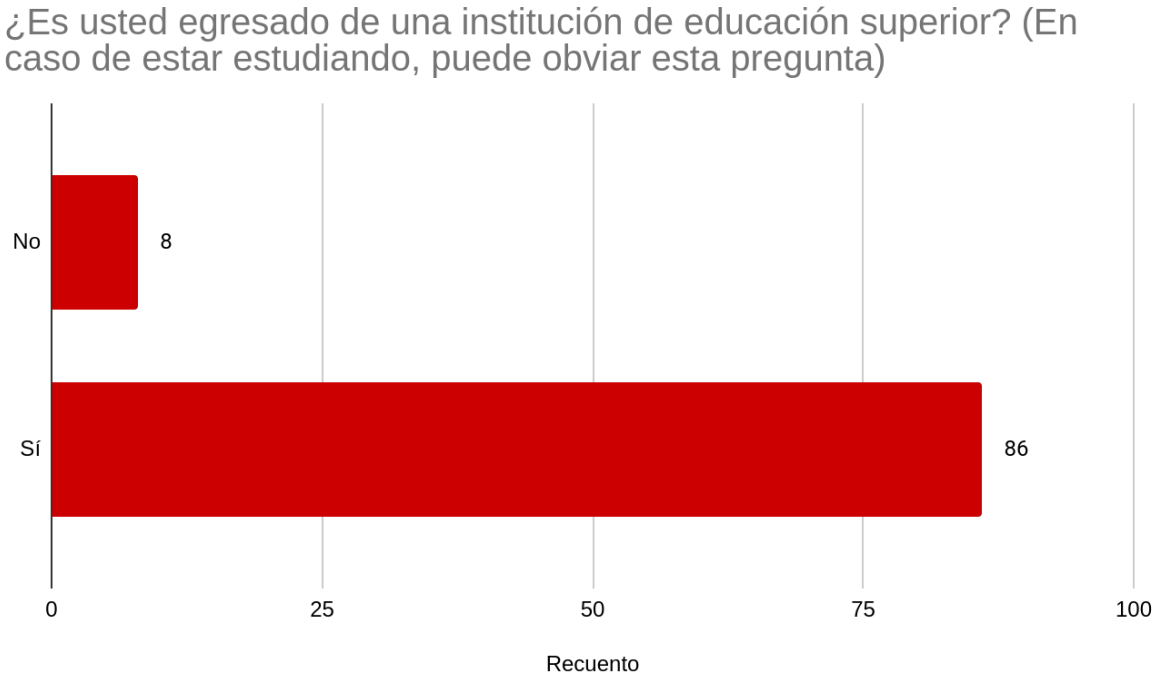

Figura A-3. Respuestas a la tercera pregunta.

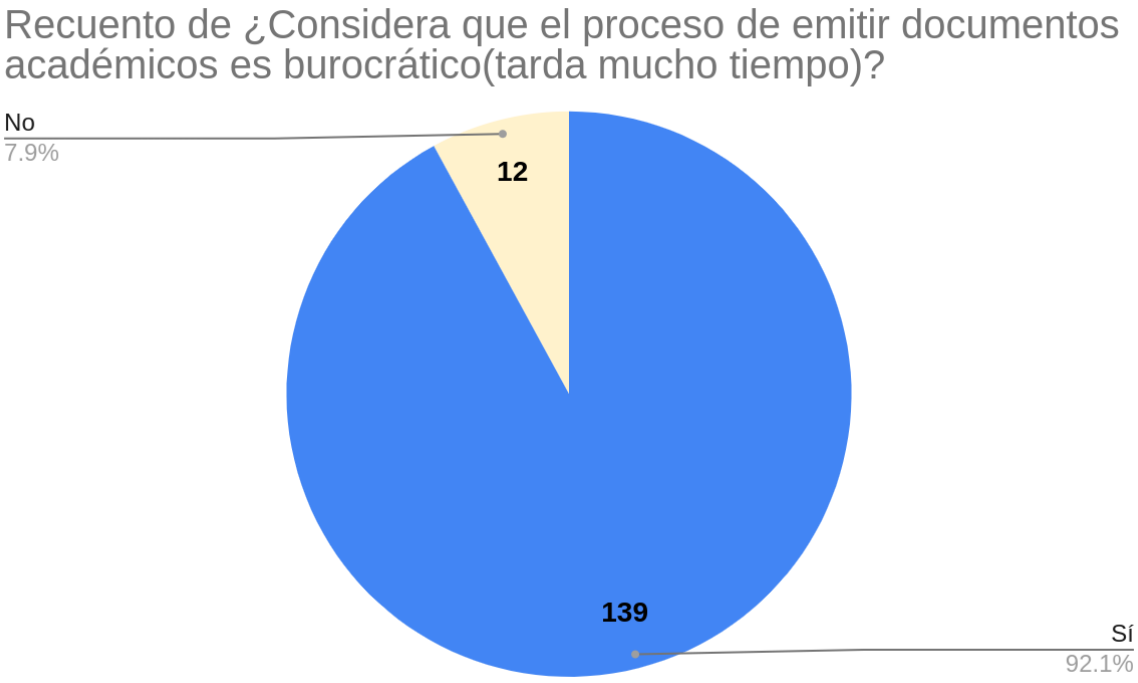

Figura A-4. Respuestas a la cuarta pregunta.

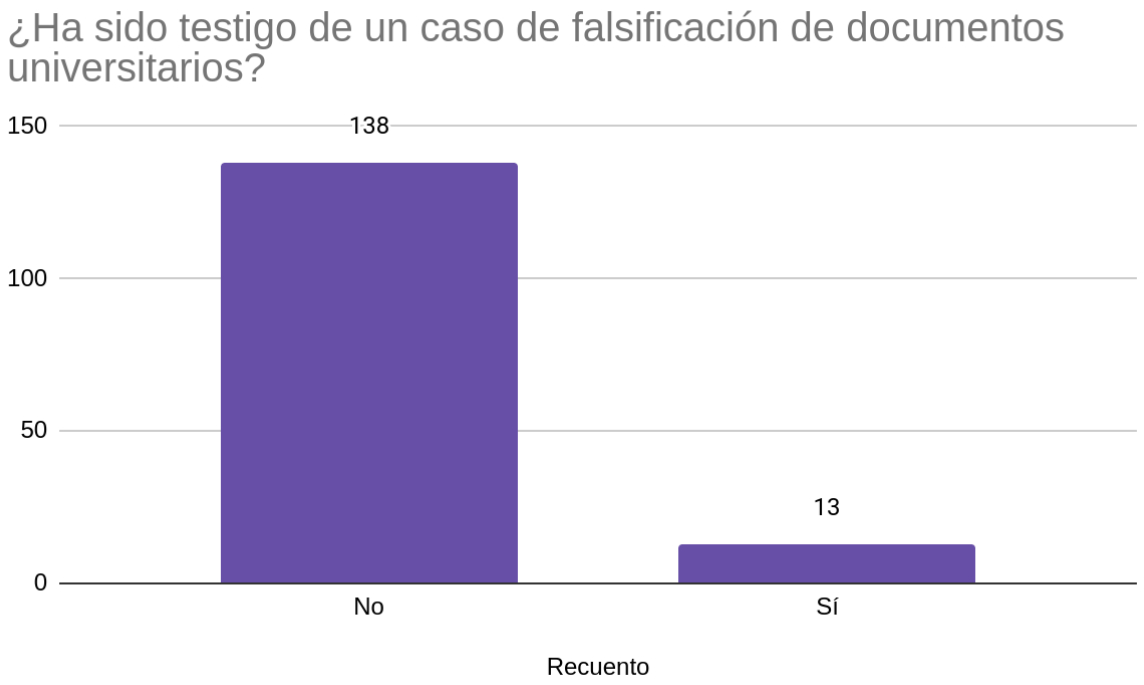

Figura A-5. Respuestas a la quinta pregunta.

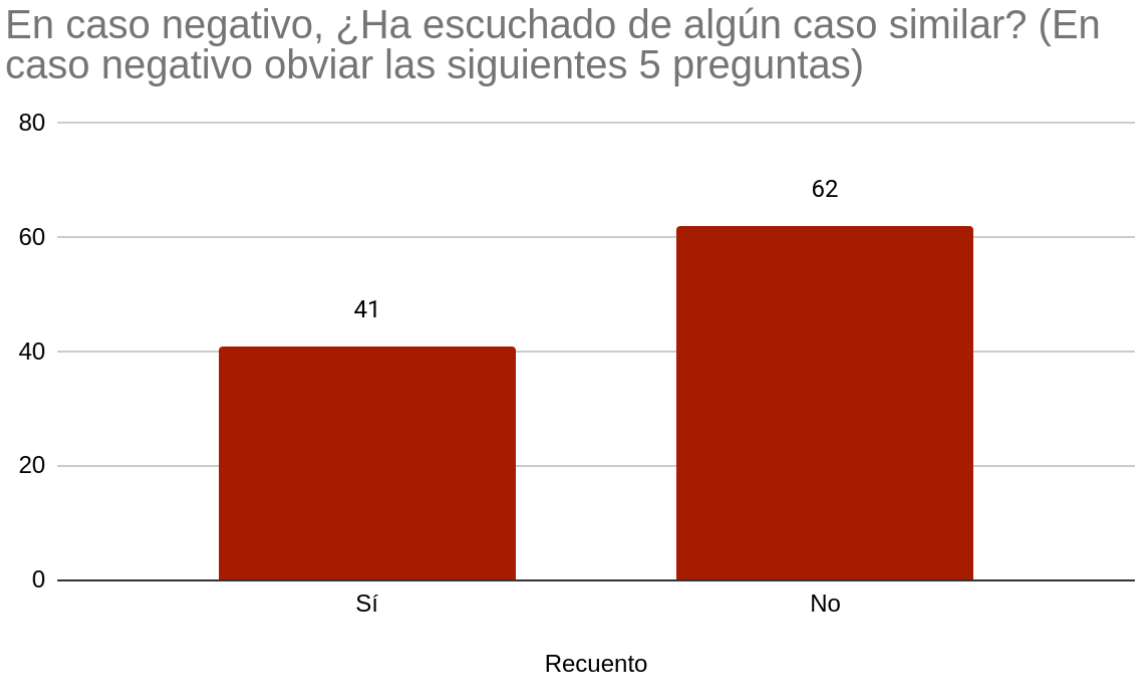

Figura A-6. Respuestas a la sexta pregunta.

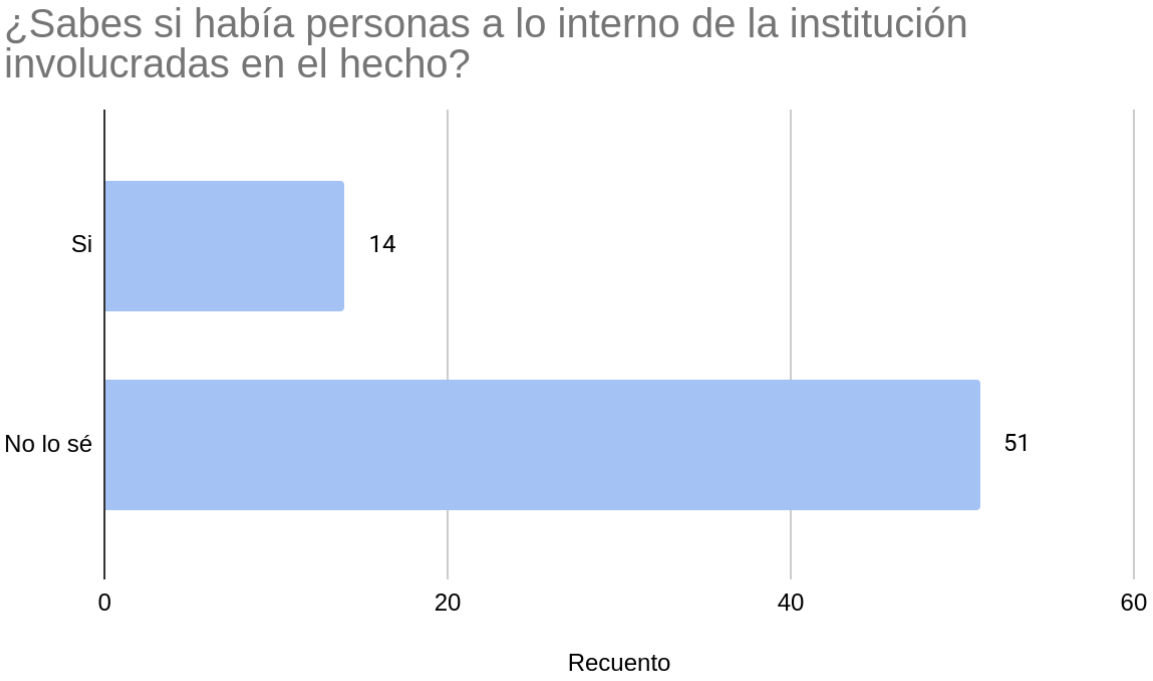

Figura A-7. Respuestas a la séptima pregunta.

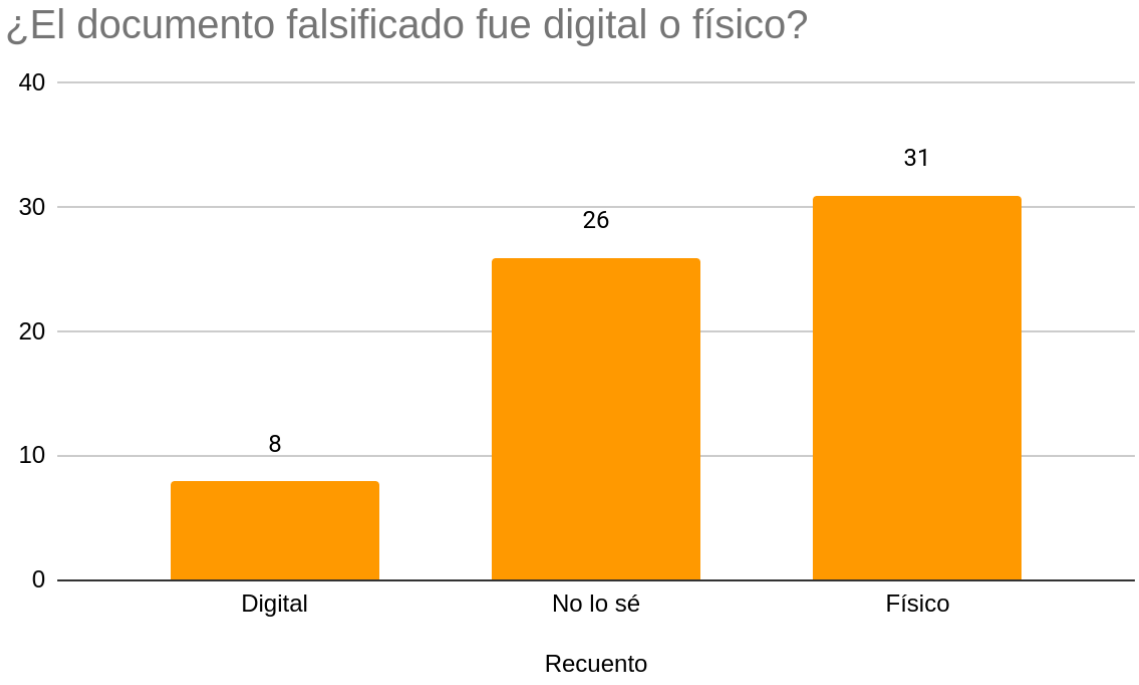

Figura A-8. Respuestas a la octava pregunta.

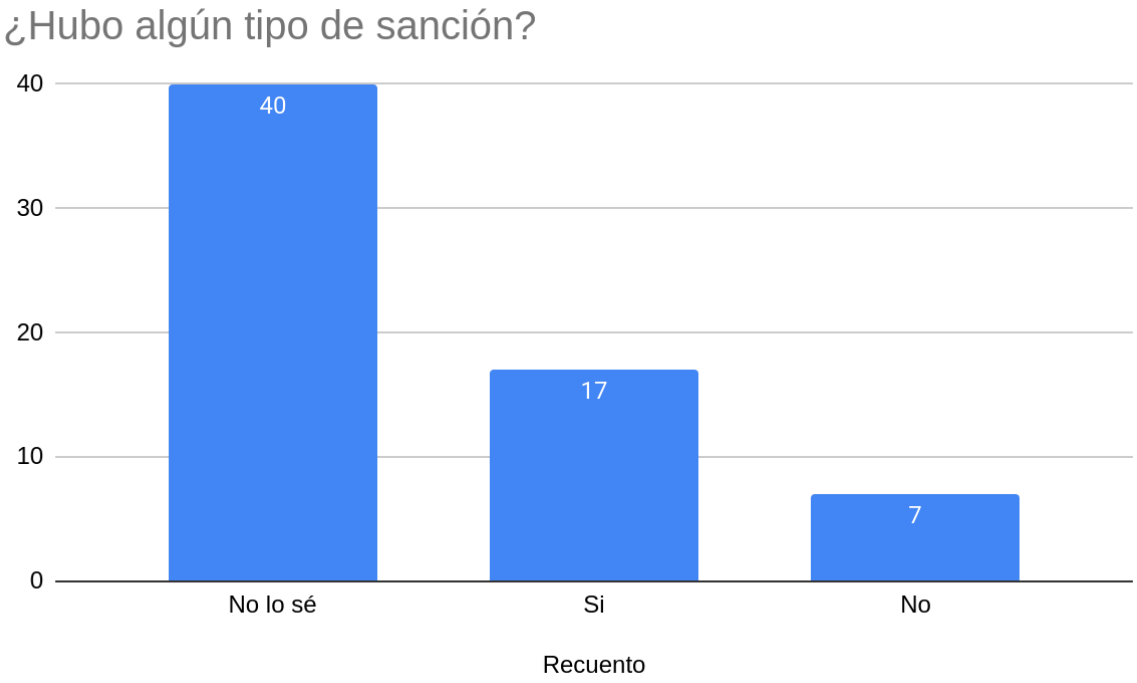

Figura A-9. Respuestas a la novena pregunta.

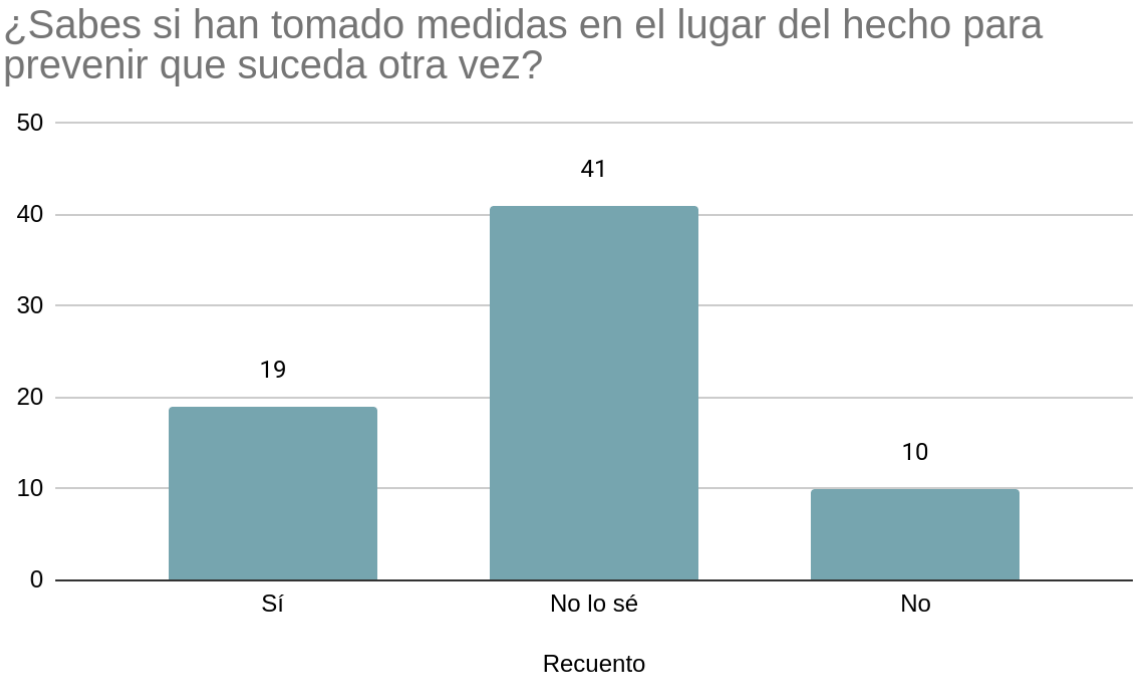

Figura A-10. Respuestas a la undécima pregunta.

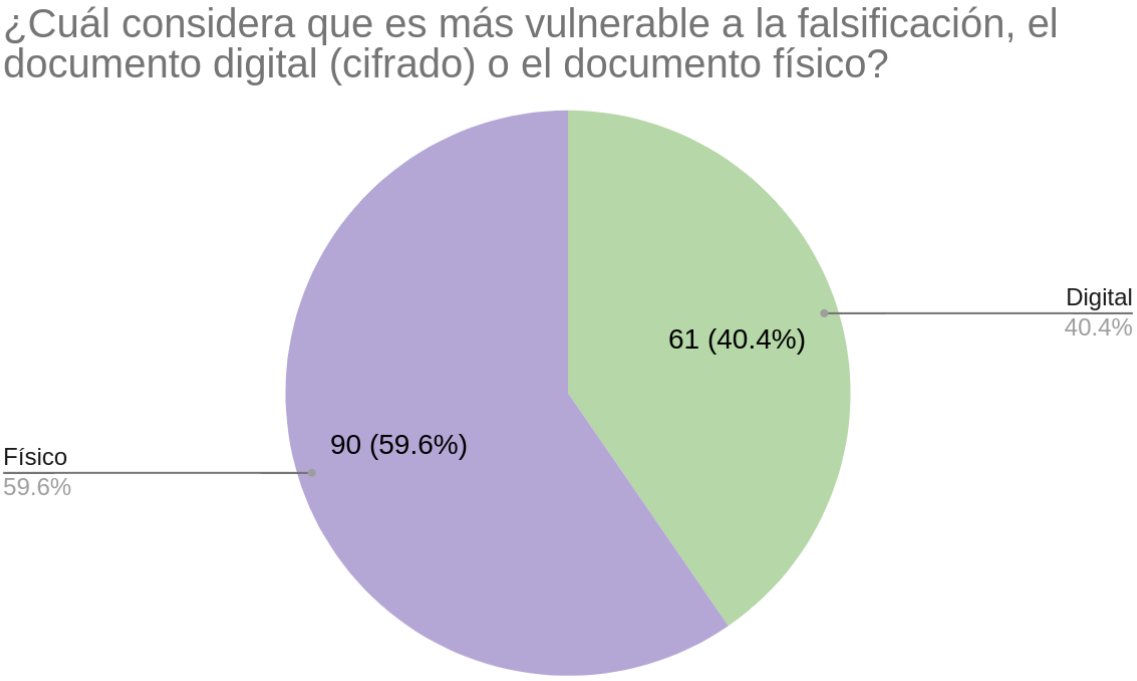

Figura A-11. Respuestas a la duodécima pregunta.

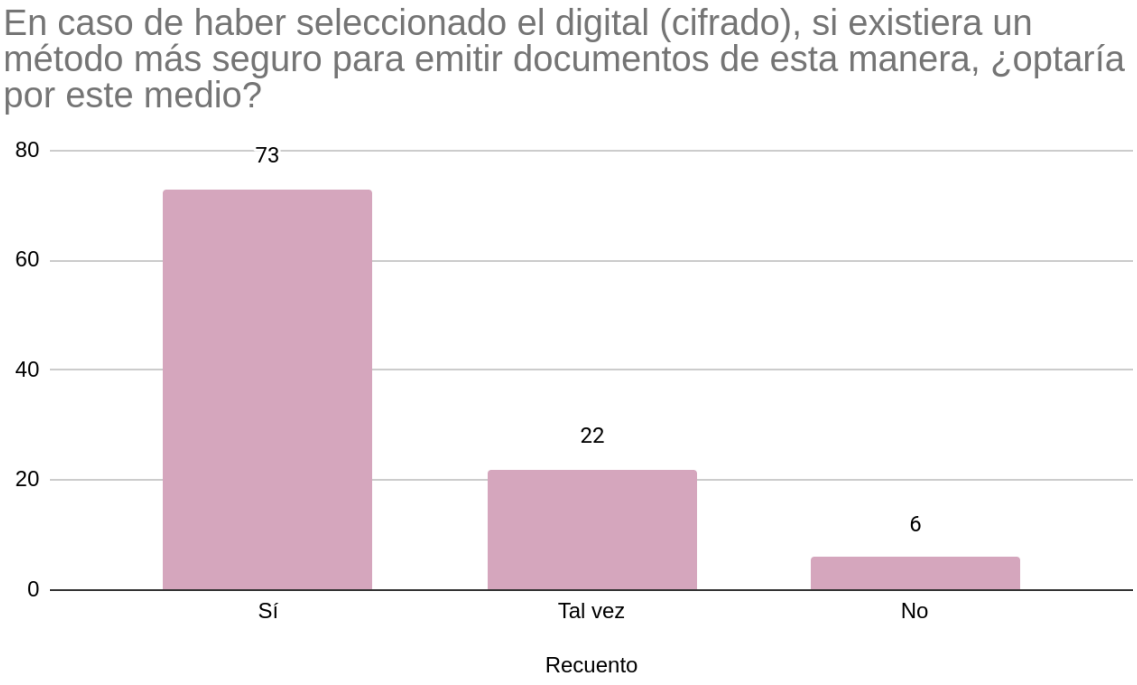

Figura A-12. Respuestas a la decimotercera pregunta.

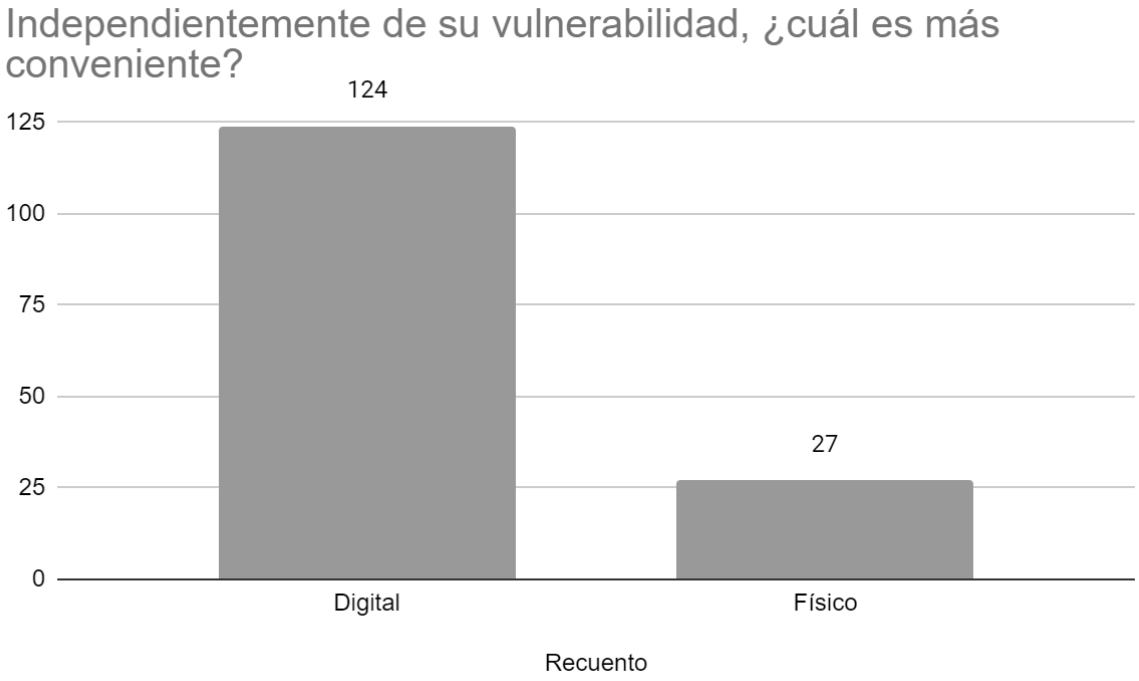

Figura A-13. Respuestas a la decimocuarta pregunta.

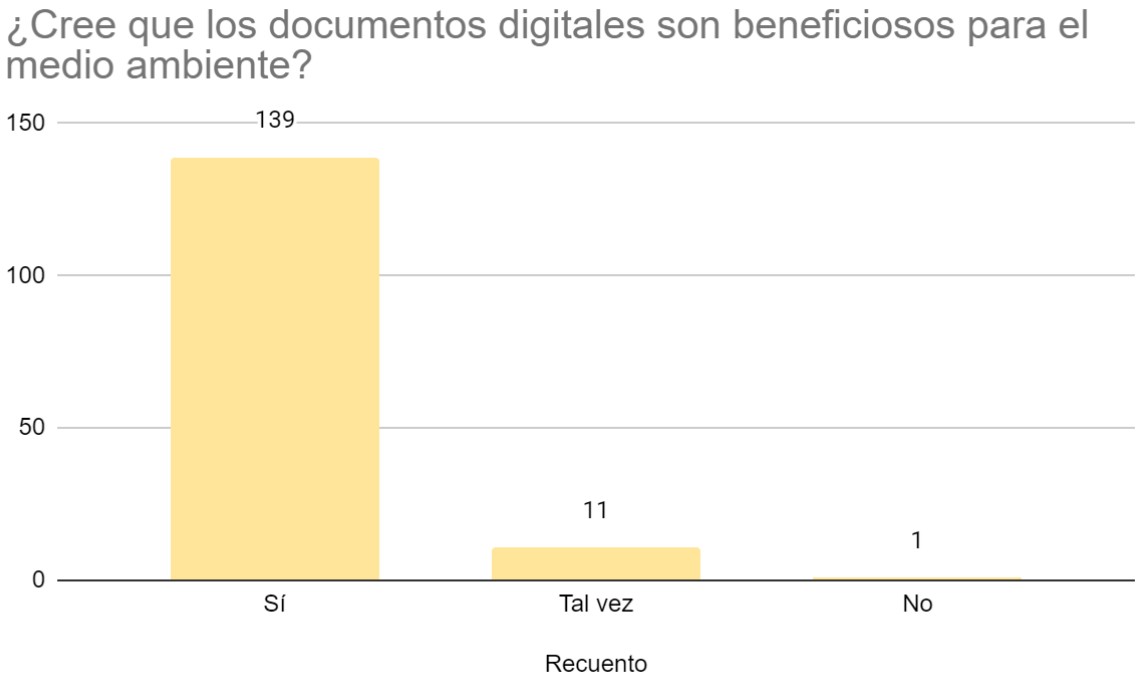

Figura A-14. Respuestas a la decimoquinta pregunta.

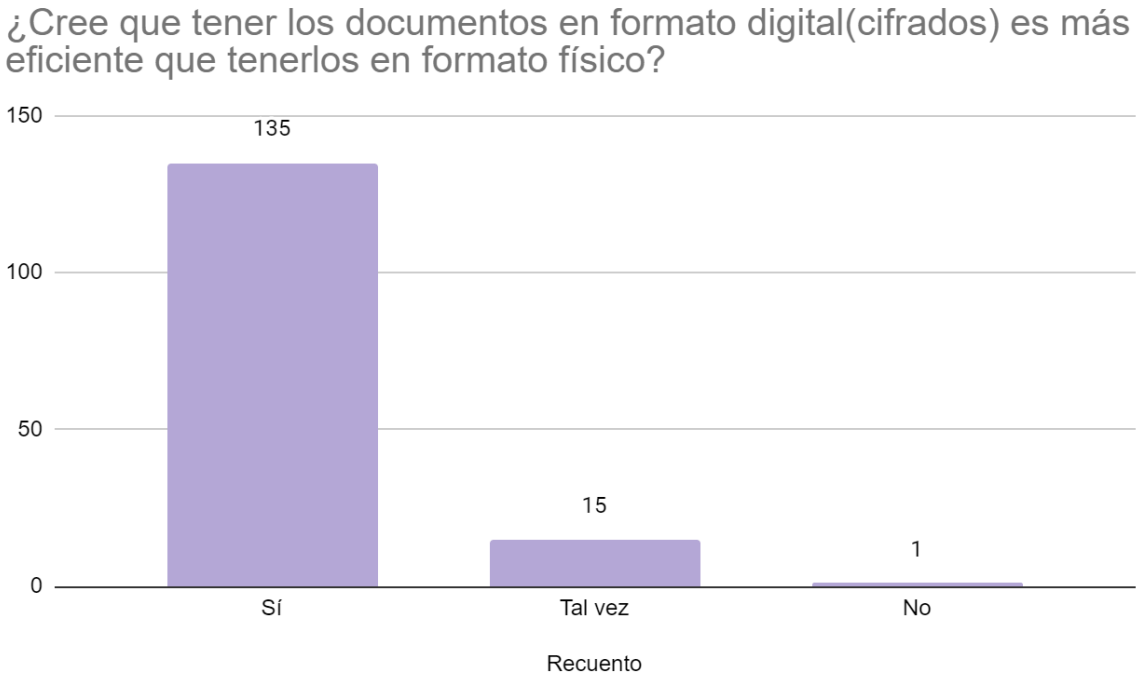

Figura A-15. Respuestas a la decimosexta pregunta.

Apéndice C (Otras partes relevantes del prototipo)

Document ID: 7
Contract ID: 0x6b3d38dac32596a0b51116582c71907754fa13a9

UNIBE
LEADING GLOBAL EDUCATION

UNIVERSIDAD IBEROAMERICANA
Av. Francia No. 129, Gazcue · Santo Domingo, D.N. · Zona Postal 10204
República Dominicana · Tels.: (809) 689-4111 · Fax: (809) 687-9384
www.unibe.edu.do · registro@unibe.edu.do

RECORD ACADÉMICO
Página 1 de 1

SELLO DIGITAL OFICIAL DE UNIBE

Sobre este sello:
https://docblock.vercel.app/seal

Verificar version digital:
https://docblock.vercel.app/verify-document

NOMBRE JOSÉ GERMÁN

MATRICULA 18-0200 ESCUELA INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNIACIÓN

NACIMIENTO 04 MARZO DEL 2000 NACIONALIDAD DOMINICANO CEDULA 402-334819-4

LUGAR NACIMIENTO NAGUA, REPÚBLICA DOMINICANA PASAPORTE **********

BACHILLER INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNIACIÓN SEGURO SOCIAL **********

TRANSFERIDO ********** FECHA DE ADMISION 25 JULIO DEL 2017

CÓDIGO	ASIGNATURA	CR	CAL	PT
	Semestre Septiembre-Diciembre 2017			
CGM-170	PRE-CÁLCULO	5	B	3
ING-110	INGLES I	3	A	4
CCI-100	INTRODUCCIÓN A LA INGENIERIA	2	A	4
CGC-100	ORIENTACIÓN UNIVERSITARIA	2	A	4
CGM-170	PRE-CÁLCULO	5	B	3
	Semestre Enero-Abril 2018			
CGR-100	ESPAÑOL I	4	A	4
ING-110	INGLES I	3	A	4
CGC-100	ORIENTACIÓN UNIVERSITARIA	2	A	4
CGR-100	ESPAÑOL I	4	A	4
CGR-100	ESPAÑOL I	4	A	4

GRADO OTORGADO **********

****

INDICE ACADÉMICO ACUMULADO **********

HONORES **********

FECHA DE GRADUACION **********

EQUIVALENCIAS

A	90	100	EXCELENTE
B	80	89	BUENO
C	70	79	SUFICIENTE
D	60	69	REPROBADO
F	0	59	REPROBADO
COV			CONVALIDACION
RET			RETIRADA
EXR			EXONERADO
S			SATISFACTORIO
NS			NO SATISFACTORIO

FECHA DE EXPEDICION 08 AGOSTO DEL 2021

Figura A-16. Documento que recibe el usuario en su correo electrónico.

```
// SPDX-License-Identifier: UNLICENSED
pragma solidity ^0.8.0;
pragma experimental ABIEncoderV2;

import "@openzeppelin/contracts/access/AccessControl.sol";
import "@openzeppelin/contracts/access/Ownable.sol";
import "./Document.sol";

contract DocumentTrack is Ownable, AccessControl {
  struct DocumentData {
    uint256 date;
    address owner;
    address documentContract;
  }

  bytes32 public constant ADMIN_ROLE = keccak256("ADMIN_ROLE");

  event DocumentTrackAdd(
    uint256 date,
    address indexed creator,
    address indexed newContract
  );

  DocumentData[] private documentsContracts;
  mapping(string => DocumentData[]) documentsByType;
  mapping(string => DocumentData) documentByHash;

  constructor() {
    _setupRole(DEFAULT_ADMIN_ROLE, owner());
    _setupRole(ADMIN_ROLE, owner());
  }

```

Figura A-17. Contrato Inteligente "Document Track".

```
32
33    /**
34     * @dev Set document to be validated
35     * @param _hash hash of the document
36     * @param _acquirer acquirer of the document. Normally the student.
37     * @param _documentType type of the document
38     * @param _expiryDate unix date of expiry for the document.
39     * @param _validators addresses for required validators.
40     */
41    function createDocument(
42      string memory _hash,
43      string memory _acquirer,
44      string memory _documentType,
45      uint256 _expiryDate,
46      address[] memory _validators
47    ) external onlyRole(ADMIN_ROLE) {
48      require(documentByHash[_hash].date == 0, "Document already exists");
49
50      Document document = new Document(
51        _hash,
52        _acquirer,
53        _documentType,      You, seconds ago • update: remove todo
54        _expiryDate,
55        _validators,
56        msg.sender
57      );
58
59      DocumentData memory data = DocumentData(
60        block.timestamp,
61        msg.sender,
62        address(document)
63      );
64
65      documentByHash[_hash] = data;
66      documentsByType[_documentType].push(data);
67      documentsContracts.push(data);
68
69      emit DocumentTrackAdd(data.date, data.owner, data.documentContract);
70    }
```

Figura A-18. Contrato Inteligente "Document Track".

```
71
72      /**
73       * @dev Return contracts list
74       * @return Data array
75       */
76      function getDocumentsContracts()
77        external
78        view
79        returns (DocumentData[] memory)
80      {
81        return documentsContracts;
82      }
83
84      function getDocumentsByType(string memory _documentType)
85        external
86        view
87        returns (DocumentData[] memory)
88      {
89        return documentsByType[_documentType];
90      }
91
92      function getDocumentByHash(string memory _hash)
93        external
94        view
95        returns (DocumentData memory)
96      {
97        return documentByHash[_hash];
98      }
99
100     function addAdmin(address _newAdmin) external onlyOwner {
101       grantRole(ADMIN_ROLE, _newAdmin);
102     }
103
104     function removeAdmin(address _admin) external onlyOwner {
105       revokeRole(ADMIN_ROLE, _admin);
106     }
107   }
108
```

Figura A-19. Contrato Inteligente "Document Track".

```
// SPDX-License-Identifier: UNLICENSED      You, 3 months ago • wip: add D
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/access/AccessControl.sol";

contract Document is AccessControl {
  string private fileHash;
  string private acquirer;
  string private documentType;

  address private creator;

  uint256 private createDate;
  uint256 private expiryDate;

  bytes32 public constant VALIDATOR_ROLE = keccak256("VALIDATOR_ROLE");

  address[] private requiredValidators;
  address[] private validators;

  mapping(address => uint256) private validated;

  event DocumentValidated(address indexed validator);

```

Figura A-20. Contrato Inteligente "Document".

```
24
25    constructor(
26      string memory _hash,
27      string memory _acquirer,
28      string memory _documentType,
29      uint256 _expiryDate,
30      address[] memory _validators,
31      address _creator
32    ) {
33      fileHash = _hash;
34      acquirer = _acquirer;
35      expiryDate = _expiryDate;
36      createDate = block.timestamp;
37      requiredValidators = _validators;
38      documentType = _documentType;
39      creator = _creator;
40
41      for (uint256 i = 0; i < _validators.length; i++) {
42        _setupRole(VALIDATOR_ROLE, _validators[i]);
43      }
44    }
45
46    /**
47     * @dev Verify Document Hash
48     * @param _hashToVerify hash of the document
49     */
50    function verifyDocumentHash(string memory _hashToVerify)
51      public
52      view
53      returns (bool)
54    {
55      if (
56        keccak256(abi.encodePacked(fileHash)) ==
57        keccak256(abi.encodePacked(_hashToVerify))
58      ) {
59        return true;
60      } else {
61        return false;
62      }
63    }
64
```

Figura A-21. Contrato Inteligente "Document".

```
65    /**
66     * @dev
67     * @param _hashToVerify hash of the document
68     */
69    function verifyDocument(string memory _hashToVerify)
70      external
71      view
72      returns (bool)
73    {
74      bool isValidHash = verifyDocumentHash(_hashToVerify);
75      bool isValidated = validators.length == requiredValidators.length;
76      bool isNotExpired = block.timestamp < expiryDate;
77
78      if (isValidHash && isValidated && isNotExpired) return true;
79      else return false;
80    }
81
82    /**
83     * @dev Validate document
84     * @param _validator address of new validator
85     */
86    function validateDocument(address _validator)
87      public
88      onlyRole(VALIDATOR_ROLE)
89    {
90      require(
91        msg.sender == _validator,
92        "Validator has to be the same as the sender."
93      );
94      require(validated[_validator] == 0, "Validator has already signed.");
95
96      validators.push(_validator);
97      validated[_validator] = block.timestamp;
98      emit DocumentValidated(_validator);
99    }
```

Figura A-22. Contrato Inteligente "Document".

```
101     /**
102      * @dev Return validated unix date
103      * @return Validator document validation unix date
104      */
105     function getValidated(address _validator) external view returns (uint256) {
106       return validated[_validator];
107     }
108
109     /**
110      * @dev Return validators
111      * @return Validators addresses
112      */
113     function getValidators() external view returns (address[] memory) {
114       return validators;
115     }
116
117     /**
118      * @dev Return required validators
119      * @return Validators addresses
120      */
121     function getRequiredValidators() external view returns (address[] memory) {
122       return requiredValidators;
123     }
124
125     /**
126      * @dev Return acquirer name
127      * @return string of acquirer
128      */
129     function getAcquirer() external view returns (string memory) {
130       return acquirer;
131     }
132
133     /**
134      * @dev Return file hash
135      * @return string of file hash
136      */
137     function getFileHash() external view returns (string memory) {
138       return fileHash;
139     }
140
```

Figura A-23. Contrato Inteligente "Document".

```
141     /**
142      * @dev Return file hash
143      * @return number of unix date
144      */
145     function getCreateDate() external view returns (uint256) {
146       return createDate;
147     }
148
149     /**
150      * @dev Return expiry date
151      * @return number of unix date
152      */
153     function getExpiryDate() external view returns (uint256) {
154       return expiryDate;
155     }
156
157     /**
158      * @dev Return expiry date
159      * @return number of unix date
160      */
161     function getCreator() external view returns (address) {
162       return creator;
163     }
164   }
```

Figura A-24. Contrato Inteligente "Document".

Vita

José Ediberto Germán Ray

Nacido el 04 de marzo del año 2000 en la ciudad de Nagua, R.D. Cursó los niveles correspondientes a la educación primaria y secundaria en el Colegio Belén de su misma ciudad natal, obteniendo el título de Bachiller en Modalidad General. Actualmente es estudiante de término de la carrera de Ingeniería en Tecnologías de la Información y la Comunicación (TIC) en la Universidad Iberoamericana (UNIBE). En materia laboral, actualmente se desempeña como Analista de Datos en la Dirección de Tecnología del Ministerio de Interior y Policía de la República Dominicana. Se define a sí mismo como un apasionado de los datos, y tiene planeado realizar una maestría en Big Data una vez haya culminado su etapa en UNIBE.

José Roberto Félix Ramírez

Nacido el 05 de febrero del año 1999 en la ciudad de Santo Domingo, República Dominicana. Cursó sus estudios primarios y secundarios en el colegio cristiano King’s Christian School. Actualmente es estudiante de término de la carrera de Ingeniería en Tecnologías de la Información y la Comunicación (TIC) en la Universidad Iberoamericana (UNIBE). Se desempeña en el área de desarrollo de software, con concentración en ingeniería de Front - End.