ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA SOFTWARE

DESARROLLO DE UNA APLICACIÓN DESCENTRALIZADA CON EL USO DE LA TECNOLOGÍA BLOCKCHAIN PARA VOTACIONES ELECTRÓNICAS EN LA COOPERATIVA DE AHORRO Y CRÉDITO "NUEVA ESPERANZA"

Trabajo de Integración Curricular

Tipo: Proyecto Técnico

Presentado para optar al grado académico de:

INGENIERO DE SOFTWARE

AUTORES: AYRTON FIDEL AVALOS CUADRADO

EDWIN STALYN MANZANO QUINZO

Riobamba - Ecuador

2023

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA SOFTWARE

DESARROLLO DE UNA APLICACIÓN DESCENTRALIZADA CON EL USO DE LA TECNOLOGÍA BLOCKCHAIN PARA VOTACIONES ELECTRÓNICAS EN LA COOPERATIVA DE AHORRO Y CRÉDITO "NUEVA ESPERANZA"

Trabajo de Integración Curricular

Tipo: Proyecto Técnico

Presentado para optar al grado académico de:

INGENIERO DE SOFTWARE

AUTORES: AYRTON FIDEL AVALOS CUADRADO

EDWIN STALYN MANZANO QUINZO

DIRECTOR: DR. DIEGO FERNANDO AVILA PESANTEZ

Riobamba - Ecuador

2023

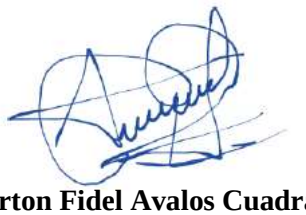
©2023, Ayrton Fidel Avalos Cuadrado & Edwin Stalyn Manzano Quinzo.

Se autoriza la reproducción total o parcial, con fines académicos, por cualquier medio o procedimiento, incluyendo la cita bibliográfica del documento, siempre y cuando se reconozca el Derecho de Autores.

Nosotros, Ayrton Fidel Avalos Cuadrado y Edwin Stalyn Manzano Quinzo, declaramos que el presente Trabajo de Integración Curricular es de nuestra autoría y los resultados de este son auténticos. Los textos en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autores asumimos la responsabilidad legal y académica de los contenidos de este Trabajo de Integración Curricular; el patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 8 de junio de 2023



Ayrton Fidel Avalos Cuadrado
C.I: 060350748-7

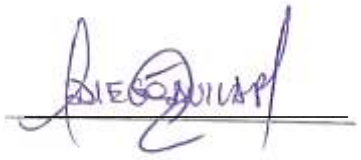
Edwin Stalyn Manzano Quinzo
C.I: 060453805-8

ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

FACULTAD DE INFORMATICA Y ELECTRONICA

CARRERA SOFTWARE

El Tribunal del Trabajo de Integración Curricular certifica que: El Trabajo de Integración Curricular; Tipo: Proyecto Técnico, **DESARROLLO DE UNA APLICACIÓN DESCENTRALIZADA CON EL USO DE LA TECNOLOGÍA BLOCKCHAIN PARA VOTACIONES ELECTRÓNICAS EN LA COOPERATIVA DE AHORRO Y CRÉDITO "NUEVA ESPERANZA",** realizado por los señores **AYRTON FIDEL AVALOS CUADRADO y EDWIN STALYN MANZANO QUINZO,** ha sido minuciosamente revisado por los Miembros del Trabajo de Integración Curricular, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal Autoriza su presentación.

	FIRMA	**FECHA**
Ing. Gloria de Lourdes Arcos Medina **PRESIDENTE DEL TRIBUNAL**		2023-06-08
Dr. Diego Fernando Ávila Pesantez **DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR**		2023-06-08
Ing. Marco Vinicio Ramos Valencia **ASESOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR**		2023-06-08

DEDICATORIA

A nuestros maestros que formaron parte de nuestra vida estudiantil, y que aportaron con sus conocimientos para poder cumplir una etapa de nuestra vida.

Ayrton

Este trabajo está dedicado a todas las personas que han formado parte de mi camino académico y personal.

En primer lugar, quiero dedicárselo a mi familia, por su amor, apoyo y paciencia a lo largo de mi carrera universitaria. Su confianza en mí ha sido un motor para seguir adelante en los momentos más difíciles. Gracias por estar siempre ahí.

También quiero dedicárselo a mis amigos y compañeros de estudio, por su compañía, motivación y enseñanzas. Han sido una fuente de inspiración y apoyo en todo momento. Gracias por compartir conmigo esta etapa de la vida.

Por último, quiero dedicar este trabajo a mis profesores, quienes han dejado una huella imborrable en mi formación académica. Gracias por su dedicación, por enseñarme a pensar y a razonar, y por compartir conmigo su conocimiento y experiencia.

Espero que este trabajo sea una forma de agradecerles a todos por el esfuerzo y la dedicación que han puesto en mí, y una muestra de mi compromiso por seguir aprendiendo y creciendo como persona y profesional.

Edwin

AGRADECIMIENTO

Agradezco a la Escuela Superior Politécnica de Chimborazo, por darnos la oportunidad de estudiar en su prestigiosa institución y brindarme todos los conocimientos necesarios para obtener una profesión y ser un miembro contribuyente para la sociedad.

A mi familia por su apoyo y comprensión, a mis compañeros de clase por compartir sus conocimientos, a mis amigos personales por acompañarme en los buenos y malos momentos, a mis profesores por instruirme en cada proyecto realizado.

Ayrton

Agradecemos a la Escuela Superior Politécnica de Chimborazo, por brindarme la oportunidad de estudiar en una institución de primer nivel, con un cuerpo docente excepcional y una variedad de recursos para ayudarme a crecer tanto académica como personalmente. Me siento bendecido por haber tenido la oportunidad de estudiar aquí y estoy seguro de que lo que he aprendido aquí me servirá durante toda mi vida.

A mi familia, quiero expresar mi profundo agradecimiento por estar siempre ahí para mí, apoyándome y dándome ánimo durante los momentos más difíciles. Su confianza en mí y su amor incondicional me han ayudado a superar muchos obstáculos y a alcanzar mis metas. Por todo esto, no tengo más que palabras de gratitud para con vosotros. Espero poder devolveros algún día todo lo que han hecho por mí y seguir haciéndoles sentir orgullosos de mí.
Con todo mi cariño y agradecimiento,

Edwin

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

RESUMEN

En el presente trabajo de integración curricular se planteó como objetivo implementar una aplicación descentralizada de votaciones electrónicas para la Cooperativa de Ahorro y Crédito "Nueva Esperanza". Se emplearon los métodos analítico, deductivo y estadístico, como técnicas de recolección de datos; se utilizó la revisión de documentación, el diagrama de Modelo y Notación de Procesos de Negocio (BPMN), encuesta adaptada al cuestionario de Seguridad con enfoque en Objetivo, Pregunta y Métrica (GQM) y métricas para evaluar la utilización de recursos. En cuanto a las herramientas, se utilizó el editor de código Visual Studio Code y Remix IDE, lenguaje de programación JavaScript tanto para el desarrollo del Backend y Frontend; para el desarrollo del contrato inteligente se utilizó el lenguaje Solidity y para la base de datos se usó PostgreSQL. Se utilizó la metodología de desarrollo de Proceso Racional Unificado (RUP) y el Lenguaje de Modelado Unificado (UML) durante el ciclo de desarrollo de la aplicación para trabajar con los usuarios en la definición de los casos de uso y requerimientos, logrando un ciclo de vida iterativo e incremental. Además, se aplicó el estándar ISO/IEC 25010 para medir la eficiencia de desempeño y seguridad del sistema. Los resultados obtenidos, en cuanto a la eficiencia de desempeño promedia un grado satisfactorio mientras que, el nivel de seguridad es del 94 %. Se concluye que el sistema cumple con los diferentes requerimientos del cliente. Se recomienda promover la utilización de normas para asegurar la calidad del proceso y del producto de software.

Palabras clave: <INGENIERIA DE SOFTWARE>, <BLOCKCHAIN>, <VOTACIONES ELECTRÓNICAS>, <METODOLOGÍA DE DESARROLLO RUP>, <APLICACIONES DESCENTRALIZADAS>, <ISO/IEC 25010>, <UTILIZACIÓN DE RECURSOS>, <SEGURIDAD>

SUMMARY

The objective of the present curricular integration work was to implement a decentralized application of electronic voting for the "Nueva Esperanza" Savings and Credit Union. Analytical, deductive and statistical methods were used as data collection techniques; The documentation review, the Business Process Model and Notation (BPMN) diagram, a survey adapted to the Security questionnaire with a focus on Objective, the Goal Question Metric (GQM) and metrics to evaluate the use of resources were used. Regarding the tools, the Visual Studio Code and Remix IDE code editor, JavaScript programming language, was used for both the development of the Backend and Frontend; Solidity language was used for the development of the smart contract and PostgreSQL was used for the database. The development methodology of the Rational Unified Process (RUP) and the Unified Modeling Language (UML) were used during the application development cycle to work with users in the definition of use cases and requirements, achieving a cycle of iterative and incremental life. In addition, the ISO/IEC 25010 standard was applied to measure the efficiency of performance and security of the system. The results obtained, in terms of performance efficiency, average a satisfactory degree, while the security level is 94%. It is concluded that the system meets the different customer requirements. It is recommended to promote the use of standards to ensure the quality of the process and the software product.

Keywords: <SOFTWARE ENGINEERING>, <BLOCKCHAIN>, <ELECTRONIC VOTING>, <RUP DEVELOPMENT METHODOLOGY>, <DESCENTRALIZED APPS>, <ISO/IEC DEVELOPMENT 25010>, <USE OF RESOURCES>, <SECURITY>.

Lic. Nelly Padilla P. Mgs
0603818717
DOCENTE FIE

INTRODUCCIÓN

El software ha sido un recurso muy importante a lo largo del tiempo, y su uso ha permitido optimizar y mejorar los procesos de trabajo en diversas áreas profesionales, incluyendo la ingeniería, construcción, matemática, educación, entre otros. Con el paso de tiempo, el software ha ido evolucionando y se han desarrollado nuevas metodologías y tecnologías que han contribuido a mejorar su calidad.

Entre las nuevas tecnologías surgidas en los últimos años, *Blockchain* se destaca como una de las más importantes. Es un pilar fundamental del Bitcoin y permite almacenar de manera segura y anónima todas las transacciones que ocurren dentro de este ecosistema financiero, manteniendo la integridad y transparencia de la información. Además, estas cualidades que otorga la *Blockchain* al *Bitcoin* dentro del ámbito financiero, han sido aplicadas a otras industrias, tales como: la medicina, cadena de productos, el internet de las cosas, etc. Y ha ayudado a mejorar sus procesos y flujos de trabajo brindando transparencia y trazabilidad.

Los procesos electorales es otra área para aplicar la *Blockchain*, con el objetivo de combatir la corrupción. La transparencia e inmutabilidad de los datos que ofrece el *Blockchain* contribuye a mejorar el proceso de conteo y resultados de una elección, así como su capacidad para mantener el anonimato y garantizar la seguridad. Estas últimas características se hacen posible porque la *Blockchain* utiliza criptografía para la firma de cada transacción u operación.

La Cooperativa de Ahorro y Crédito Nueva Esperanza, ubicada en la ciudad de Riobamba, realiza procesos electorales cada cuatro años entre sus socios y administrativos para elegir a las personas encargadas de gestionar la organización, el proceso es manual y no cuentan con un sistema de votaciones de ningún tipo, por lo que tienen que invertir en toda la logística y recurso humano. Desafortunadamente, este proceso manual puede resultar en errores que pueden afectar los resultados finales de la elección.

Para el desarrollo de la solución se tomó en cuenta los siguientes módulos, a continuación, se los menciona de forma breve.

El módulo de usuarios permitirá registrar todos los usuarios que formaran parte del proceso electoral; el módulo de elecciones, el cual permitirá crear un proceso electoral; el módulo de candidatos el cual permitirá escoger a los usuarios que formarán parte del proceso electoral; el

módulo de votos o votación que permitirá registrar los votos de los usuarios y, por último, el módulo de reportes, que permitirá visualizar los resultados de un proceso electoral.

Con respecto al presente documento, se encuentra dividido en cinco capítulos que se detallan a continuación:

CAPÍTULO I: Se presenta los antecedentes, la formulación del problema, la sistematización y finalmente, la justificación teórica tanto como aplicativa, objetivo general y los objetivos específicos.

CAPÍTULO II: Corresponde a los fundamentos teóricos, se aborda el tema de las votaciones electrónicas, la tecnología Blockchain, las aplicaciones descentralizadas, los métodos de comunicación entre las aplicaciones descentralizadas y la Blockchain, las herramientas de desarrollo y la Normas ISO/IEC 25010.

CAPÍTULO III: Se aborda el tipo de estudio, los métodos y técnicas, la operacionalización conceptual y metodológica de la seguridad y eficiencia de desempeño, la población y muestra, también se presenta el desarrollo del sistema utilizando la metodología RUP.

CAPÍTULO IV: Se presenta los resultados obtenidos en función a los objetivos planteados.

CAPÍTULO V: En el último capítulo se aborda las conclusiones y recomendaciones, de acuerdo con los objetivos planteados en el planteamiento del problema

CAPÍTULO I

1. PLANTEAMIENTO DEL PROBLEMA

En este capítulo se presenta los antecedentes, la formulación del problema, la sistematización y finalmente, la justificación (teórica y aplicativa) y los objetivos (general y específicos).

1.1. Antecedentes

Los procesos eleccionarios son una actividad para establecer individuos en cargos importantes dentro de una organización, entidad o estado democrático. Por otra parte, los sistemas de votación tradicionales son herramientas fundamentales para poder llevar a cabo las actividades que determinen un ganador. Así mismo, cuentan con recursos humanos designados para realizar tareas de recepción y conteo de votos. Además, también requieren recursos materiales, por ejemplo, las papeletas donde se presentan los candidatos y toda la logística necesaria para el proceso de votación.

Los sistemas de votaciones tradicionales se presentan como un proceso costoso y poco transparente debido a la mala planificación que puede existir en los organismos encargados para su organización. Además, estos sistemas tienen otros defectos, tales como: la presencia del error humano, personales poco capacitados o la carencia de un proceso poco ético, manipulación de los votos y la corrupción. Así mismo, esto desencadena en un alto consumo de recursos en cuanto a la logística, tales como: gastos en los kits electorales y su transporte, alto consumo de tiempo en el conteo de votos y en una auditoria (de ser necesaria), alto consumo de tiempo en la publicación de resultados, entre otros.

La incorporación de varias innovaciones tecnológicas (TICs) en los procesos eleccionarios ha llevado a la automatización de estos, reemplazando los procesos manuales con procesos sistematizados y dando como resultado el voto electrónico. Este cambio ofrece ventajas sobre el sistema de votación tradicional y hace que el proceso electoral sea transparente, eficiente y accesible. Sin embargo, varias personas no están de acuerdo con las ventajas que ofrece debido al riesgo potencial de fraude a gran escala. A pesar de ello, los sistemas de votación electrónica siguen en constante evolución y ofrecen una variedad de opciones. (Cuenca, Meza 2019).

Antagónicamente, el uso de los sistemas de votación electrónico soluciona gran parte de la problemática de un proceso electoral, pero trae consigo una serie de complicaciones. Por ejemplo,

el sistema Direct Recording Electronic (DRE, por sus siglas en inglés) promueve un proceso de votación, conteo y recuento de votos más eficiente, pero se ha probado que este sistema es vulnerable y contiene bugs que son difícilmente detectables (Bannet et al. 2004). Esto ocasiona una falta de confianza entre los sufragantes, especialmente con los sistemas en línea, ya que sus transacciones están expuestas a ciberataques, aprovechamiento de vulnerabilidades en los dispositivos, elevando riesgo de fraude y/o ataques.

La tecnología *Blockchain* tiene su primera concepción desde el año 1991, a partir del trabajo de Stuart Haber y W. Scott Stornetta, proponen el uso de funciones hash, esquemas de firma digital y generadores pseudoaleatorios para generar esquemas de sellado de documentos, que eviten la modificación y manipulación a través del tiempo (Haber y Stornetta 1991). Estas características forman parte de la *Blockchain* y fue mejorada en 1992, incorporando árboles Merkle, permitiendo la recopilación de más documentos en un solo bloque (Rodriguez 2018). Luego, en el año de 1992, Satoshi Nakamoto plantea la implementación de esta tecnología para la creación de *Bitcoin* y detalla como las características de la *Blockchain* puede ayudar a la red de *Bitcoin* para ser descentralizada, transparente, segura e inmutable (Nakamoto 2009). A partir de ello, esta tecnología empezó a tomar gran relevancia y ser aplicada en muchas más áreas que la financiera, tales como: las cadenas de producción, la seguridad, el área gubernamental, el Internet de las Cosas, etc.

Con respecto a estudios realizados sobre los sistemas de votación electrónica existe *FollowMyVote*, una compañía que ofrece una plataforma que usa la *Blockchain* para un desarrollo eleccionario, donde permite a los sufragantes enviar sus votos de manera remota y guardarlos de forma segura (Follow My Vote 2021).

Por otra parte, *Voatz* es otra compañía que ofrece un sistema de votaciones con el uso de la *Blockchain* y *Smartphones*, permiten a los sufragantes votar de forma anónima y verificando su identidad (Voatz 2017). Por último, *Polys*, una plataforma de votación basada en la *Blockchain*, proveída por *Kaspersky*, que utiliza algoritmos criptográficos, además ayuda a reducir los gastos económicos y de tiempo, para que las organizaciones se centren en recopilar y preparar propuestas (Kaspersky 2021).

La Cooperativa de Ahorro y Crédito “Nueva Esperanza” de la provincia de Chimborazo, desde sus inicios, ha venido llevando el proceso de votaciones de manera tradicional, basándose en las normas establecidas por la Superintendencia de economía popular y solidaria. Sin embargo, esto ha conllevado a una serie de inconvenientes que se listan a continuación:

1. Alto consumo de tiempo y recursos (económicos, materiales y humanos) para la ejecución del proceso electoral y su auditoría (de ser necesaria).

2. Perdida de la información
3. Demora de la emisión de los resultados
4. Baja participación de los socios en los procesos electorales

Ante lo expuesto, se considera necesaria la creación de una aplicación de voto electrónico con el uso de la tecnología *Blockchain*, para mejorar y agilizar el proceso de elecciones de los representantes para la asamblea general de la Cooperativa. La población que utilizará este sistema, son todos los socios pertenecientes a cada agencia que conforman a la Cooperativa en su totalidad.

1.2. Formulación del problema

¿En qué medida la aplicación descentralizada mejora y agiliza el proceso de votaciones de la cooperativa de ahorro y crédito "Nueva Esperanza"?

1.3. Sistematización del problema

¿Cómo es el proceso de elecciones que tiene una cooperativa de ahorro y crédito?

¿Qué tecnologías se utilizan en las aplicaciones descentralizadas de votaciones electrónicas?

¿Cuáles son los métodos transaccionales entre aplicaciones descentralizadas y la *Blockchain*?

¿Cuál es la arquitectura que se utiliza para el desarrollo de aplicaciones descentralizadas?

¿Cómo se evalúa la eficiencia y seguridad de las aplicaciones descentralizadas?

1.4. Justificación

1.4.1. Justificación teórica

Desde el surgimiento de *Bitcoin* y el boom de las criptomonedas, la tecnología *Blockchain* ha tomado gran popularidad en el mundo, usándose para manejar y almacenar las transacciones que ocurren dentro del ecosistema financiero de *Bitcoin.* Esto ha llevado a la *Blockchain* a ser una tecnología utilizada en varias áreas de la industria, por las ventajas y beneficios que ofrece. Esto ha llevado a una evolución de la tecnología, presentado diversos sistemas/propuestas con sus propias funciones, características y aplicaciones.

Las aplicaciones descentralizadas (por sus siglas DAPP), forman parte de la evolución del *Blockchain* y brindan beneficios tales como: código abierto, permitiendo que el código pueda ser auditado por terceros; compatibilidad con criptomonedas internas, con el uso de tokens para

cuantificar los créditos y transacciones de los participantes; transparencia, mediante el uso de consensos descentralizados entre todos los nodos del ecosistema; ausencia de puntos centrales de falla, debido a la característica de la descentralización, ya que todos los componentes se alojaran y ejecutarán en la cadena de bloques. (Cai et al. 2018).

La implementación de la tecnología *Blockchain* en diferentes áreas de la industria, presentan varias ventajas, entre las cinco más importantes y representativas se tiene:

a) La seguridad reforzada, ya que se crean registros que no pueden ser modificados y con cifrado *end-to-end*, ayudando a prevenir el fraude y actividades no autorizadas.
b) Mayor transparencia, la *Blockchain* permite registrar las transacciones idénticas en múltiples ubicaciones y todos los participantes de la red (con acceso autorizado) pueden acceder a la información, de esta forma se puede eliminar cualquier tipo de fraude.
c) Trazabilidad instantánea, la *Blockchain* crea una ruta documentada que muestra la procedencia de un activo en cada paso que ha recorrido en la red
d) Mayor eficiencia y velocidad, las transacciones se pueden completar de forma más rápida y eficiente, evitando el papeleo o trámites.
e) La automatización, las transacciones dentro del entorno *Blockchain* pueden ser automatizadas con los denominados contratos inteligentes (del inglés *Smart Contracts*), ayudando a reducir la intervención humana o de terceros para verificar el cumplimiento de términos de un contrato (IBM 2021).

Las características descritas, han llevado a crear sistemas resistentes a la censura, transparentes e inmutables, ya que no se puede cambiar la información de un bloque a menos que todos los participantes estén de acuerdo (seguros de su decisión), además la *Blockchain* utiliza la criptografía asimétrica para firmar cada transacción. (Rojo 2019).

En definitiva, si la tecnología *Blockchain* se incorpora en el desarrollo de un sistema de votación electrónica o en un sistema ya implementado, se puede aprovechar sus características y beneficios para evitar fraudes electorales, garantizar una auditoria mucho más rápida, automatizar todas las tareas que requieren intervención humana y ahorrar dinero invertido en logística y recursos utilizados.

1.4.2. Justificación aplicativa

Es necesario la creación de la aplicación descentralizada para el proceso eleccionario de representantes para la asamblea general de la Cooperativa de Ahorro y Crédito Nueva Esperanza, puesto que reduce el tiempo de la publicación de los resultados, ahorro de costos en la logística y

mayor participación de los socios. Este proceso se podrá realizar desde los distintos dispositivos informáticos como lo son computadoras portátiles o dispositivos móviles, este último es el más utilizado en la actualidad.

Cabe recalcar que el problema planteado se encuentra incluido dentro de las líneas de investigación de la ESPOCH tales como: ingeniería de software, proceso de desarrollo de software basado en el ámbito de análisis y diseño de software. Las líneas de investigación se encuentran dentro del eje transversal de las tecnologías de información y comunicación. A su vez, se incluye en el Plan de Creación de Oportunidades (por sus siglas PCO) el mismo que se ajusta a los objetivos 14 y 15, aquellos que se detallan a continuación:

- Objetivo 14. Fortalecer las capacidades del Estado con énfasis en la administración de justicia y eficiencia en los procesos de regulación y control, con independencia y autonomía. Dentro de este objetivo se contempla la política 14.2 Potenciar las capacidades de los distintos niveles nacionales y la presentación de servicios con calidad.
- Objetivo 15. Fomentar la ética pública la transparencia y la lucha contra la corrupción. Dentro de este objetivo se contempla la política 15.1 fomentar la integridad pública y la lucha en contra de la corrupción en coordinación interinstitucional efectiva entre todas las funciones del Estado y la participación ciudadana.

La aplicación descentralizada estará compuesta por los siguientes módulos:

MÓDULO DE SOCIOS: La aplicación llevará el control de los socios, tanto como de acceso, como también para el almacenamiento de información, estableciendo sus roles y permisos al momento de interactuar con la aplicación.

MÓDULO DE ELECCIONES: La aplicación podrá agregar, modificar y eliminar una elección realizadas por el usuario administrador detallando los parámetros necesarios con los que se llevará a cabo dicho proceso.

MÓDULO DE VOTOS: La aplicación registrará los votos emitidos controlando que el voto sea único y una vez que se haya enviado el voto este no se pueda cambiar.

MÓDULO DE CANDIDATOS: La aplicación llevará el control de los candidatos, así como el registro, eliminación y almacenamiento de información al momento de interactuar con este módulo.

MÓDULO DE REPORTES: La aplicación permitirá mostrar la información y los resultados de una elección, por ejemplo, la cantidad de votos de cada candidato, la cantidad de votos nulos, la cantidad de votos por agencia, entre otros.

1.5. Objetivos

1.5.1. Objetivo General

Desarrollar una aplicación descentralizada de votaciones electrónicas con el uso de la Blockchain para la Cooperativa de Ahorro y Crédito Nueva Esperanza.

1.5.2. Objetivos Específicos

- Describir los métodos utilizados de comunicación entre aplicaciones descentralizadas y la Blockchain.
- Analizar el proceso electoral que se lleva a cabo en las cooperativas de ahorro y crédito, así como los actores que intervienen en este.
- Desarrollar el módulo de usuarios, el módulo de elecciones, el módulo de votos, el módulo de candidatos y el módulo de reportes.
- Evaluar la seguridad y la utilización de recursos de la aplicación descentralizada mediante el estándar ISO 25010.

CAPITULO II

2. FUNDAMENTOS TEÓRICOS

En este capítulo se definen los fundamentos teóricos necesarios para el desarrollo de una aplicación descentralizada para las votaciones en una Cooperativa de Ahorro y Crédito.

2.1. Votaciones Electrónicas

El voto electrónico, conocido como e-voting (del inglés *electronic voting*), es definido por (Prince, Jolías y Lacabanne 2012) como la incorporación de las Tecnologías de la Información y Comunicación (por sus siglas TIC) al proceso de sufragio de manera total o parcial. De esta manera, se automatizan los procesos de construcción y actualización del registro electoral, la emisión del voto, escrutinio, y se proporciona una red de comunicaciones para la transmisión y consolidación de los resultados electorales. Estas características marcan la diferencia entre una votación electrónica y aquellos procesos electorales que se sirven de metodologías tradicionales.

Por su parte, (Smith 2009) define al voto electrónico como un sistema donde el votante registra directamente sus preferencias, usando un dispositivo electrónico; ya sea una máquina diseñada específicamente para ello, una computadora personal o incluso un teléfono celular.

Según (Hernández Trejo 2011) el voto electrónico es un recurso tecnológico que presenta algunas modalidades de acuerdo con su implementación y ejecución, clasificándolas en dos tipos:

- La votación electrónica remota u online: Se desarrolla con el uso de computadoras, teléfonos celulares, televisiones digitales o dispositivos electrónicos que tengan acceso a internet. Permiten a los sufragantes ejercer su derecho al voto desde cualquier lugar.
- La votación electrónica presencial u offline: El sufragante se traslada de forma física o presencial a su lugar de votación para ejercer su derecho al voto, apoyado de recursos tecnológicos e informáticos para cumplir con su tarea.

De acuerdo con (Reniu 2011) la inclusión del voto electrónico a un proceso electoral presenta beneficios, tales como: la modernización de los procesos electorales, reducción de los costes económicos e incremento de la participación de determinados sectores sociales. Así mismo, se presentan certezas, tales como: múltiples aplicaciones participativas, necesidad de autoridades electorales específicas y coexistencia con el voto tradicional e implementación gradual. Es necesario recalcar que una múltiple aplicación participativa, se refiere a que aplicar el voto electrónico es altamente recomendable (mejorar los procesos participativos) en cualquier tipo de

escenario como consultas ciudadanas, procesos electivos civiles, de universidades, partidos políticos, entidades profesionales públicas y privadas. Por otra parte, la necesidad de autoridades electorales específicas se refiere a la inclusión de expertos en el recurso humano del proceso electoral, debido a la complejidad que presenta incluir las TICs a los procesos electorales. Por último, la coexistencia con el voto tradicional e implementación gradual plantea que el voto electrónico debe considerarse como una opción o alternativa al voto tradicional, es decir, que estas soluciones tecnológicas sean complementarias, para no centrarse en una sola tecnología y optar por diferentes soluciones tecnológicas, en función a las necesidades, intereses o capacidades de los entes organizadores y sufragantes.

Conviene subrayar a las TICs como un aspecto fundamental de las votaciones electrónicas, ya que este recurso se fundamenta en las tecnologías existentes, para una implementación novedosa y de nuevas características, que satisfagan las demandas de seguridad y transparencia presentes en un proceso electoral. Una de esas tecnologías es la *Blockchain* o cadena de bloques, debido a su transversalidad de ser aplicado en varias áreas de la industria.

2.2. Tecnología *Blockchain*

La tecnología *Blockchain* permite a los usuarios almacenar de forma permanente, simultánea y pública los datos de una transacción (bloque) dentro de una cadena de bloques (libro distribuido) que es compartido por distintos actores de la red, también denominados nodos. La agrupación de nodos da el nombre de registro distribuido, por la participación y dispersión de los nodos en la red, aunque también es llamado registro descentralizado, debido a que no existe una entidad central que intervenga en las operaciones o transacciones que ocurren en la red (Ibáñez Jiménez 2018).

De acuerdo con (Rojo 2019), la *Blockchain* es un conjunto de bloques enlazados entre sí de forma consecutiva por el hash del bloque anterior, para que los bloques puedan ingresar al registro distribuido deben ser validado por nodos validadores (también llamados mineros). Esto genera varías características tales como: ahorro de costes y tiempo, seguridad, transparencia, confianza y transacciones en tiempo real. Por otra parte, (Drescher 2017)menciona a la suite de tecnología de Blockchain, está se conforma por los elementos que se indica en la **Figura 1-2** y se describen a continuación:

a) Lógica de almacenamiento: se ocupa de mantener todo el historial de datos de transacciones actualizado y protegerlo de manipulaciones o falsificaciones, para mantener la integridad del sistema. Se logra estas características al mantener un almacén de datos inmutable, agregando;

bloques validados por un protocolo de consenso y la estructura de datos de la cadena de bloques.

b) Lógica de consenso: Dado que todos los nodos (mineros) del sistema distribuido mantienen su historial de datos de transacciones de forma independiente, su contenido puede diferir debido a retrasos u otras adversidades en el paso de mensajes a través de una red, en la que cada rama representa una versión idéntica del historial de transacciones. En resumen, esta lógica hace que todos los nodos del sistema sean eventualmente consistentes al hacer que elijan la versión idéntica del historial de transacciones que une el mayor esfuerzo colectivo.

c) Lógica de procesamiento de datos: Garantiza que solo se agreguen datos de transacciones válidos al historial mantenido colectivamente. A su vez, cada nodo del sistema de forma aislada puede realizar la validación de los datos de la transacción. Sin embargo, algún nodo podría cometer errores al validar los datos de transacciones, esto amenaza a la integridad de todo el sistema. Por ello, el procesamiento de datos involucra una sofisticada mecánica que contiene la validación de nuevos bloques o sus cabeceras, con el apoyo de la arquitectura P2P (por sus siglas en inglés, Peer-to-Peer), peer control y competencia. Se debe agregar que, la competencia se apoya en las fuerzas de recompensa y castigo.

d) Criptografía asimétrica: Este elemento es muy útil en la parte de seguridad, se usa para la identificación, autenticación de usuarios y autorización de transacciones. Por otra parte, los números de cuenta en la cadena de bloques son en realidad claves criptográficas públicas. Se debe agregar que, solo quien posee la clave privada correspondiente puede acceder a la propiedad que está asociada a una cuenta. Además, los datos de transacciones que contienen una firma digital (generada por una clave privada) son válidos y pueden transferir la propiedad de una cuenta a otra. En resumen, la criptografía asimétrica siempre utiliza dos claves complementarias, la clave pública y privada.

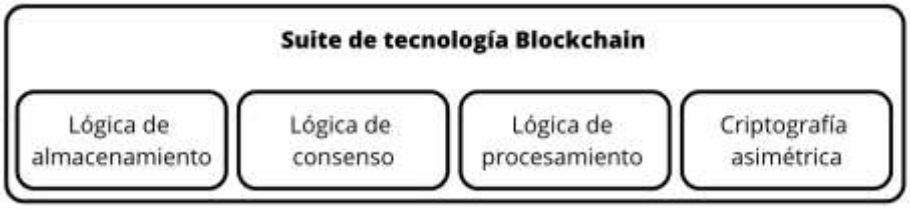


Figura 1-2: Suite de tecnología Blockchain

Fuente: Drescher 2017

Realizado por: Avalos, A.; Manzano. E. 2023

La suite tecnológica de Blockchain brinda una estructura para el correcto funcionamiento de la Blockchain, abriéndola a una amplia gama de áreas de aplicación, tales como: financiero

(mediante criptomonedas), en las cadenas de producción, bienes raíces, en la salud, votaciones, la web y la incorporación de esta tecnología en aplicaciones web tradicionales dando nacimiento a las aplicaciones descentralizadas.

2.3. Aplicaciones descentralizadas

La primera implementación de Blockchain se la hizo en el área financiera, a medida que la *Blockchain* fue adaptándose a diferentes áreas surgieron varias generaciones, tales como: Blockchain 1.0, Blockchain 2.0, Blockchain 3.0 y Blockchain 4.0. Las aplicaciones descentralizadas (por sus siglas en ingles DAPPS, *Decentralized Applications*) se encuentran en la generación de la *Blockchain* 3.0, en esta generación se pasó de utilizar la *Blockchain* en contratos inteligentes y registros distribuidos al desarrollo de aplicaciones que interactúen con la *Blockchain* para almacenar la información de manera íntegra e inmutable (Cai et al. 2018).

Para el desarrollo de una aplicación descentralizada (DAPP, por sus siglas en inglés) intervienen conceptos importantes, tales como: la arquitectura sobre la que se rigen, el uso de contratos inteligentes, la utilización de redes Punto a Punto para el funcionamiento de una aplicación descentralizada, los protocolos de consenso que pueden intervenir para validar las transacciones y una nueva tendencia que surge debido a la incorporación de este tipo de aplicaciones en el entorno web (Web 3.0). Estos conceptos se verán desarrollados en los siguientes apartados.

2.3.1. Arquitectura

De acuerdo con (Kasireddy 2021) una DAPP es muy diferente una aplicación Web 2.0 porque estas aplicaciones se dividen en lo general en tres componentes, los cuales son: la base de datos, el back-end y el front-end. Por otro lado, las DAPPs al usar la Blockchain no requiere de una base de datos centralizada y mucho menos de un servidor centralizado en el cual se almacena la lógica del Back-End.

La arquitectura de una DAPP según (Kasireddy 2021), se lo ilustra en la **Figura 2 – 2**:

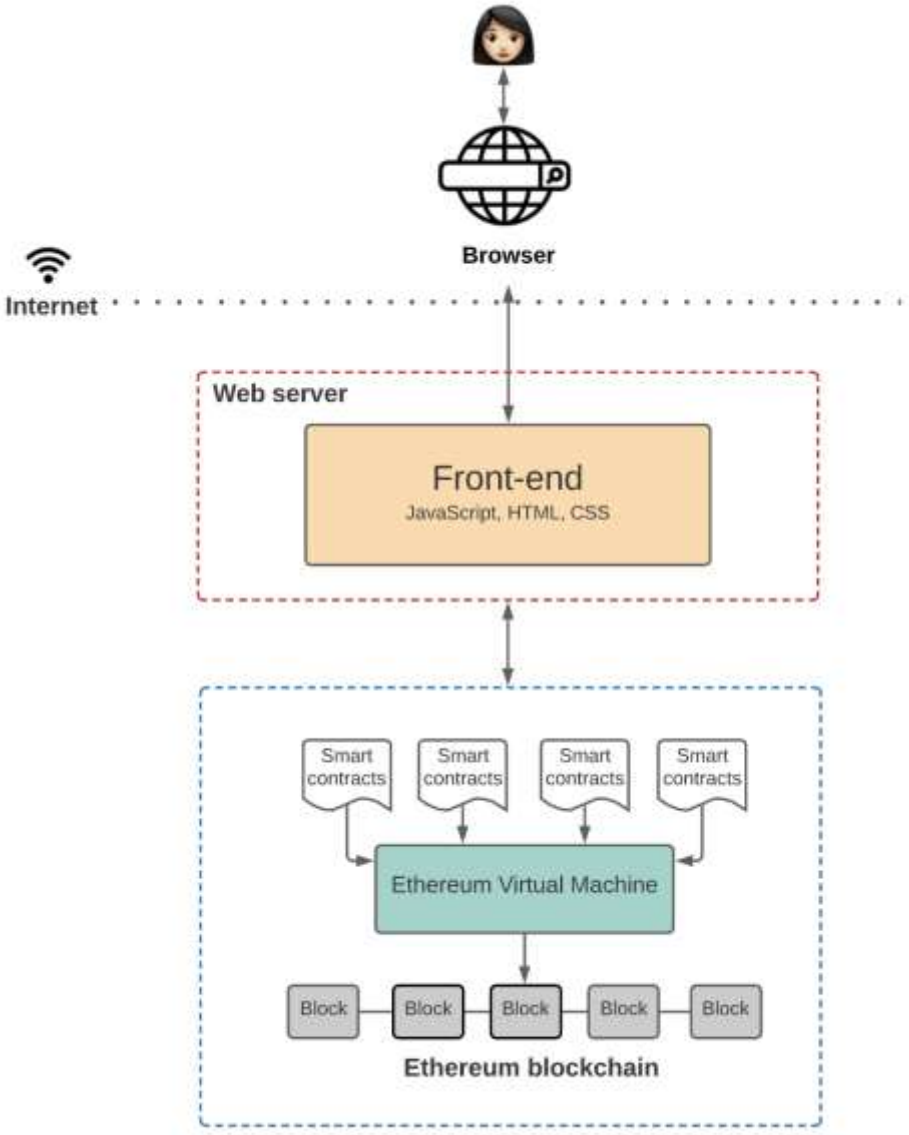


Figura 2-2: Arquitectura de una DAPP

Fuente: (Kasireddy 2021)

Como se puede ver en la **Figura 2 - 2**, la arquitectura de un DAPP tiene cuatro componentes los cuales se describirán a continuación:

a) Blockchain (cadena de bloques): es un ordenador global el cual es mantenido por una red P2P (del inglés, *Peer-to-Peer*), dentro de esta todos pueden acceder y escribir, pero se encuentra restringido por las reglas de consenso.

b) Contratos inteligentes: es un código informático que se ejecuta automáticamente en la *Blockchain* en la cual se da un cambio de estado es la misma.

c) Máquina virtual Ethereum: sobre la *Ethereum Virtual Machine* (EVM, por sus siglas en inglés) se ejecutan los contratos inteligentes, estos son escritos en lenguajes como Solidity o Vyper, pero se deben compilar a *bytecode* para que se puedan ejecutar.

d) Front-End: es la interfaz de usuario, en este componente se realiza la interacción con el usuario, además este componente se comunica con la *Blockchain* para utilizar los contratos inteligentes.

Según (Shanker 2019) una DAPP está compuesta por una interfaz Frontend (HTML, CSS, Bootstrap) y una interfaz Backend (Web3.js, JavaScript). Para que estas interfaces puedan interactuar se conectan a MetaMask, este sirve de puente y permite ejecutar aplicaciones descentralizadas utilizando el procedimiento JSON RPC, el cual permite interactuar a la DAPP con la EVM.

2.3.2. Contratos Inteligentes

Los contratos inteligentes (del inglés *Smart Contracts*), son programas capaces de ejecutarse de forma automática una vez que se cumplen ciertas condiciones, además no necesitan intermediaros para su resolución (Rojo 2019). Lo que diferencia un contrato inteligente de un programa informático tradicional son sus resultados, ya que a diferencia de los tradicionales estos son consensuados por un conjunto de computadores comunicados entre sí y no son simplemente obtenidos tras la ejecución del código. Los resultados se escriben en un registro público (*Blockchain*) de forma que se puedan detectar posibles alteraciones, además este registro es mantenido por una parte de los ordenadores del sistema. (Arroyo Guardeño, Díaz Vico y Hernández Encinas 2019).

Hay que mencionar que los contratos inteligentes presentan características tales como: públicos, ya que se almacenan en la *Blockchain* y cualquier usuario puede acceder a la misma; inmutables, al estar almacenados en la cadena de bloques la información no puede ser modificada; configurables, cuando se suben los contratos a la *Blockchain* solo pueden ser modificados por su dueño; distribuido, los mineros son quienes los ejecutan y se evita cualquier tipo de censura o burocracia, porque no se puede saber la nacionalidad del minero que ejecute el contrato, ni las leyes que se aplican en su país (Rojo 2019).

Por otra parte, (Rojo 2019) menciona que los contratos inteligentes fueron popularizados a través del criptoproyecto *Ethereum*, haciéndolos sencillos y posibles de implementar, a su vez estos podían ser implementados en la red de *Bitcoin*, pero era muy complejo realizarlo y la *Blockchain* de *bitcoin* no estaba pensada para funcionalidades tan complejas.

Se debe agregar que uno de los fundadores de *Ethereum* definió a los contratos inteligentes como una forma que tienen todas las personas del mundo para hacer negocios entre ellos, sin importar su idioma y la moneda que utilicen (Rojo 2019).

Por último, para ejemplificar el comportamiento de un contrato inteligente se supondrá un contrato que bloquee un auto en caso de que la mensualidad del préstamo concedida por el banco no sea cancelada por el propietario, el algoritmo sería el siguiente: (i) El propietario realiza la operación de abrir el automóvil, la operación se transmite a todos los nodos de la red (el coche forma parte de esos nodos); (ii) Cada nodo comprueba en el registro de la *Blockchain* si el dueño cancelo su último pago, el resultado es denegado si el dueño no ha cancelado; (iii) El resultado de denegación se almacena (por parte de los mineros/nodos) en un nuevo bloque dentro de la red; (iv) Al detectar la escritura en el registro, el auto recibe la notificación y rechaza abrirse informando el motivo al dueño. Para ilustrar mejor, en la **Figura 3 – 2** se muestra otra aplicación de un contrato inteligente para la adquisición de una casa (Arroyo Guardeño, Díaz Vico y Hernández Encinas 2019).

Figura 3-2: Funcionamiento de un Contrato Inteligente

Fuente: Seaz J., 2023

Realizado por: Avalos, A.; Manzano. E. 2023

2.3.3. Redes Punto a Punto

Según (Steinmetz y Wehrle 2005) una red Punto a Punto, conocida como *Peer-to-Peer* (P2P, por sus siglas en ingles), es un paradigma para la comunicación en Internet que original y exclusivamente se diseñó para aplicaciones pragmáticas (y legalmente controvertidas) de intercambio de archivos. Los mecanismos punto a punto pueden usarse para acceder a cualquier tipo de recursos distribuidos y pueden ofrecer nuevas posibilidades para aplicaciones basadas en Internet.

Como se ilustra en la **Figura 4 – 2**, otro rasgo de un sistema Punto a Punto es ser autoorganizado de entidades iguales y autónomas (pares), tiene como objetivo el uso compartido de recursos distribuidos en un entorno de red (internet) evitando los servicios centrales. En resumen, es un sistema con autoorganización y uso de recursos completamente descentralizados.

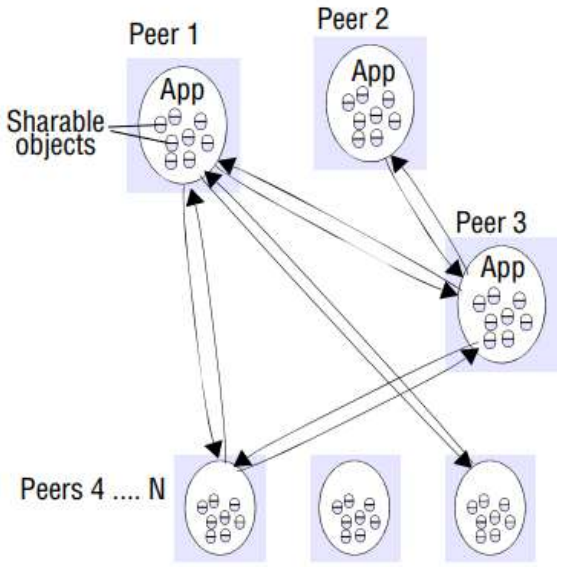


Figura 4-2: Red P2P
Fuente: Coulouris, 2017

2.3.4. Protocolos de consenso

En la *Blockchain*, el proceso de armar un bloque de transacciones y sumarlo definitivamente en la cadena se llama sellado o minado. Cuando un bloque queda sellado, la información que contiene pasa a formar parte de la cadena de forma permanente, inmutable e inalterable. Según (Blockchain Federal Argentina 2019), los protocolos de consenso son mecanismos que regulan los acuerdos existentes entre todos los nodos de la red para sellar o validar los bloques e incorporarlos a la cadena. A continuación, se describen tres de los protocolos de consenso más importantes:

a) Prueba de trabajo: Uno de varios protocolos de consenso que existen, posiblemente uno de los más populares. También denominado *Proof of Work* (*PoW*, por sus siglas en inglés), o Prueba de Trabajo. En este modelo todos los nodos son pares iguales en la red, y todos compiten para sellar un bloque antes que el resto para conseguir una criptomoneda como recompensa. Para cumplir con este proceso, es necesario solucionar un algoritmo complicado. Aquel que logre resolverlo y añadir un bloque a la cadena de bloques recibirá una recompensa en forma de criptomoneda. Pero para realizar ese trabajo se necesita un alto nivel de

procesamiento, lo que se termina traduciendo en un mayor costo energético y de hardware(Blockchain Federal Argentina 2019).

b) Prueba de autoridad: En el modelo de *Proof of Authority* (PoA, por sus siglas en inglés) solo hay una cantidad determinada de nodos que están autorizados a resolver el sellado de bloques. Este protocolo no está basado en la competencia, sino en el hecho de que un grupo reducido tiene permisos para agregar bloques a la cadena se turne para hacerlo. Como aquí no hay necesidad de resolver algoritmos complejos, la cantidad de procesamiento es mínima. Por eso se considera a estos modelos como livianos y más eficientes con relación a consumo energético. La otra gran característica es que generalmente en modelos de Prueba de Autoridad no hay circulación de criptomonedas con valor económico, ya que en realidad no es necesaria una recompensa por esa participación (Blockchain Federal Argentina 2019).

c) Prueba de participación: El modelo *Proof of Stake* (PoS, *por sus siglas en inglés*) es el segundo método de consenso más frecuente en la Blockchain. A diferencia de PoW no genera una competencia entre nodos, la lotería selecciona un nodo para que sea el encargado de resolver el siguiente bloque (Salimitari y Chatterjee 2018). Este nodo se conoce como "minero" y es seleccionado de manera determinística en base a su participación en la red. (Debus 2017). El nodo seleccionado usa una firma digital para demostrar su propiedad sobre la participación en lugar de resolver un problema de hash complejo, de esta forma no necesita altos recursos computacionales (Debus 2017). Es un protocolo de consenso que busca ahorrar energía mediante un incentivo monetario, pero al requerir una mayor cantidad de participación de nodos, puede llevar a una centralización de la cadena de bloques (Salimitari y Chatterjee 2018) y no necesariamente lo hace más eficiente que la prueba de trabajo que PoW (Swan 2018).

2.3.5. Web 3.0

La Web 3.0 (abreviada como Web3) es una nueva tendencia que ha surgido en los últimos años donde se plantea un nuevo tipo de servicio de internet construido juntamente con la *Blockchain* o cadena de bloques descentralizada. También es definida como una internet que es propiedad de los desarrolladores y los usuarios, coordinada por *tokens*.

Las personas que impulsan el concepto de la web3 plantean la adopción de esta tecnología en diversos tipos de sistemas o aplicaciones como puede ser en la creación de redes sociales descentralizadas, en los videojuegos *play to earn* (recompensan a los jugadores por jugar), plataformas NFT que permiten a los usuarios comerciar con arte digital y otros tipos de áreas de

la industria y la sociedad para de esta manera dar paso a un ecosistema sin intermediarios (Roose 2022).

2.4. Métodos de comunicación entre aplicaciones descentralizadas y la Blockchain

La invocación remota (del inglés, *remote invocation*) es el paradigma de comunicación más común para conectar una aplicación descentralizada con la Blockchain, cubren una gran variedad de métodos basados en intercambios bidireccionales entre las entidades que participan en una aplicación descentralizada y la *Blockchain*. Estos métodos dan como resultado la llamada a una operación, procedimiento o método remoto (Coulouris 2017).

Son varios los métodos que nos ofrece la invocación remota, entre los más destacados tenemos a la llamada de procedimiento remoto y la invocación de método remoto. Estos métodos se profundizarán en los siguientes apartados.

2.4.1. Llamada de procedimiento remoto

El método de llamada de procedimiento remoto (RPC, por sus siglas en inglés *remote procedure call*) permite la abstracción de llamadas a procedimientos usadas en la programación convencional para entornos descentralizados. Como resultado, los procedimientos almacenados en máquinas o nodos remotos se pueden llamar como si fueran procedimientos almacenados en una dirección o nodo local (Coulouris 2017).

De acuerdo con (Coulouris 2017) la semántica de llamadas en RPC se sirve de protocolos de solicitud y respuesta e implementan métodos para invocar operaciones remotas. Los métodos de invocación brindan tres opciones principales que se describen a continuación:

a) Mensaje de solicitud de reintento: Controla si se retransmite el mensaje de solicitud hasta que se recibe una respuesta o se asume que el servidor ha fallado.
b) Filtrado de duplicados: Controla la utilización de retransmisiones y el filtrado de solicitudes duplicadas en el servidor.
c) Retransmisión de resultados: Controla la existencia de un historial de mensajes de resultados para permitir la retransmisión de resultados perdidos sin volver a ejecutar las operaciones en el servidor.

La implementación de RPC requiere una serie de componentes software que se ilustran en la **Figura 5 – 2**. Se divide en dos partes, en el cliente y el servidor, por parte del cliente se encuentra el proceso principal que accede a un servicio y por cada procedimiento en la interfaz del servicio se brinda un procedimiento *stub*. El procedimiento *stub* se comporta como un proceso local para

el cliente, pero a cambio de ejecutar la llamada, convierte el identificador del procedimiento y sus argumentos en un mensaje de solicitud que serán enviados a través del módulo de comunicación con destino al servidor. Por último, cuando la solicitud llega se deshace esa conversión (Coulouris 2017).

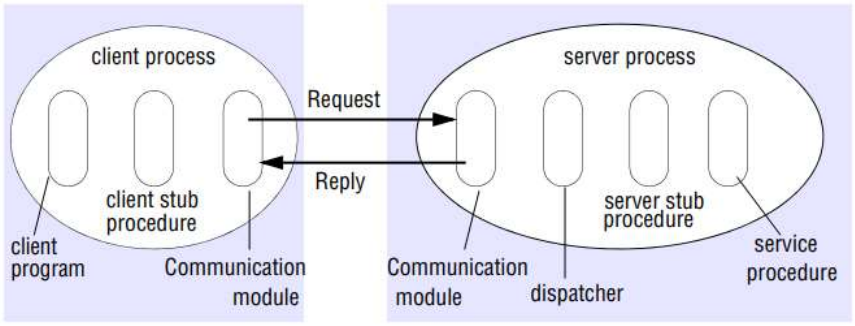


Figura 5-2: Esquema de implementación en RPC

Fuente: *Coulouris*, 2017

Por otro lado, se tiene al servidor y su proceso principal que se apoya en un procedimiento *stub*, un despachador y un procedimiento de servicio para cada procedimiento que se halle en la interfaz de servicio. La función del despachador es seleccionar uno de los procesos *stub* del servidor que coincida con el identificador del procedimiento suministrado por el mensaje de solicitud, luego el proceso *stub* del servidor deshace la conversión de los argumentos de la solicitud y llama al procedimiento de servicio correspondiente para calcular los valores que se retornarán en el mensaje de respuesta. El contenido de los mensajes de solicitud y respuesta son los mismos y se ilustran en la **Figura 6 – 2**. Por último, el módulo de comunicación del servidor enviará el mensaje de respuesta al cliente (Coulouris 2017).

messageType	*int (0=Request, 1= Reply)*
requestId	*int*
remoteReference	*RemoteRef*
operationId	*int or Operation*
arguments	*// array of bytes*

Figura 6-2: Formato de los mensajes de solicitud y respuesta

Fuente: *Coulouris*, 2017

2.4.2. Invocación de método remoto

El Remote Method Invocation (RMI, por sus siglas en inglés) es una tecnología desarrollada por Sun que permite la colaboración entre objetos localizados remotamente. En lugar de que los objetos se comuniquen a través de protocolos estándares de red programados por el usuario, un objeto cliente envía una solicitud de datos a un objeto ubicado en un servidor. El objeto remoto luego accede a fuentes de datos, como bases de datos y otros objetos, para preparar la información requerida y enviarla de vuelta al cliente. La intención es que la interacción sea lo más similar posible a las solicitudes realizadas localmente (Universidad de Alicante 2003).

Figura 7-2: Arquitectura RMI
Fuente: (Universidad de Alicante 2003)
Realizado por: Avalos, A.; Manzano. E. 2023

En la **Figura 7-2** se pueden ver las diferentes capas que se utilizan en la arquitectura RMI, la primera capa es la de aplicación, y se corresponde con la implementación real de las aplicaciones cliente y servidor. En este proceso se realizan llamadas a nivel alto para acceder y compartir objetos remotos. Cualquier aplicación que desee hacer disponibles sus métodos para su acceso por parte de clientes remotos debe declararlos en una interfaz que extienda java.rmi.Remote. La interfaz se utiliza para identificar un objeto como accesible de forma remota. Una vez que los métodos han sido implementados, el objeto debe ser compartido, ya sea de manera implícita si extiende la clase UnicastRemoteObject (del paquete java.rmi.server) o de manera explícita mediante una llamada al método exportObject() del mismo paquete (Sharan 2018).

La capa 2 es la capa *proxy*, o capa stub-skeleton. Esta capa es la que interactúa directamente con la capa de aplicación. Todas las llamadas a objetos remotos y acciones sobre sus parámetros y retorno de objetos tienen lugar en esta capa (Universidad de Alicante 2003).

La capa 3 es la de referencia remota, es responsable del manejo de la parte semántica de las invocaciones remotas. También es responsable de la gestión de la replicación de objetos y realización de tareas específicas de la implementación con los objetos remotos, como el establecimiento de las persistencias semánticas y estrategias adecuadas para la recuperación de conexiones perdidas. En esta capa se espera una conexión de tipo *stream* (*stream-oriented connection*) desde la capa de transporte (Universidad de Alicante 2003).

La capa 4 es la de transporte. Es la responsable de realizar las conexiones necesarias y manejo del transporte de los datos de una máquina a otra. El protocolo de transporte subyacente para RMI es JRMP (*Java Remote Method Protocol*), que solamente es "comprendido" por programas Java (Universidad de Alicante 2003).

2.5. Herramientas de desarrollo

En esta sección se describen los lenguajes de programación, librerías, frameworks y entornos de desarrollo integrados que se utilizaran como herramientas de desarrollo.

2.5.1. Lenguajes de programación

Los lenguajes de programación es un lenguaje informático para escribir o desarrollar programas de computadoras, mediante la implementación de algoritmos que el computador puede entender (Aguilar 2008). En este apartado se describirán los lenguajes de programación a utilizar para el desarrollo del sistema de votaciones.

2.5.1.1. JavaScript

JavasScript es un lenguaje de alto nivel adaptado a los navegadores web y posteriormente adaptado para la construcción de páginas web, aplicaciones web, aplicaciones de escritorio, aplicaciones móviles y la construcción de librerías, entre los usos más importantes (Haverbeke 2018). Es un lenguaje compacto y muy flexible utilizado para desarrollar varias herramientas y liberando una cantidad de funcionalidades adicionales para este lenguaje. En estas funcionalidades se incluye:

- Interfaces de Programación de Aplicaciones del Navegador (por sus siglas API, del inglés Application Programming Interface) implementadas dentro de los navegadores para ofrecer funcionalidades tales como: manipular el contenido de un archivo html o DOM (del inglés Document Object Model), establecer estilos en cascada, manipulación de video de una cámara web, generar gráficos en tercera dimensión y manipular el sonido.

- APIs de terceros, proporcionadas por proveedores de contenidos para incorporar nuevas funcionalidades a un sitio web.
- Librerias y frameworks de terceros aplicables a HTML para construir y desplegar sitios y aplicaciones de una manera mucho más rápida (MDN contributors 2023).

(MDN contributors 2022) describe a Javascript como un lenguaje ligero, interpretado, orientado a objetos, dinámico, multiparadigma, basado en prototipos. Este lenguaje admite estilos de programación funcional, imperativa y orientado a objetos. El dinamismo de JavasScript permite la construcción de objetos en tiempo de ejecución, listas de parámetros variables, variables de función, recuperación de código fuente y creación dinámica de scripts.

2.5.1.2. Solidity

Según (Rojo 2019) *Solidity* es un lenguaje de programación de código abierto y alto nivel que se utiliza para implementar contratos inteligentes. Es influenciado por C++, Python y JavaScript y se creó específicamente para la Máquina Virtual de Ethereum (EVM). Nació cuando *Vitalik Buterin* propuso *Ethereum* y varias personas se unieron al proyecto, entre ellos *Gavin Wood*, cuya aportación fue un lenguaje de programación propio para contratos inteligentes (*Solidity*).

Si bien se pueden desarrollar contratos inteligentes con cualquier otro lenguaje, *Solidity* llegó para quedarse ya que trae consigo muchas características que ayudan a desarrollar contratos inteligentes más eficientes y sencillos para los programadores, por ello se lo considera como uno de los lenguajes más importantes para la creación de contratos inteligentes (Rojo 2019).

Solidity tiene implementado el paradigma orientado a objetos, contiene tipos estáticos, soporta la herencia y tipos de datos complejos definidos por el usuario, entre otras características. Solidity ha sido usado para crear contratos en procesos de votación, subastas a ciegas, billeteras de múltiples firmas y *crowdfunding*. Para implementar contratos se debe usar la última versión de este lenguaje, debido a correcciones de seguridad, cambios importantes y nuevas funciones disponibles (Ethereum 2021).

2.5.2. Librerías

Las librerías de programación son conjuntos de archivos de código que se utilizan para desarrollar software. Su objetivo es facilitar la programación, al proporcionar funcionalidades comunes que ya han sido resueltas previamente por otros programadores (Waskom 2021). En este apartado se describirán las librerías de programación a utilizar para el desarrollo del sistema de votaciones.

2.5.2.1. React.JS

React.js es una librería de código abierto para JavaScript, su utilidad es la de construir interfaces de usuario de una sola página para aplicaciones móviles y web. También, permite el desarrollo de componentes UI reutilizables (React 2022). A continuación, se destacan algunas características principales:

a) Declarativo: al contrario que otros lenguajes, como jQuery, React.js es declarativo, además permite mediante la modificación de las propiedades de los componentes que se produzca un cambio en la funcionalidad.

b) Basado en componentes: React.js está basado en componentes. Éstos son representados como clases que heredan de Component y todos los componentes definen un método render() que se encarga de establecer el contenido del componente para renderizarlo. Además, está permitido el uso de JSX, una extensión que permite emplear etiquetas HTML dentro de JavaScript, aumentando la expresividad del lenguaje.

c) Propiedades: son los atributos de configuración de cada componente, también se conocen como "PROPS" y permiten que los componentes sean dinámicos, configurables y reutilizables.

d) Estado: se trata de la definición del propio componente en un instante determinado de tiempo, existen dos tipos de componentes, con estado y sin estado.

Hay que mencionar que React.js maneja su propio DOM (del inglés *Document Object Model*) y almacena la versión anterior del DOM en la actual, comparándola para actualizar de la mejor forma el DOM del navegador (React 2022).

2.5.2.2. Web3.JS

Web3.js es un conjunto de librerías que brindan la posibilidad de interactuar con un nodo Ethereum tanto local como remoto a través de HTTP, IPC o WebSocket. (Ethereum 2016). También, esta librería brinda acciones que permiten enviar Ether de una cuenta a otra, leer y escribir datos de contratos inteligentes, crear contratos inteligentes, entre otras funciones. En resumen, permite escribir y leer en la *Blockchain* de Ethereum (McCubbin 2022).

Como se muestra en la **Figura 8–2**, Web3.js se comunica con la Blockchain de Ethereum usando el protocolo de llamada a procedimiento remoto JSON RPC. El protocolo de JSON RPC permite realizar solicitudes a un nodo individual de la red de Ethereum para leer y escribir datos.

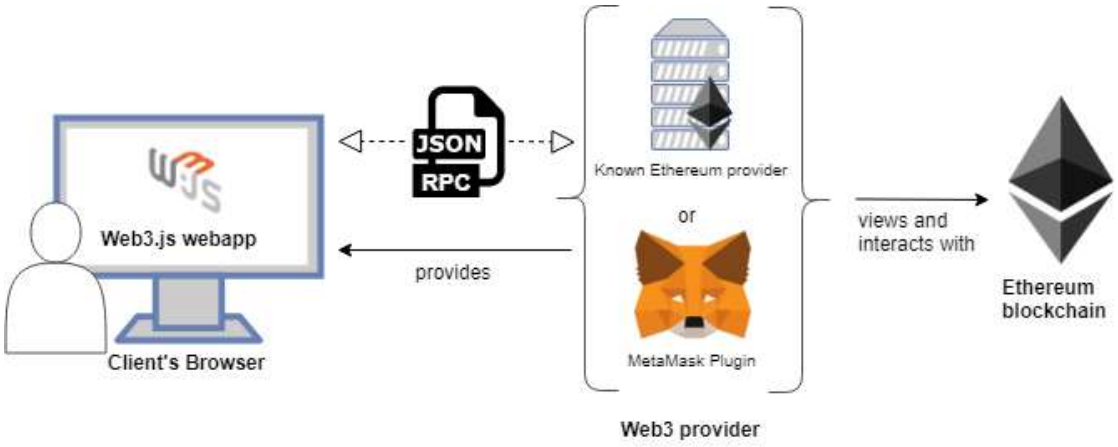


Figura 8-2: Implementación de Web3.js en una aplicación descentralizada
Fuente: Shanker, 2019

De acuerdo con (Ethereum 2016), los módulos que se incluyen en la librería Web3.js contienen la funcionalidad para el ecosistema *Ethereum*. A continuación, se listan los módulos que componen a la librería:

1) web3-eth: se usa para la cadena de bloques de *Ethereum* y los contratos inteligentes.
2) web3-shh: se usa para el protocolo *whisper*, para comunicarse con la red punto a punto y transmitir.
3) web3-bzz: se usa para el protocolo *swarm*, el almacenamiento de archivos descentralizado.
4) web3-utils: contiene funciones auxiliares útiles para los desarrolladores de aplicaciones descentralizadas.

2.5.3. Frameworks

Un *framework* es un esquema o marco de trabajo que ofrece una estructura base para elaborar un proyecto con objetivos específicos, es decir una plantilla que sirve como punto de partida para la organización y desarrollo de software (Edix 2023). En este apartado se describirán los *frameworks* a utilizar para el desarrollo del sistema de votaciones.

2.5.3.1. Node.JS

Node.js fue creado por los desarrolladores originales de JavaScript en 2009. Transformaron a JavaScript a un lenguaje que ha mas de ejecutarse en el navegador se podría ejecutar en los ordenadores como si de aplicaciones independientes se tratara, es decir del lado del cliente (OpenJS

Foundation y Node.js 2022). Node.js permite avanzar en la programación con JavaScript, no solo permitiendo la creación de sitios web interactivos, sino también ofreciendo la capacidad de realizar tareas similares a las que se pueden crear con otros lenguajes de secuencia de comandos, como Python (Lucas 2019).

2.5.4. Entornos de desarrollo integrados

Un entorno de desarrollo integrado (por sus siglas IDE del inglés *Integrated Development Enviroment*) es un sistema de software para el diseño de aplicaciones, combina herramientas comunes para desarrolladores en una sola interfaz de usuario gráfica (RedHat 2019). En este apartado se describirán los entornos de desarrollo integrado a utilizar para el desarrollo del sistema de votaciones.

- Visual Studio Code

Visual Studio Code es un editor de código fuente que brinda la posibilidad de trabajar con diferentes lenguajes de programación, tiene la capacidad de administrar atajos de teclado personalizados y de reorganizar el código. Además, es de acceso libre y gratuito, y cuenta con una amplia gama de extensiones que se pueden utilizar para personalizar y mejorar esta herramienta. (Microsoft 2022).

De acuerdo con (Microsoft 2022), las extensiones de Visual Studio Code otorgan infinidad de opciones, como colorear tabulaciones, etiquetas o recomendaciones de autocompletado. También hay extensiones que ayuda con el lenguaje de programación que vayamos a usar, como por ejemplo para Python, C / C++, JavaScript, etc.

A continuación, se listan algunas extensiones para el desarrollo web en Visual Studio Code:

1) Better Haml: Una extensión que brinda asistencia con la sintaxis y completado automático de Haml.
2) YML (Yseop Markup Language): Provee soporte para YML, dando color y atajos.
3) HTML Snippets: Agrega color a las etiquetas HTML y proporciona accesos directos para ese lenguaje.
4) Beautify: Deja un código más atractivo y facilita su lectura.

- RemixIDE

Remix IDE permite desarrollar, implementar y administrar contratos inteligentes para *Ethereum* como cadenas de bloques. Además, no requiere configuración, fomenta un ciclo de desarrollo rápido y tiene un amplio conjunto de complementos con GUI intuitivas, el entorno de desarrollo integrado posee dos versiones: aplicación web o aplicación de escritorio. Así mismo, se puede agregar a Visual Studio Code como una extensión. Por último, se puede utilizar como plataforma de aprendizaje (Remix 2022).

De acuerdo con (Remix 2022), RemixIDE es soportado en varios navegadores tales como: Firefox, Chrome, Brave. Sin embargo, este entorno de desarrollo integrado no tiene soporte para ser utilizado en tables o dispositivos móviles. Todavía cabe señalar que es parte del Remix Project, una plataforma para herramientas de desarrollo que incluye proyectos como Remix Plugin Engine y Remix Libs.

Otro rasgo de RemixIDE son las herramientas que tiene incorporadas, tales como: (i) el analizador de remix, que realiza análisis estáticos sobre los contratos inteligentes escritos en Solidity para verificar seguridad y malas prácticas de desarrollo; (ii) remix astwalker, proporciona una manera fácil de leer el AST de un contrato inteligente; (iii) depurador de remix, brinda las herramientas de depuración para Solidity; (iv) remix Solidity, una herramienta de ayuda para compilador de Solidity; (v) Remix Lib, es un espacio para librerías que se utilizan en diferentes módulos; (vi) Pruebas de remix, ayuda a realizar pruebas unitarias e integración continua; (vii) Remix Url Resolvers, una herramienta para manejar la importación de contenido de diferentes fuentes (Remix 2023).

2.5.5. Suite Truffle

La Suite de truffle es un stack de herramientas que ofrece a un desarrollador la posibilidad de crear aplicaciones descentralizadas de la forma más cómoda posible. Trae consigo herramientas tales como: Truffle, un ambiente de desarrollo para crear contratos inteligentes con un marco de prueba y una canalización de activos para cadenas de bloques que utilizan Ethereum Virtual Machine (por sus siglas EVM); Ganache, una *Blockchain* personal que vive de forma local en el ordenador del desarrollador y que permite desplegar contratos inteligentes, desarrollar aplicaciones y correr pruebas; Drizzle, una colección de librerías enfocadas en el Frontend de la aplicación. (ConsenSys Software Inc 2022).

De acuerdo con (Maldonado 2021), el conjunto de herramientas proveído por la Suite de Truffle permite realizar operaciones, aquellas que se listan a continuación:

a) Soporte integrado para compilar, implementar y vincular contratos inteligentes.
b) Prueba de contrato automatizada.
c) Soporte de aplicaciones en consola y aplicaciones web.
d) Capacidad de gestionar una red y sus paquetes.
e) Una consola Truffle para comunicarse directamente con contratos inteligentes.
f) Incorporación de una estrecha integración entre herramientas
g) Configuración de los canales de compilación y soporte para procesos de compilación personalizados.
h) Uso de marcos de implementación y migraciones programables.
i) Consola interactiva para comunicación contractual directa.
j) Reconstrucción instantánea de activos durante el desarrollo.
k) Ejecución de scripts externos dentro de un entorno Truffle.

En resumen, el objetivo de la suite de Trufle es proveer un ambiente de desarrollo enfocado en la tecnología *Blockchain* para facilitar el desarrollo a los programadores que crean aplicaciones descentralizadas y contratos inteligentes para la plataforma de *Ethereum* (Maldonado 2021).

2.5.6. Sistema de gestión de bases de datos relacional

Un sistema de gestión de base de datos (por sus siglas SGBD), es un software encargado de controlar y gestionar el acceso a la base de datos, tiene un rol muy importante para que las aplicaciones actuales tengan un correcto funcionamiento (Prieto de Lope, 2015). En este apartado se describirá el SGBD a utilizar para el desarrollo del sistema de votaciones.

2.5.6.1. PostgreSQL

Según (PostgreSQL Global Development Group, 2023), PostgreSQL es un sistema de gestión de base de datos relacional orientado a objetos basado en la versión 4.1 de POSTGRES, desarrollado por la universidad de California en el departamento de computación científica de Berkeley. Así mismo, es un software de código abierto que ofrece una serie de características, tales como se muestra en la **Tabla 1 – 2.**

Tabla 1-2: Características de PostgreSQL

Características estándar	**Características ampliables**
Consultas complejas	Tipos de datos
Claves foráneas	Funciones
Disparadores	Operadores
Vistas actualizables	Funciones agregadas
Integridad transaccional	Métodos indexados
Control de concurrencia multiversión	Lenguajes de procedimiento

Fuente: (PostgreSQL Global Development Group, 2022)

Realizado: Manzano Edwin, Ayrton Avalos, 2023

2.5.7. Ethereum

Ethereum es una plataforma que permite transferir monedas criptográficas a cualquier destinatario con una tarifa reducida. También potencia aplicaciones que todo el mundo puede usar y que nadie puede derribar (Etherereum, 2022).

Es la *Blockchain* programable del mundo. Ethereum se basa en la innovación de Bitcoin, con algunas grandes diferencias. Ambos te permiten usar dinero digital sin proveedores de pagos, ni bancos. Pero Ethereum es programable, por lo que también puede ser usado para muchos activos digitales diferentes, incluyendo Bitcoin. Esto también significa que Ethereum es más que pagos. Es un mercado de servicios financieros, juegos y aplicaciones, donde no se puede robar datos ni censurar a un usuario.

2.5.8. Amazon Web Services

Amazon Web Services (por sus siglas AWS) es una plataforma en la nube que brinda acceso a una amplia gama de servicios de infraestructura, plataforma y software a través de internet. Esta solución en la nube es altamente flexible y escalable, permitiendo a las empresas y desarrolladores adaptarse fácilmente a sus necesidades cambiantes. Además, Amazon Web Services es fácil de usar y ofrece una amplia gama de opciones de pago, como pago por uso, lo que significa que solo se pagan por los recursos que se utilizan (Amazon 2023).

Con Amazon Web Services, las empresas pueden aprovechar la escalabilidad y la flexibilidad de la nube para impulsar su negocio y mejorar la eficiencia y la productividad, mientras que los desarrolladores pueden usar los servicios en línea para crear, desplegar y ejecutar aplicaciones y

servicios innovadores. En resumen, AWS es una solución en la nube poderosa y versátil para una amplia gama de necesidades empresariales y de desarrollo de aplicaciones utilizan (Amazon 2023).

2.6. Metodología de desarrollo

De acuerdo con (Gómez, Cervantes y González Pérez 2019), una metodología de desarrollo se compone de fases y actividades ya definidas, obviando el sentido clásico de fabricación de mayoría de productos e implicando conceptos de ensamblaje, reusabilidad y extensibilidad. Por ello, en esta sección de abordará la metodología de desarrollo para el sistema de votaciones.

2.6.1. Proceso Racional Unificado

Para (Krutchen 2003) el Proceso Racional Unificado (por sus siglas RUP), es un modelo de proceso adaptable que se ha derivado del trabajo de (Arlow y Neustadt 2005) sobre el UML y el Proceso de Desarrollo de Software Unificado asociado (Rumbaugh, Jacobson y Booch 1999). Reúne elementos de todos los modelos de procesos genéricos, ilustra las buenas prácticas en especificación y diseño, además de apoyar la creación de prototipos y la entrega incremental. Se describe normalmente desde tres perspectivas, aquellas que se listan a continuación:

a) Una perspectiva dinámica, que muestra las fases del modelo a lo largo del tiempo.
b) Una perspectiva estática, que muestra las actividades de proceso que se promulgan.
c) Una perspectiva práctica, que sugiere buenas prácticas que se utilizarán durante el proceso.

Hay que mencionar, además, el Proceso Racional Unificado reconoce que los modelos de procesos convencionales presentan una visión única del proceso.

La mayoría de las descripciones del Proceso Racional Unificado intentan combinar las perspectivas estáticas y dinámicas en un solo diagrama (Krutchen 2003). El combinar las perspectivas provoca que el proceso sea más difícil de entender, por lo que es recomendable usar descripciones separadas de cada una de estas perspectivas.

(Martínez y Martínez 2000) plantean al Proceso Racional Unificado como una metodología que integra todos los componentes o aspectos necesarios en todo el ciclo de vida del software, con el objetivo de abarcar proyectos de software pequeños o grandes. Por otra parte, esta metodología brinda todas las herramientas para todas las etapas de desarrollo y su respectiva documentación para los interesados. También, se plantea las características principales, aquellas que se describen a continuación:

a) Manejado por casos de uso: son una guía establecida para las tareas y actividades a realizar en el proceso de desarrollo sin excluir las fases de diseño, implementación y pruebas, aquellas que se ilustran en la **figura 9 – 2.**
b) Centrado en la arquitectura: la arquitectura del sistema es representada en diferentes vistas que se centran los aspectos principales del sistema y abstrayéndose de lo demás. De manera más precisa, se crean las vistas lógicas, de implementación, proceso y despliegue, aquellas que se juntan para formar el modelo arquitectónico 4+1.
c) Iterativo e Incremental: el proyecto se divide en ciclos y en cada uno de ellos se establecen fases de referencia, así mismo, las fases se constituyen de iteraciones de las principales actividades, como se ilustra en la **figura 9 – 2.**
d) Basado en componentes: es una característica donde el desarrollo de software requiere dividir el sistema en componentes con interfaces bien definidas, para posteriormente ser ensambladas y generar el sistema completo.
e) Uso de un único lenguaje de modelado: la metodología Proceso Unificado Racional adopta el uso de UML como el único lenguaje de modelado para crear todos los modelos.
f) Proceso integrado: establece una estructura que abarque e integre todos los aspectos, tales como: ciclos, fases, flujos de trabajo, mitigación de riesgos, control de calidad, gestión del proyecto y control de configuración.

En cuanto a la estructura estática, (Martínez y Martínez 2000) definen cuatro elementos base que se describen a continuación:

a) Roles: Comportamiento y responsabilidades de uno o varios individuos. Las responsabilidades de un rol son las de llevar a cabo un conjunto de actividades
b) Actividades: una unidad de trabajo atribuida a un rol. Tienen un objetivo concreto, por ejemplo, crear o actualizar algún producto.
c) Productos: También llamado artefacto, es un pedazo de información producido, utilizado y modificado por un proceso u actividad. Los productos son los resultados tangibles del proyecto.
d) Flujos de trabajo: secuencia de actividades realizadas por los diferentes roles que producen resultados observables. El Proceso Unificado Racional define dos grandes flujos, los de proceso y los de soporte, como se muestra en la **Figura 9 – 2**.

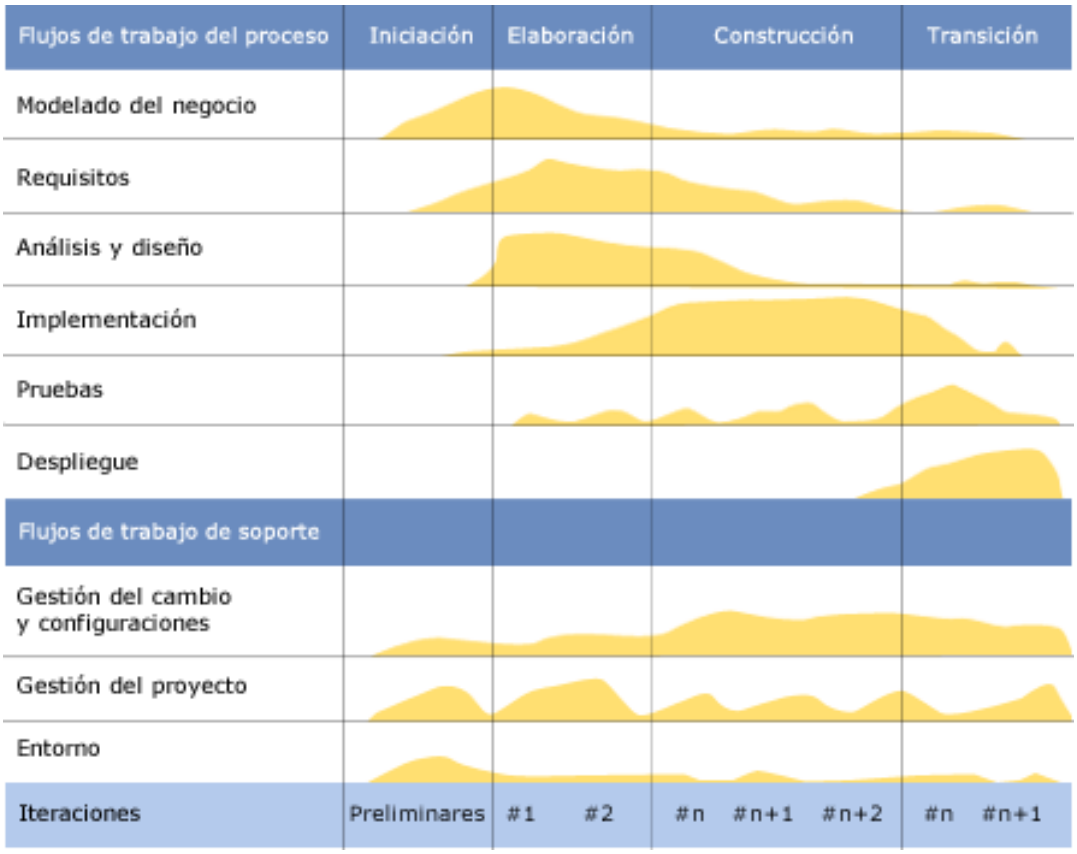


Figura 9-2: Ciclo de vida RUP

Fuente: Krutchen 2003

Por último, el Proceso Racional Unificado se divide en dos grandes flujos de trabajo, como se ilustra en la **Figura 9–2**, el flujo de trabajo del proceso y el flujo de trabajo del soporte. En el flujo del trabajo del proceso se realizan seis fases, tales como: Modelado del negocio, Requisitos, Análisis y diseño, Implementación, Pruebas y Despliegue. Por otra parte, los flujos de trabajo de soporte presentan tres fases, tales como: Gestión del cambio y configuraciones, gestión del proyecto y entorno. Cada fase estará sujeta a iteraciones de sus principales actividades.

2.7. Norma ISO/IEC 25010

La calidad de software es importante para garantizar que el software cumpla con las expectativas y necesidades de los usuarios, reduce los costos a largo plazo, aumenta la confiabilidad y mejora la reputación de una empresa o organización. Utilizar un enfoque de calidad de software durante todo el ciclo de vida del desarrollo del software es esencial para garantizar que se produzca un software de alta calidad. Para garantizar la calidad de software se debe guiar en un modelo de calidad, este representa la piedra angular en torno a la cual se establece el sistema para la evaluación de la calidad del producto. En el modelo se determinan las características de calidad

que se van a tener en cuenta a la hora de evaluar las propiedades de un producto software determinado (Organización Internacional de Normalización. 2011).

Un ejemplo de un modelo de calidad de software es el modelo de calidad ISO/IEC 9126, el cual establece seis características de calidad para el software: funcionalidad, fiabilidad, usabilidad, eficiencia, mantenibilidad y portabilidad. Otro ejemplo de modelo de calidad es el modelo de calidad de Capability Maturity Model Integration (CMMI) que establece 5 niveles de madurez para la gestión de proyectos de software y mejora continua.

La familia ISO/IEC 25000 incluye normas basadas en ISO/IEC 9126 y en ISO/IEC 14598 cuya finalidad es indicar el desarrollo de software a través de la especificación de requisitos y evaluación de características de calidad. También proporciona una guía para la implementación de nuevos estándares llamada requisitos y Evaluación de Calidad de Productos Software (por sus siglas SQuaRE, del *inglés System and Software Quality Requirements and Evaluation*) (IEEE Std 2011a).

La norma ISO/IEC 25010 es un modelo genérico que clasifica a la calidad de un producto software en dos partes, tales como: modelo para la calidad interna y externa de un producto software y el modelo para la calidad en uso de un producto software. En el presente trabajo, se considerará más al modelo para la calidad interna y externa del producto software, aquel que define ocho características de calidad, tales como: Adecuación Funcionalidad, Fiabilidad, Eficiencia en el Desempeño, Facilidad de Uso, Seguridad, Compatibilidad, Mantenibilidad y Portabilidad. Aquellas que se subdividen en subcaracterísticas que se describen en la **Figura 10 – 2** (IEEE Std 2011a).

Figura 10-2: Características de calidad

Fuente: IEEE Std 2011a.

En las siguientes secciones se profundizará en las características de calidad, tales como: Seguridad y Eficiencia del desempeño. Aquellas que se aplicarán para medir el sistema de votaciones desarrollado.

2.7.1. Seguridad

Es la capacidad de protección de la información y los datos de manera que personas o sistemas no autorizados no puedan leerlos o modificarlos (IEEE Std 2011b). Esta característica se subdivide a su vez en las siguientes subcaracterísticas que se listan a continuación:

a) Confidencialidad: Capacidad de protección para el acceso de datos e información no autorizada, ya sea accidental o deliberadamente (IEEE Std 2011b).
b) Integridad: Capacidad del sistema o componente para prevenir accesos y modificaciones no autorizados a datos o programas de ordenador (IEEE Std 2011b).
c) No repudio: Capacidad de demostrar las acciones o eventos que han tenido lugar, de manera que dichas acciones o eventos no puedan ser repudiados posteriormente (IEEE Std 2011b).
d) Responsabilidad: Capacidad de rastrear de forma inequívoca las acciones de una entidad (IEEE Std 2011b).

2.7.1.1. Goal Question Metrical

Según (Calabrese et al. 2021) el enfoque GQM (Goal Question Metrical, GQM por sus siglas en inglés) es una técnica para medir un objetivo específico a través de preguntas. Se inicia identificando uno o más objetivos de calidad y generando preguntas detalladas para ellos. Después, se establecen métricas que tengan un único resultado basado en las respuestas a esas preguntas para evaluar el grado de cumplimiento con respecto al objetivo identificado. Finalmente, se desarrollan procesos para validar y analizar los resultados obtenidos.

2.7.2. Eficiencia de desempeño

Esta característica representa el desempeño relativo a la cantidad de recursos utilizados bajo determinadas condiciones (IEEE Std 2011a). Esta característica se subdivide a su vez en subcaracterísticas, aquellas que se listan a continuación:

a) Comportamiento temporal: Representa a los tiempos de respuesta, procesamiento y ratios de throughput de un sistema cuando lleva a cabo sus funciones bajo condiciones determinadas en relación con un banco de pruebas (benchmark) establecido (IEEE Std 2011a).

b) Utilización de recursos: Las cantidades y tipos de recursos utilizados cuando el software lleva a cabo su función bajo condiciones determinadas (IEEE Std 2011a).
c) Capacidad: El grado de cumplimiento de los requisitos del producto o sistema en relación a los límites máximos de un parámetro (IEEE Std 2011a).

2.8. Trabajos relacionados

La evolución continua de la tecnología *Blockchain* y la gran adopción de las aplicaciones descentralizadas en la industria ha causado la creación de varias propuestas o sistemas en diferentes áreas, con respecto al voto electrónico se puede destacar:

El sistema de votación electrónico basado en la tecnología *Blockchain* para las elecciones en Jordania, cuenta con seis componentes principales tales como: partes interesadas, Frontend, Backend, Hyper ledger Blockchain, bases de datos y algoritmos de consenso. El sistema se desarrolló para presentar una solución que ayude al proceso de elecciones de Jordania, ya que el proceso tradicional es susceptible al fraude, falta de confianza, falta de seguridad y falta de privacidad. Por ello, incorpora la tecnología Blockchain para contrarrestar estos defectos del sistema tradicional (Qatawneh, Quzmar y Al-Maaitah 2022).

Por otra parte, la interacción de los componentes es descrita a continuación: las partes interesadas votan usando la aplicación del lado del cliente, el Frontend se implementa como una interfaz de usuario que se desarrollará en REACT.JS para poder para ser manejado por el servidor Backend Node.JS, que estará a cargo de todas las responsabilidades. Las partes interesadas pueden interactuar con la aplicación utilizando cualquier dispositivo ingresando la URL en el navegador, iniciando sesión y luego votando, con la posibilidad de ver los resultados para cada área o todas las regiones (Qatawneh, Quzmar y Al-Maaitah 2022).

El trabajo (Garcia 2019) en la Universidad de Córdoba en Colombia, desarrolla un sistema de votaciones usando la tecnología *Blockchain* y el Framework *Hyperledger* para las elecciones de representante estudiantil. Para esto, incorpora la tecnología *Blockchain* dentro de los procesos electorales con el fin de que las decisiones políticas tomadas por individuos tengan mayor participación ciudadana, reduzca los costos de la logística y el sufragante perciba transparencia y confianza al votar.

Por último, (Kamil et al. 2021) plantea el uso de un sistema de votación electrónica basado en la tecnología Blockchain para ayudar a controlar los disturbios electorales para la elección de lideres regionales durante la pandemia de Covid-19 y disminuir la cantidad de contagias posibles que

puede existir en un proceso presencial. Se debe agregar que se implementó la tecnología Blockchain con un fuerte protocolo criptográfico para crear un bloque de cifrado seguro y los resultados de las votaciones realizadas por el público sean reales, seguros y transparentes sin que puedan ser manipulados. Por otra parte, el sistema fue analizado mediante un SUS Score y se obtuvo un 90 de resultado en aceptación al voto electrónico, lo que significa que la comunidad puede aceptarlo porque trae impactos positivos y significativos como la eficacia y la eficiencia.

CAPÍTULO III

3. MARCO METODOLÓGICO

Para el cumplimiento de los objetivos planteados en este trabajo, el presente capítulo detalla el diseño del estudio experimental y la metodología para la automatización del proceso electoral de la Cooperativa de Ahorro y Crédito Nueva Esperanza.

3.1. Diseño de estudio

En esta sección se detallan el tipo de estudio, métodos, técnicas y fuentes de estudio, operacionalización conceptual y metodológica de las variables, la población y la muestra.

3.1.1. Tipo de estudio

El presente trabajo de titulación corresponde al tipo aplicativo, puesto que se utiliza los conocimientos adquiridos en la carrera y la información sobre el proceso eleccionario de la Cooperativa de Ahorro y Crédito Nueva Esperanza.

3.1.2. Métodos y técnicas

Los métodos para utilizar en el trabajo de integración curricular se detallan a continuación:

Analítico: Permite dividir el proceso a un nivel adecuado de entendimiento y de sus reglas de negocio utilizado por la Cooperativa de Ahorro y Crédito "Nueva Esperanza" para las votaciones.

Sintético: Permite abstraer la información analizada del proceso de votaciones y representarla de manera gráfica usando una notación que permita al equipo de trabajo tener una representación visual y clara de lo que se quiere automatizar.

Inductivo: Permite analizar los pequeños procesos que se realizan en una votación para desarrollarlos e implementarlos en un sistema completo para las votaciones en la Cooperativa de Ahorro y Crédito Nueva Esperanza.

Estadístico: Este método permite recolectar datos cuantitativos a través de la entrevista, encuesta y observación para analizar las métricas a utilizar dentro de las características de calidad de la ISO/IEC 25010.

En base a los objetivos específicos del trabajo de integración curricular, en la **Tabla 1 – 3** se establecen los métodos, técnicas y fuentes de estudio.

Tabla 1-3: Métodos y técnicas

Métodos y Técnicas			
Objetivos	**Métodos**	**Técnicas**	**Fuentes**
Describir los métodos utilizados de comunicación entre aplicaciones descentralizadas y la Blockchain.	Sintético, Analítico	Revisión de documentos	• Papers • Bases de datos • Documentación • Resultados de Motores de búsqueda
Analizar el proceso electoral que se lleva a cabo en las cooperativas de ahorro y crédito, así como los actores que intervienen en este.	Analítico	• Entrevistas • Revisión de documentos • Modelado y notación de procesos del negocio - BPMN	• Administrativos • Reglamentos de la Superintendencia • Reglamento de elecciones representantes de la Cooperativa
Desarrollar el módulo de usuarios, el módulo de elecciones, el módulo de votos, el módulo de candidatos y el módulo de reportes	RUP	• Análisis estático y dinámico del código • Revisión de documentación • Diagrama Entidad Relación • Diagrama modelo relacional • Documento de arquitectura • Diagrama de secuencia • Diagrama de estados • Diagrama de colaboración • Mapa de comportamiento a nivel del hardware	• Estándares • Especificación de requisitos • Documentación sobre las tecnologías • Usuarios/Clientes • Documentación sobre diagramas UML • Libros • Artículos científicos • Revistas

Evaluar la seguridad y la utilización de recursos de la aplicación descentralizada mediante el estándar ISO 25010	Estadístico, Inductivo	**Seguridad** • Cuestionario • GQM • ISO/IEC 25010	• Sistema desarrollado • Usuarios • Artículo científico
		Utilización de recursos • ISO/IEC 25010 • Observación	• Sistema desarrollado • Software que proporcione información sobre los procesos del sistema • Libros

Realizado por: Manzano Edwin, Avalos Ayrton, 2023

3.1.3. Operacionalización conceptual de la seguridad y la eficiencia de desempeño

De acuerdo con la sistematización del problema para la variable de seguridad se establece su operacionalización conceptual en la **Tabla 2 – 3.**

Tabla 2-3: Operacionalización conceptual de la variable de seguridad

Sistematización de problema	Variable	Tipo	Concepto
¿Cómo se evalúa la eficiencia y seguridad de las aplicaciones descentralizadas?	Seguridad	Cualitativa Compleja	La seguridad del software se relaciona por completo con la calidad. Debe pensarse en seguridad, confiabilidad, disponibilidad y dependencia, en la fase inicial, en la de diseño, en la de arquitectura, pruebas y codificación, durante todo el ciclo de vida del software [proceso].

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

Por otra parte, en la **Tabla 3 – 3** se detalla la operacionalización conceptual para la variable de eficiencia de desempeño

Tabla 3-3: Operacionalización conceptual de la variable de eficiencia de desempeño

Sistematización de problema	Variable	Tipo	Concepto
¿Cómo se evalúa la eficiencia y seguridad de las aplicaciones descentralizadas?	Eficiencia de desempeño	Cuantitativa Simple	Capacidad de un producto software en proporcionar un rendimiento adecuado, respecto a la cantidad de recursos utilizados en un determinado escenario (Karla et al. 2016).

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

3.1.4. Operacionalización metodológica de la seguridad y la eficiencia de desempeño.

En siguiente apartado, mediante la **Tabla 4 – 3** y la **Tabla 5 – 3** se detalla la operacionalización metodológica de las variables de seguridad y eficiencia de desempeño respectivamente.

Tabla 4-3: Operacionalización metodológica de la variable de seguridad

Sistematización del problema	Variable	Categoría	Indicador	Técnica	Fuente
¿Cómo se evalúa la eficiencia y seguridad de las aplicaciones descentralizadas?	Seguridad	**Confidencialidad**	Conexiones seguras	Evaluación	• Sistema desarrollado • Fichas tecnicas • Cuestionario GQM
			Control de acceso	Evaluación	• Sistema desarrollado • Fichas tecnicas • Cuestionario GQM
			Encriptación de datos	Evaluación	• Sistema desarrollado • Fichas técnicas • Cuestionario GQM
			Contraseña de bajo | medio | alto nivel	Evaluación	• Sistema desarrollado • Fichas técnicas

					• Cuestionario GQM
		Integridad	Prevención de accesos	Evaluación	• GQM Sistema desarrollado • Fichas técnicas • Cuestionario GQM
			Prevención de modificaciones	Evaluación	• Sistema desarrollado • Fichas técnicas • Cuestionario GQM
			Confirmación de datos	Evaluación	• Sistema desarrollado • Fichas técnicas • Cuestionario GQM
		No-Repudio	Operaciones realizadas	Evaluación	• Sistema desarrollado • Fichas tecnicas • Cuestionario GQM
			Mecanismos de cifrado	Evaluación	• Sistema desarrollado • Fichas tecnicas • Cuestionario GQM
			Confirmación de acciones	Evaluación	• Sistema desarrollado • Fichas tecnicas • Cuestionario GQM
			Registro de ubicación	Evaluación	• Sistema desarrollado • Fichas tecnicas • Cuestionario GQM
		Responsabilidad	Registro de acciones y datos	Evaluación	• Sistema desarrollado • Fichas tecnicas • Cuestionario GQM

			Control de ubicación	Evaluación	• Sistema desarrollado • Fichas tecnicas • Cuestionario GQM
		Autenticidad	Comprobación de identidad	Evaluación	• Sistema desarrollado • Fichas tecnicas • Cuestionario GQM
			Comprobaciones adicionales	Evaluación	• Sistema desarrollado • Fichas tecnicas • Cuestionario GQM

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

Tabla 5-3: Operacionalización metodológica de la variable de eficiencia de desempeño

Sistematización del problema	Variable	Categoría	Indicador	Técnica	Fuente
¿Cómo se evalúa la eficiencia y seguridad de las aplicaciones descentralizadas?	Eficiencia del desempeño	Utilización de recursos	Utilización de CPU	Observación	• Sistema desarrollado • Software que proporcione información sobre los procesos del sistema • Fichas técnicas
			Utilización de memoria RAM	Observación	
			Consumo de GAS	Observación	• Smart Contract Desplegado en una red de prueba (Goerli) • Plataforma de exploración y análisis de bloques para Ethereum • Fichas técnicas

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

A continuación, en la **Tabla 6 – 3**, **Tabla 7 – 3** y **Tabla 8 – 3** se definen las fichas técnicas para el indicador de utilización de CPU, el indicador de utilización de memoria RAM y el indicador de consumo de GAS respectivamente.

Tabla 6-3: Ficha técnica para el indicador de utilización de CPU

Característica	Utilización de recursos
Subcaracterística	Utilización de CPU
Métrica	Uso del CPU
Propósito	¿Cuál es el porcentaje de tiempo del CPU para realizar una determinada tarea?
Fórmula	X = (B * A)/100 A = La cantidad de tiempo de CPU usado para realizar una tarea. B = Intervalo de tiempo Donde B > 0 y A ≤ B
Valor deseado	0 ≤ X ≤ 100; Cuanto más se acerque a 0 es mejor. Donde el peor caso es X = 100%.
Tipo de medida	X = Porcentaje
Tipo de escala	Ratio
Fuente de medición	Tiempo estimado para cada tarea
Audiencia	Desarrolladores

Fuente: (Karla et al. 2016)

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

Tabla 7-3: Ficha técnica para el indicador de utilización de memoria RAM

Característica	Utilización de recursos
Subcaracterística	Utilización de la memoria
Métrica	Uso de la memoria RAM
Propósito	¿Cuánto espacio de memoria es usado para realizar una tarea dada?
Fórmula	X = B - A A = Cantidad de espacios de memoria que realmente es usado para realizar una tarea. B = Cantidad total de espacios de memoria Donde B > 0
Valor deseado	0 ≤ X ≤ 15 Cuanto más se acerque a 0 es mejor.
Tipo de medida	X = TAMAÑO EN MB
Tipo de escala	Ratio
Fuente de medición	Tamaño estimado para cada tarea
Audiencia	Desarrolladores

Fuente: (Karla et al. 2016)

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

Tabla 8-3: Ficha técnica para el indicador de consumo de gas

Característica	Utilización de recursos
Subcaracterística	Consumo de gas
Métrica	Cantidad de consumo de gas
Propósito	¿Cuánto gas consume una determinada transacción en la Máquina Virtual de Ethereum?
Fórmula	X = A A = Cantidad de gas consumido Donde A >= 0
Valor deseado	$0 \leq X \leq 15$ Cuanto más se acerque a 0 es mejor.
Tipo de medida	X = GWEI
Tipo de escala	Ratio
Fuente de medición	Cantidad de GWEIS consumidos dada una tarea
Audiencia	Desarrolladores

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

Por otra parte, según el enfoque GQM, se establece un modelo de medición utilizando sus características tales como:

a) **Objetivo general (GOAL):** medir la seguridad del sistema de votaciones a través de las subcaracterísticas de seguridad provistas por la norma ISO/IEC 25010.
b) **Cuestionario** (**QUESTION)**: a nivel operativo se definen un total de 31 preguntas de SI/NO que se detallan en la **Tabla 9-3,** el cuestionario se lo realiza en base a las subcaracterísticas de Confidencialidad, Integridad, No-Repudio, Responsabilidad y Autenticidad, descritas en la **Tabla 4-3.**

Tabla 9-3: Cuestionario para la característica de Seguridad

ID	PREGUNTA
P01	¿Se requiere que la contraseña posea al menos 8 caracteres?
P02	¿Se requiere que la contraseña posea letras mayúsculas y minúsculas?
P03	¿Se requiere que la contraseña posea números y letras?
P04	¿Se requiere que la contraseña posea caracteres especiales?
P05	¿El sistema utiliza conexión segura mediante HTTPS?
P06	¿La base de datos posee los datos encriptados?
P07	¿El sistema permite acceder a funcionalidades en las cuales no se tiene permiso?
P08	¿El sistema permite que cualquier persona tenga acceso a la base de datos?

P09	¿El sistema permite que cualquier persona tenga acceso al código del servidor de la aplicación?
P10	¿Cualquier persona tiene acceso al servidor físico?
P11	¿Cualquier persona tiene acceso al servidor remoto?
P12	¿El sistema posee redireccionamientos hacia sitios no seguros?
P13	¿El sistema garantiza que los datos utilizados en el sufragio no hayan sido alterados o modificados por terceros?
P14	¿El sistema permite que cualquier persona pueda modificar la base de datos?
P15	¿El sistema permite que cualquier persona pueda modificar el código del servidor de la aplicación?
P16	¿El sistema posee un registro de las transacciones de votación?
P17	¿El sistema posee algoritmos de cifrado de datos?
P18	¿El sistema posee un mecanismo criptográfico, como firma digital?
P19	¿El sistema solicita confirmación a la hora de realizar una acción?
P20	¿El sistema posee una protección con certificados SSL?
P21	¿El sistema registra la información del sufragio en la cadena de bloques usando contratos inteligentes?
P22	¿El sistema informa vía mail las operaciones realizadas?
P23	¿El sistema guarda un registro de fecha y hora de ingreso al mismo?
P24	¿El sistema registra la dirección IP desde la cual se ingresa al sitio?
P25	¿El sistema realiza una comprobación de identidad mediante un certificado digital?
P26	¿El sistema posee un sistema de verificación en dos pasos?
P27	¿Es requerida una clave de segundo nivel para el ingreso al sistema?
P28	¿El sistema realiza una comprobación de identidad mediante un correo electrónico o número de celular propiedad del usuario?
P29	¿El sistema realiza una comprobación de identidad para establecer una transmisión de información entre dos o más campos usando JSON Web Token?
P30	¿El sistema realiza una comprobación de identidad mediante credenciales?
P31	¿El sistema realiza una comprobación de identidad mediante una firma digital?

Fuente: (Calabrese et al. 2017)

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

Tabla 10-3:

c) **Métricas (METRIC):** Para alcanzar el objetivo general, en la **Tabla 10-3** se describen los criterios de evaluación y se agrupan las preguntas de forma lógica, usando conectivos lógicos y asignando un puntaje.

Tabla 11-3: Descripción de criterios de evaluación (CE)

ID	Nombre	Descripción	Fórmula	Puntos
C-1	Conexiones seguras	Una conexión se considera segura si se utiliza HTTPS y si no se tienen redireccionamientos hacia sitios no seguros	P5 & ~P12 = V	1
C-2	Control de acceso	Se debe controlar que no se permita acceder a funcionalidades sin autorización, tampoco a la base de datos, al código de la aplicación ni a los servidores, físico ni remoto	si P7 | P8 | P9 | P10 | P11 = F	1
C-3	Encriptación de datos	Los datos de la base de datos deben estar encriptados	P6 = V	1
C-4	Contraseña de bajo nivel	La contraseña se considera de bajo nivel si posee menos de 8 caracteres, no posee letras mayúsculas y minúsculas, no posee letras y números y no posee caracteres especiales	P1 | P2 | P3 | P4 = F	0
	Contraseña de medio nivel	La contraseña se considera de medio nivel si posee al menos 8 caracteres o letras mayúsculas y minúsculas o letras y números o	P1 | P2 | P3 | P4 = V	0.5
	Contraseña de alto nivel	La contraseña se considera de alto nivel si posee al menos 8 caracteres, letras mayúsculas y minúsculas, letras y números y caracteres especiales	P1 & P2 & P3 & P4 = V	1
I-5	Prevención de accesos	Se debe prevenir que no se permita acceder a funcionalidades sin autorización, tampoco a la base de datos ni al código de la aplicación, y que no se permitan inyecciones SQL	P7 | P8 | P9 =F	1
I-6	Prevención de modificaciones	Se debe prevenir que no se permita modificar datos de la base de datos ni modificar el código de la aplicación sin autorización	P14 | P15 = F	1
I-7	Confirmación de datos no alterados	Se debe realizar una confirmación de que los datos de los votos no hayan sido alterados	P13 = V	1

NR-8	Operaciones realizadas	Se debe poseer un historial de acciones realizadas o las mismas deben ser enviadas por mail	P16 | P22 = V	1
NR-9	Mecanismos de cifrado	Se debe poseer un algoritmo de cifrado de datos o un mecanismo criptográfico, como firma digital, o una protección con certificados SSL	P17 | P18 | P20 = V	1
NR-10	Confirmación de acciones	Se debe solicitar una confirmación al realizar una determinada acción	P19 = V	1
NR11	Registro de votos	Se debe registrar los votos en la cadena de bloques para el rastreo del proceso electoral	P21 = V	1
R-12	Registro de acciones y datos	Se debe poseer un historial de acciones realizadas, o un registro de fecha y hora de ingreso al sistema o de la dirección IP desde la cual se ingresa o del tipo de navegador y sistema de operación utilizado	P16 | P23 | P24 = V	1
R-13	Control de votos	Se debe registrar a un usuario cuando a emitido un voto	P21 = V	1
A-14	Comprobación de identidad	El sistema debe realizar una comprobación de identidad mediante alguno de los siguientes métodos: datos biométricos, tarjeta de coordenadas, credenciales, firma electrónica o certificado digital	P25 | P28 | P29 | P30 | P31 = V	1
A-15	Comprobación es adicionales	Se debe poseer un sistema de verificación en dos pasos, o se debe requerir una clave de segundo nivel para el ingreso al sistema o una confirmación de actualización de datos	P26 | P27 | P13 = V	1

Fuente: (Calabrese et al. 2017)

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

Por último, a nivel cuantitativo se combinan los criterios de evaluación para definir las métricas que satisfacen los objetivos de las subcaracterísticas. En la **Tabla 11-3** se detalla la ficha técnica para evaluar la Confidencialidad, el resto de las fichas técnicas se detalla en el **ANEXO D.**

Tabla 12-3: Métricas para evaluar la Confidencialidad

Característica	Seguridad
Subcaracterística	*Confidencialidad*
Propósito	*¿Cuán eficiente es el sistema a la hora de proteger el acceso de datos e información no autorizados, ya sea accidental o deliberadamente?*
Método de aplicación:	*Contestar las preguntas de los CE correspondientes a la subcaracterística "Confidencialidad" y calcular la puntuación obtenida, sumando los puntajes de los CE referenciados que cumplan con la meta esperada. "Puntaje total" hace referencia al máximo puntaje que se puede obtener*
Entradas	*A = Puntaje obtenido. B = Puntaje total*
Fórmula	X = A/B
Tipo de escala	Nominal
Observaciones	*Los CE a utilizar son: C-1, C-2, C-3 y C-4.*
Audiencia	Equipo TI

Fuente: (Calabrese et al. 2017)

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

Tabla 13-3:

Finalmente, la **Tabla 12-3** detalla las fórmulas para cada subcaracterísticas.

Tabla 14-3: Fórmula para cada subcaracterística

MÉTRICA	**FÓRMULA**
CONFIDENCIALIDAD	(C1+C2+C3+C4)/4
INTEGRIDAD	(I5+I6+I7)/3
NO REPUDIO	(NR8+NR9+NR10+NR11)/4
RESPONSABILIDAD	(R12+R13)/2
AUTENTICIDAD	(A14+A15)/2

Fuente: (Calabrese et al. 2017)

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

3.1.5. Población y Muestra

En esta sección se define la población a la que se enfoca la ejecución de la operacionalización de las variables, además, la muestra sobre la cual se van a realizar las mediciones y obtener los resultados que permitirán afirmar o negar la hipótesis planteada.

3.1.5.1. Población y muestra de la seguridad

En este caso particular, debido a que el tamaño de la población es de seis personas, que lo conforma el Equipo TI de la Cooperativa de Ahorro y Crédito "Nueva Esperanza", se ha decidido trabajar con toda la población como muestra. Con un error de estimación de 0% y nivel de confianza del 100%.

3.1.5.2. Población y muestra de la eficiencia del desempeño

Para medir la característica de la eficiencia del desempeño la población definida consta de todas las operaciones o procesos que se realizan sobre cada módulo del sistema de votaciones. En el **ANEXO E** mediante el diagrama de casos de uso se definen 50 procesos, obteniendo una población finita.

$$n = \frac{N * Z_{\alpha}^{2} * p * q}{d^{2} * (N-1) + Z_{\alpha}^{2} * p * q}$$

N = 50, población

Z = 95% => 1.96, nivel de confianza

P = 50% => 0.5, probabilidad de éxito

Q = 50% => 0.5, probabilidad de fracaso

D = 8% => 0.8, Error de estimación máximo aceptado

$$n = \frac{50 * 1.96^{2} * 0.5 * 0.5}{0.8^{2} * (50-1) + 1.96^{2} * 0.5 * 0.5} = 37{,}69 = 38$$

El tamaño muestral obtenido al aplicar la fórmula de población finita es de 38 procesos u operaciones.

3.2. Desarrollo de la aplicación descentralizada usando RUP

En esta sección se detalla el desarrollo del sistema de votaciones utilizando la metodología RUP, aquella que contempla cuatro fases, tales como: Análisis, diseño, desarrollo y transición.

3.2.1. Fase de análisis

En esta fase se realiza la comprensión e inducción al problema y la respectiva solución. Para ello, se ha detallado el estudio de factibilidad, en la **Tabla 13 – 3** se detalla un ejemplo de la factibilidad técnica, el resto de los componentes acerca del estudio de factibilidad se hallan en el **ANEXO A.**

Tabla 15-3: Factibilidad técnica, hardware requerido

Cantidad	Descripción
1	MacBook Pro (13-inch, M1, 2020)
1	Lenovo IDEAPAD S145, 8GB RAM, SSD 250GB
1	Samsung A03 – 64gb ALMACENAMIENTO – 4 GB RAM
1	iPhone Xs 64 GB ALMACENAMIENTO

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

El siguiente análisis en realizarse en esta fase es acerca del análisis de riesgos, aquel que se ejemplifica en la **Tabla 14 – 3.** Los riesgos asociados a cada identificación y toda la información adicional se encuentra detallado en el **ANEXO B.**

Tabla 16-3: Análisis de riesgos

Identificación	Probabilidad			Impacto		Exposición al riesgo	
	%	Valor	Probabilidad	Valor	Impacto	Valor	Exposición
RG1	20%	1	Baja	2	Moderado	2	Media
RG2	30%	2	Media	2	Moderado	2	Media
RG3	18%	1	Bajo	1	Bajo	1	Bajo
RG4	15%	1	Bajo	1	Bajo	1	Bajo
RG5	10%	1	Bajo	1	Bajo	1	Bajo
RG6	10%	1	Bajo	1	Bajo	1	Bajo
RG7	15%	1	Bajo	1	Bajo	1	Bajo

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

También se define la planificación del proyecto y las fases a ejecutarse, actividades que se detallan en el **ANEXO C.** Por otra parte, en la **Figura 1 – 3** ejemplifica un diagrama de casos de para la definición de los requisitos funcionales, el resto de los diagramas se detallan en el **ANEXO E**.

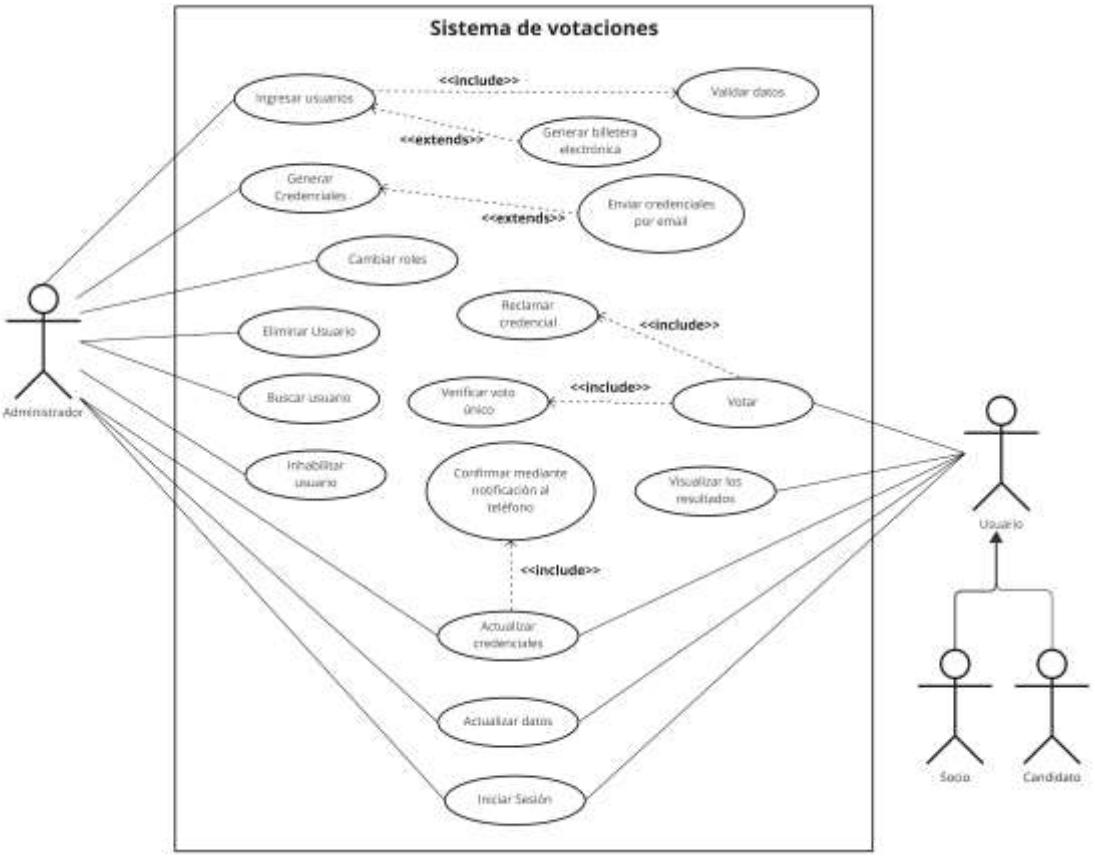


Figura 1-3: Diagrama de casos de uso del sistema de votaciones

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

Mediante la **Tabla 15 – 3** se ejemplifica la documentación de los casos de uso (requerimientos funcionales) el resto de los casos de uso se detallan en el **ANEXO F,** así como los requerimientos no funcionales mediante la especificación textual de requerimientos de seguridad, arquitectura, interfaz de usuario, etc.

Tabla 17-3: Caso de uso para el ingreso de una agencia

Caso de uso	Ingresar agencia		**Identificador**	CU-01
Descripción	Registrar los campos de una agencia en el sistema			
Actores	Usuario, Base de datos, Sistema de Votaciones	**Evento**	Pulsar en el botón para agregar una nueva Agencia	
Precondiciones	1. El usuario debe autentificarse en el sistema 2. El usuario debe poseer el rol de administrador para realizar la operación de ingreso de agencias 3. Disponibilidad del sistema web			

Pasos	1. El usuario accede a la url del sistema 2. El usuario inicia sesión mediante la interfaz gráfica 3. El usuario se dirige a la vista de Agencias 4. El usuario da clic en el botón de Agregar Agencia 5. El usuario llena el formulario con todos los campos requeridos 6. El usuario envía los datos 7. Los datos son guardados en la base de datos
Resultados	a) Mensaje exitoso de creación de una nueva agencia b) Mensaje de error en la creación de una nueva agencia c) Retorno a la página principal para agencias.
Excepciones	a) No se admiten agencias duplicadas, se enviará un mensaje de error b) Todos los campos del formulario para agregar una Agencia son requeridos, no se admiten campos vacíos c) Todos los campos deben tener un formato correcto, de acuerdo al tipo de dato d) La cantidad de ganadores no debe ser igual o mayor a la cantidad de representantes e) El campo correspondiente al nombre de la agencia debe ser único

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

3.2.1.1. Análisis del proceso electoral de la COAC Nueva Esperanza

Por último, se realiza un profundo análisis del proceso electoral utilizado en la Cooperativa de Ahorro y Crédito Nueva Esperanza, para ello se realizó una revisión de la documentación y reglamentos establecidos por la Superintendencia de economía popular y solidaria, así como el reglamento de elección de representantes de la cooperativa. Para ello, se considera el modelado del negocio mediante un Diagrama BPMN como se muestra en la **Figura 2 – 3** y la **Figura 3 – 3**.

En el proceso electoral de la cooperativa intervienen varios actores y la elección se divide en dos fases, la primera corresponde a la elección de los representantes de la asamblea general y la segunda en la elección de los representantes para el consejo de administración y consejo de vigilancia.

Las elecciones arrancan desde la primera fase, en la etapa de planificación, mediante el **consejo de administración** que tiene las siguientes facultades:

- Constituir los miembros de la Junta General Electoral
- Revisar y aprobar el cronograma de actividades presentados por la Junta General Electoral
- Revisar y aprobar la guía de logística.

Después de haber conformado a los miembros de la **Junta General Electoral,** estos tienen las siguientes tareas:

- Convocar para las elecciones de representantes de la asamblea general
- Elaborar un cronograma de actividades, donde se define el periodo de inscripción de los candidatos a representantes de cada agencia y el calendario de votaciones
- Determina el presupuesto
- Los documentos se envían a aprobar al consejo de administración.
- Determina el lugar de inscripción de los candidatos
- Determina los recintos electorales
- Determina la fecha máxima de inscripción
- Realizar y presentar la guía logística

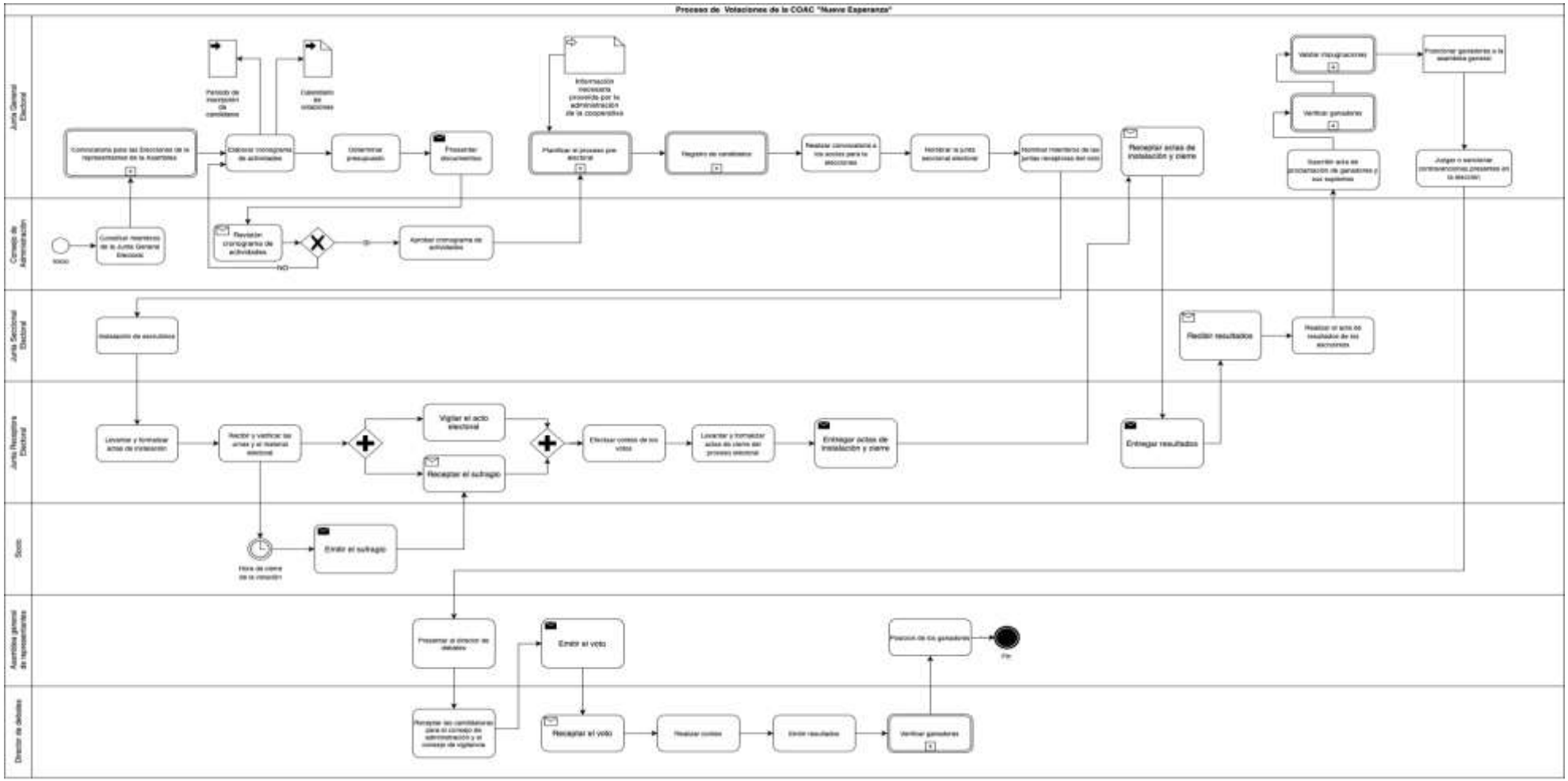


Figura 2-3: Diagrama BPMN del proceso electoral de COAC Nueva Esperanza

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

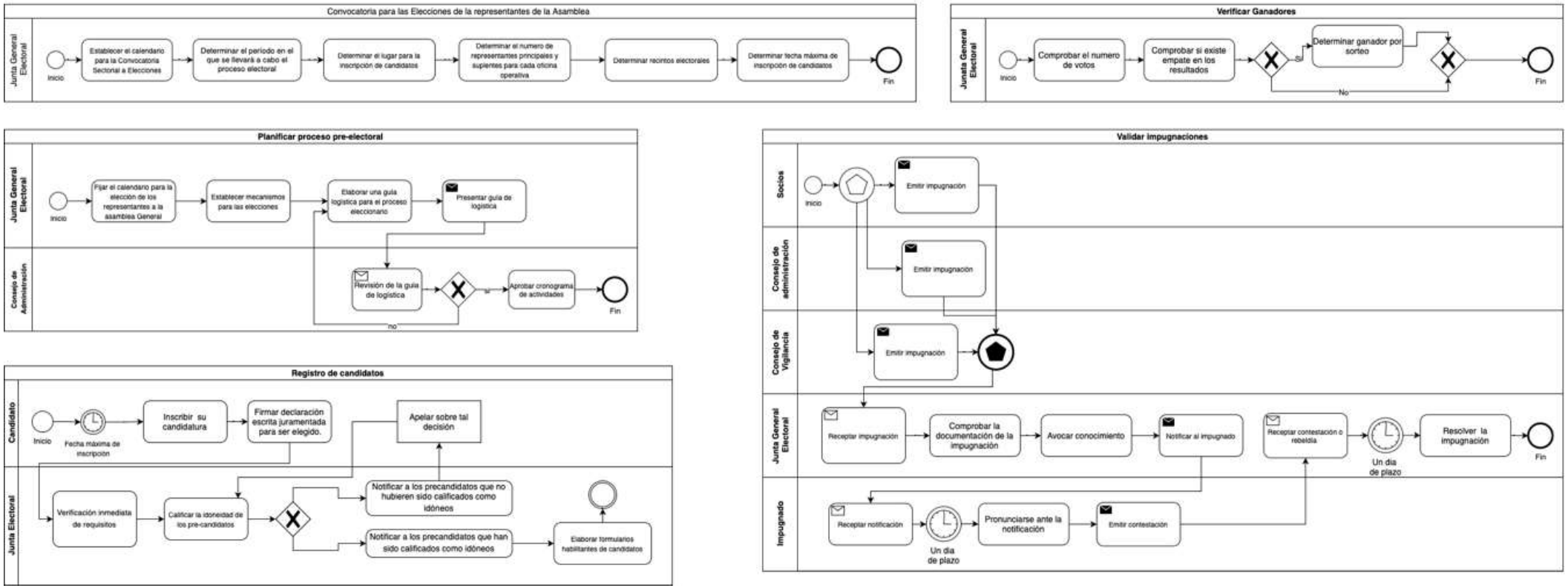


Figura 3-3: Diagrama BPMN de los subprocesos de las elecciones de COAC Nueva Esperanza

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

Posteriormente, arranca la etapa de inscripciones de candidaturas, donde intervienen los **candidatos,** los cuales tienen las siguientes tareas:

- Inscribir la candidatura
    - Firmar una declaración juramentada para ser elegido
    - Inscribirse mediante un formulario que cuente con 5 firmas de respaldo
    - Presentar la información con los dos suplentes, sus hojas de vida y su copia de la cédula
- Enviar a aprobar la inscripción.
- En caso de ser rechazada la inscripción el candidato puede apelar la decisión

Mientras tanto, el deber de la **Junta General Electoral** es:

- Verificar los requisitos del candidato
- Calificar la idoneidad de los candidatos
- Notificar a los candidatos sobre su decisión en la inscripción
- Elaborar formularios habilitantes para los candidatos

Luego de las inscripciones, se realiza una etapa de nombramiento, la Junta General Electoral definirá a los miembros de la **Junta Seccional Electoral** y **Junta Receptora del Voto.**

La siguiente etapa, es el proceso eleccionario, empieza el día planificado por la Junta General Electora y de la mano de la **Junta Seccional Electoral,** quienes proceden a realizar las siguientes tareas:

- Instalación de escrutiños
- Recepción de resultados
- Realizar el acta de resultados de los escrutiños

Por otra parte, las tareas de la **Junta Receptora del Voto** son:

- Levantar y formalizar las actas de instalación
- Recibir y verificar las urnas y material de instalación
- Receptar el sufragio
- Vigilar el acto electoral
- Efectuar el conteo de votos
- Levantar y formalizar actas de cierre del proceso electoral y entregarlas

Así mismo la participación del **socio** es fundamental pues su única tarea es emitir el sufragio en las horas habilitadas por la **Junta General Electoral**

Para terminar la primera fase, la etapa a seguir es la de cierre y consolidación de resultados, donde la tarea de la **Junta General Electoral** es de receptar las actas de instalación y cierre, para que posteriormente la **Junta Receptora del Voto** entregue los resultados a la **Junta Seccional Electoral** para que realice el acta de resultados de escrutinio.

En la etapa de cierre y consolidación de resultados, la **Junta General Electoral** realizará tareas, tales como:

- Suscribir acta de proclamación de ganadores y sus suplentes
- Verificar los ganadores, si hay un empate en el conteo de votos determinar el ganador por sorteo
- Validar y procesar las impugnaciones generadas por un candidato ayudado por el **Consejo de Vigilancia** y el **Consejo de Administración.**
- Posicionar los ganadores de la asamblea general
- Juzgar o sancionar contravenciones presentes en la elección

La segunda fase de las elecciones corresponde a la del consejo de administración y el consejo de vigilancia, aquí participan los ganadores a la asamblea general quienes presentarán al **director de debates,** cuyas tareas son:

- Receptar las candidaturas para el consejo de administración y el consejo de vigilancia
- Receptar el voto otorgado por cada miembro de la **asamblea general**
- Realizar el conteo
- Emitir resultado
- Validar ganadores, si hay un empate entonces realizar un sorteo.
- Posicionar a los ganadores.

El sistema se centrará en la automatización de la primera fase, la elección de los representantes a la asamblea, ya que es la fase que más recursos y tiempo consume. Además, la segunda fase presenta un proceso informal con respecto al uso de la tecnología y no necesita de un sistema de votaciones ya que todo se define entre pocos sufragantes y de forma formal en una reunión.

3.2.2. Fase de diseño

En esta fase incluye la definición del estándar de codificación, arquitectura del sistema, interfaz de usuario que se va a implementar en el producto de software, además se realiza el análisis y diseño de la base de datos misma que será utilizada en el sistema.

3.2.2.1. Arquitectura del sistema

Hoy en día las aplicaciones y sistemas web son cada vez más extensas, integradas y se implementan mediante la utilización de diferentes tecnologías, también son necesarias para asegurar cada vez más la calidad del producto software. De esta manera se realiza una arquitectura de 3 capas para que permita una mejor escalabilidad y eficiencia dentro del sistema. En la **Figura 4 – 3,** se presenta uno de los diagramas que forma parte del documento de arquitectura en el **ANEXO N** y que detalla la arquitectura del sistema.

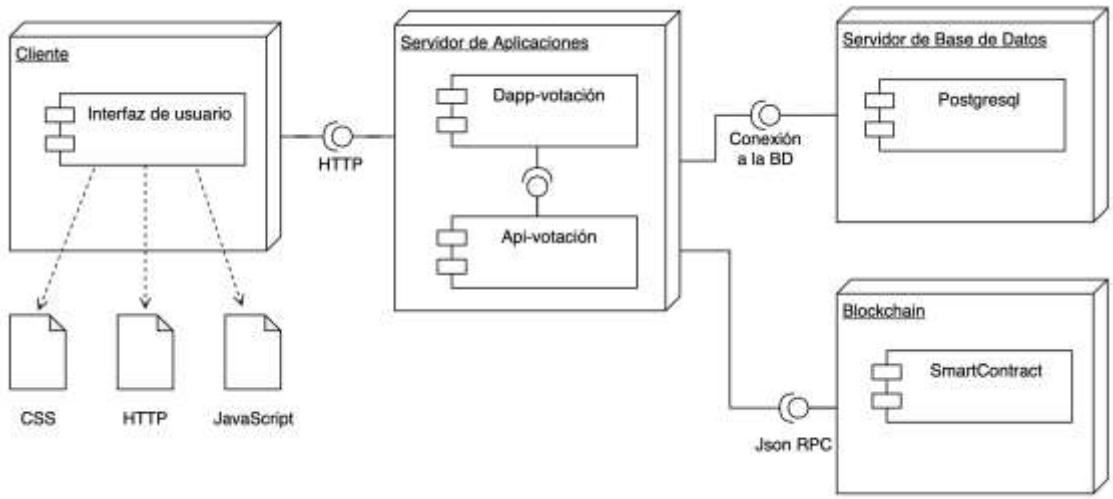


Figura 4-3: Diagrama de componentes del sistema de votaciones

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

3.2.2.2. Diseño de la interfaz de usuario

Con el objetivo de generar una maquetación para distribuir y organizar la información en la interfaz de usuario, se utilizado la herramienta Figma para desarrollar un maqueta de baja fidelidad agradable y entendible, por ejemplo en la **Figura 5 - 3**. En el **ANEXO M**, se encuentran las demás propuestas de diseño web.

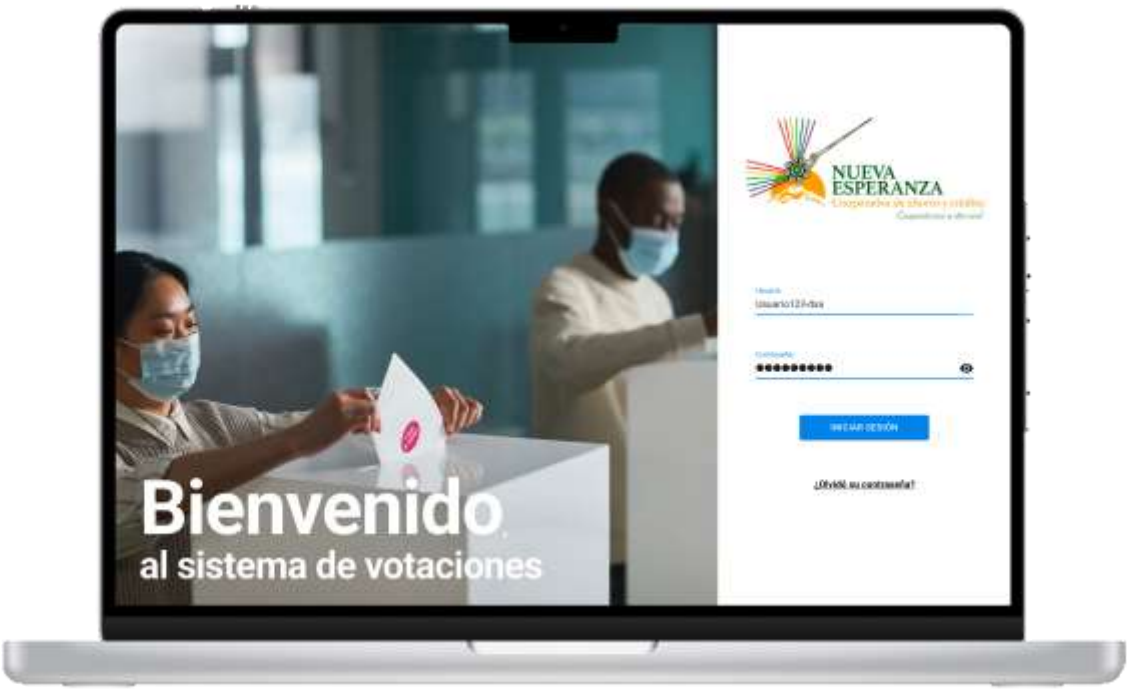


Figura 5-3: Prototipo de la pantalla de inicio de sesión del sistema

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

3.2.2.3. Definir el estándar de codificación

Debido a que el desarrollo del sistema se realiza en pareja es necesario establecer un estándar de codificación para mantener un código legible y organizado. Al codificar bajo un estándar permite que el desarrollo parezca que fue hecho por un único desarrollador, también permite a otros desarrolladores la fácil comprensión del código, además, favorece en un futuro las tareas de corrección y o mantenimiento con facilidad, para ello sea seleccionado el estándar Camel Case.

Camel Case, es una notación que consiste en escribir secuencias de palabras con la primera letra de cada palabra en mayúscula. Pero la primera letra de la primera palabra puede ser a veces minúscula según el tipo de Camel Case. Estas diferentes palabras pueden estar pegadas o separadas por un espacio. El objetivo es que las palabras compuestas sean más legibles. En la SEO, su función principal es hacer que los **títulos de las páginas web sean** más visibles en las SERP**.**

3.2.2.4. Diseño de la base de datos

Para el diseño de la base de datos, en el **ANEXO G** se ejemplifica el modelo conceptual de la base de datos a través del diagrama relacional, a partir de ello se genera el modelo lógico de la base de datos. En la **Figura 6 – 3** se ilustra el diagrama lógico que se compone de 10 tablas relacionadas, tales como: Usuarios, Notificación, Recuperación, Cuenta, Billetera, Justificaciones, Agencias, Inscripciones, Representantes y Elecciones.

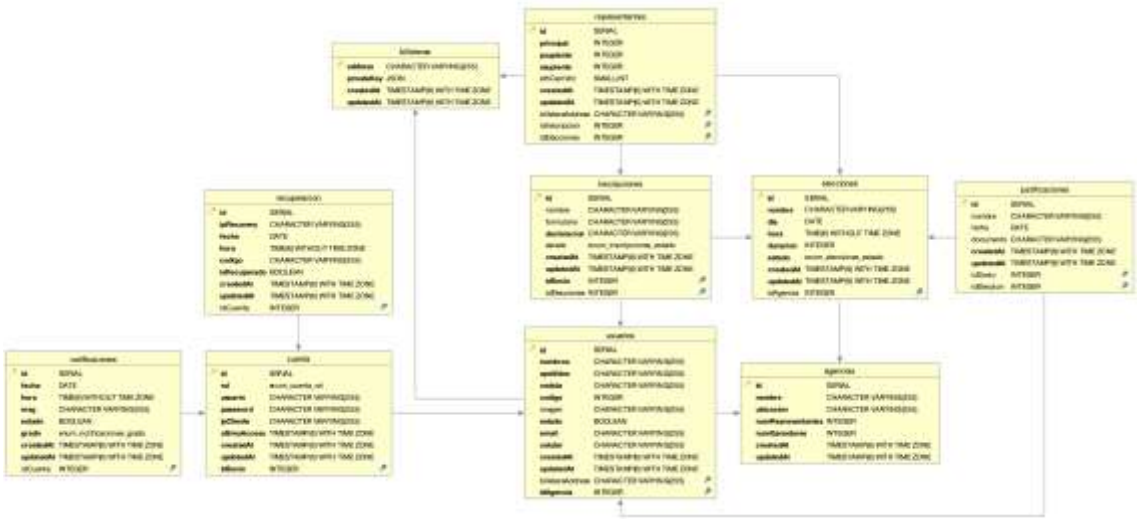


Figura 6-3: Diagrama lógico de la base de datos

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

El modelo de la base de datos se divide en dos gráficos, se ilustran en la **Figura 7-3** y **Figura 8-3** para mejorar la apreciación de las tablas y las relaciones entre ellas. La división del modelo permite una representación más clara y visual de cada tabla individual con sus relaciones. En resumen, las figuras brindan una comprensión más profunda de cómo los datos se almacenan y se relacionan.

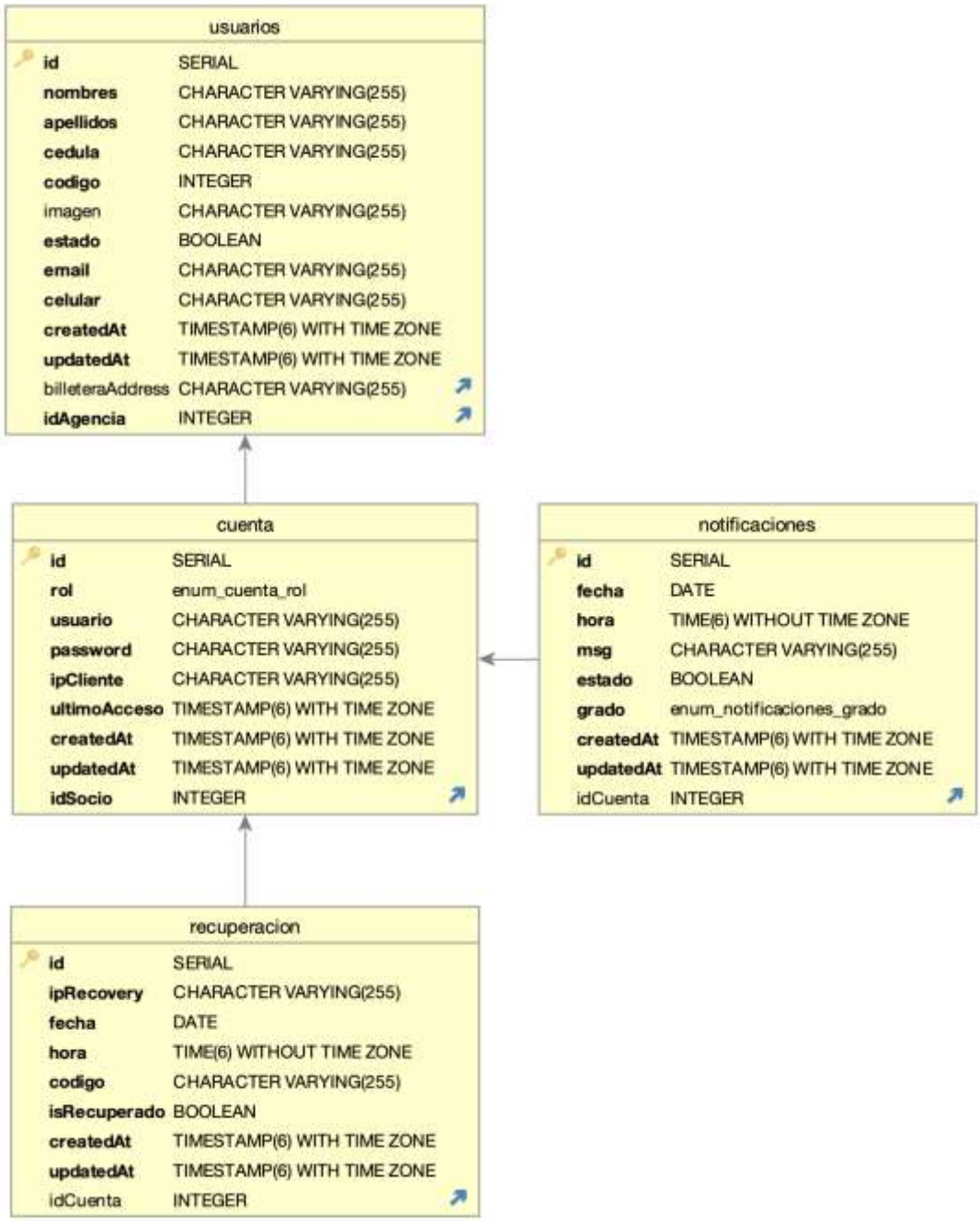


Figura 7-3: Diagrama lógico de la base de datos, parte 1

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

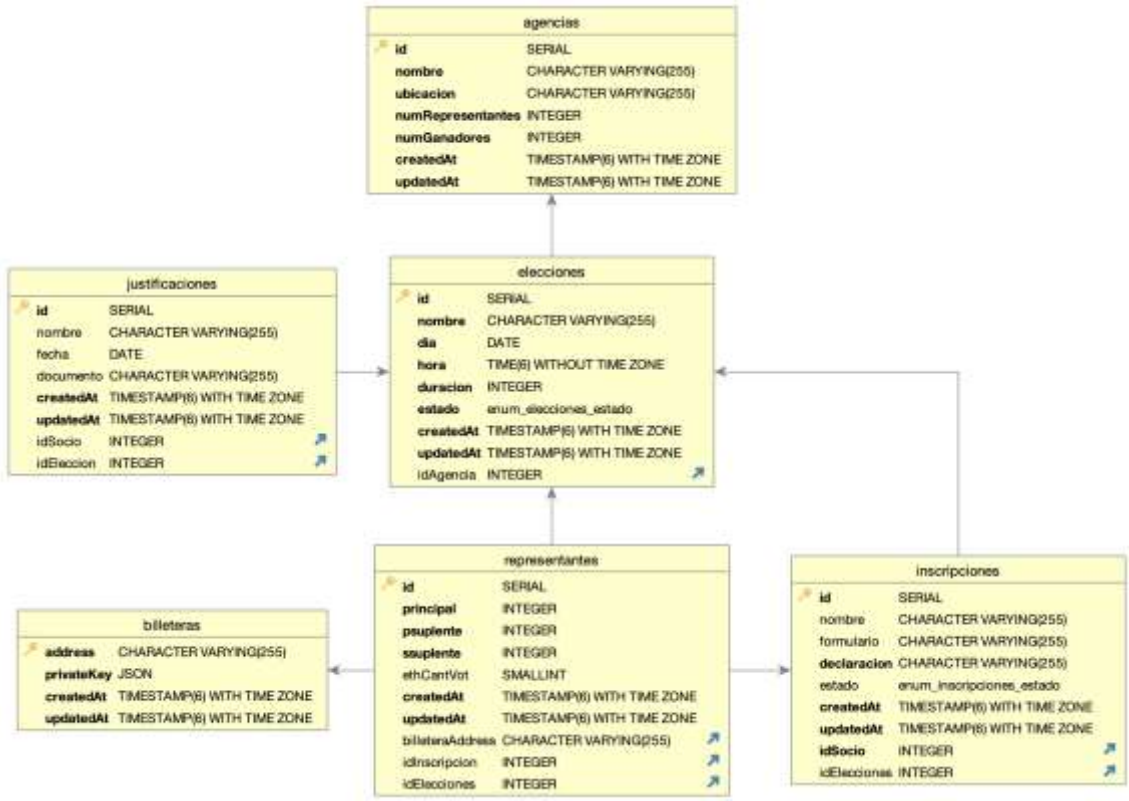


Figura 8-3: Diagrama lógico de la base de datos, parte 2

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

Para tener una correcta documentación de las tablas de la base de datos y los campos de estas, el diccionario de datos es una herramienta que promueve el entendimiento y utilización de los datos. En la **Tabla 13 – 3**, se ejemplifica un diccionario de datos de una de las tablas de la base de datos utilizada en el sistema, el resto de las tablas se encuentran detalladas en el **ANEXO L.**

Tabla 18-3: Diccionario de datos para la tabla Usuarios

Nombre del archivo: Usuarios **Descripción del archivo**: Persona que pertenece a una agencia				
Nombre del campo	**Descripción**	**Tipo de dato y tamaño**	**Permite NULL**	**Valor permitido del dato**
idUsuario (PK)	Identificador del usuario	int	no	[000000000] *El valor es autoincremental*
nombres	Nombres completos del usuario	string	no	primer nombre + (segundo nombre) = {[A-Z][a-z]}
apellidos	Apellidos completos del usuario	string	no	primer apellido + (segundo apellido) = {[A-Z][a-z]}
cedula	Numero de cedula de	string	no	[0000000000]

	identidad del usuario			* permite un digito de [0-9] y requiere la entrada de los 10 dígitos *
codigo	Código que identifica a un usuario	int	no	[000000] * permite un digito de [0-9] y requiere la entrada de los 6 dígitos *
imagen	Imagen del usuario	string	si	* Path/Dirección del servidor donde se encuentra alojada la imagen *
estado	Estado del usuario en las elecciones	bool	no	[true | false] *significado: true: Activo | false: Inactivo *
email	Dirección de correo electrónico del usuario	string	no	nombre + @ + dominio = {[a-z]} + @ + {[a-z].[a-z]}
telefono	Número de teléfono del usuario	string	no	[0000000000] * permite un digito de [0-9] y requiere la entrada de los 10 dígitos *
billetera (FK)	Identificador de la billetera asignada al usuario	string	no	* unique *
idAgencia (FK)	Identificador de la agencia a la que pertenece el usuario	int	no	* *

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

3.2.2.5. Diagramas de actividades

Los diagramas de actividades representan un flujo de acciones que se realizan dentro del sistema, simulando el comportamiento de este. En la **Figura 9 – 3** se ejemplifica un diagrama de actividades del sistema, el resto de los diagramas correspondientes a las operaciones que se realizan sobre cada tabla de la base de datos se detallan en el **ANEXO H.**

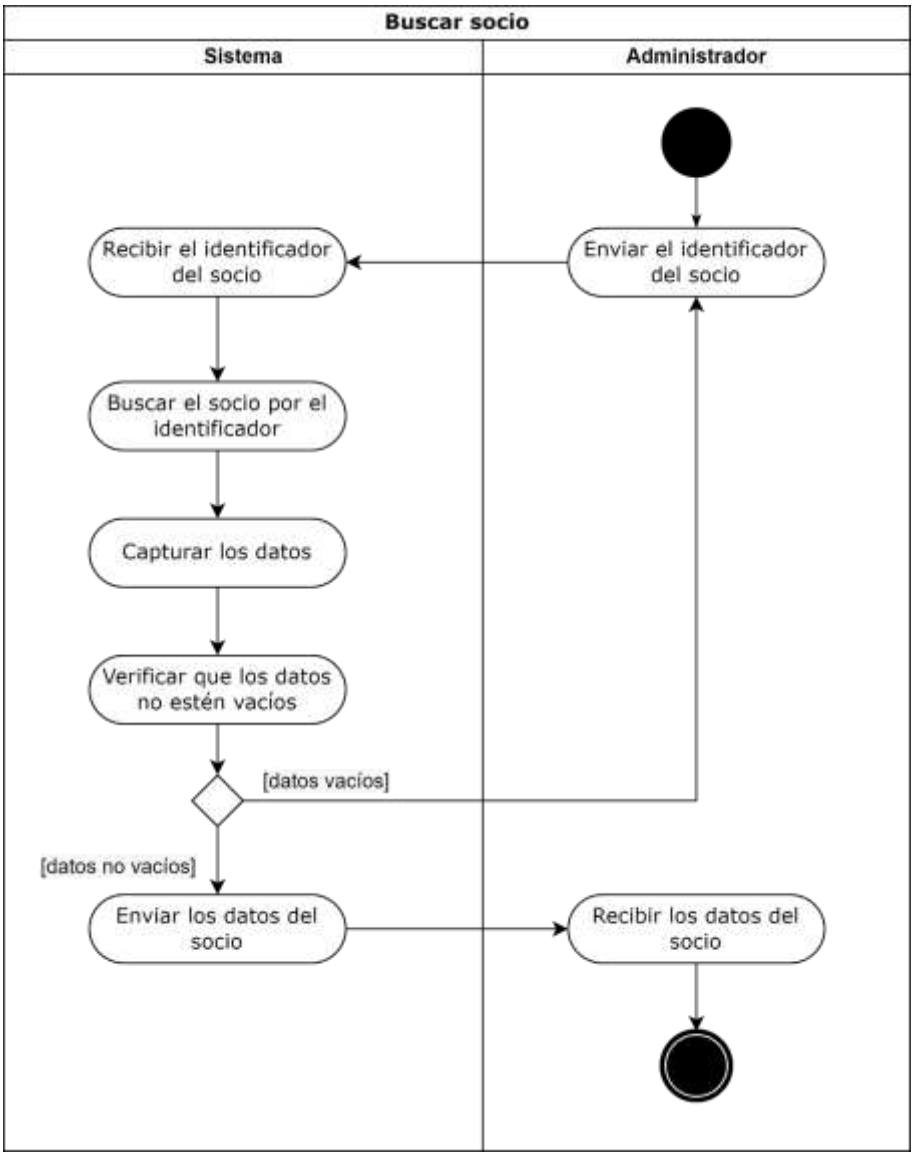


Figura 9-3: Diagrama de actividades para la búsqueda de un usuario

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

3.2.2.6. Diagramas de secuencia

Los diagramas de secuencia representan la interacción entre los objetos del sistema en un proceso a lo largo del tiempo. En la **Figura 10 – 3** se ejemplifica un diagrama de secuencia del sistema, el resto de los diagramas correspondientes a las operaciones que se realizan sobre cada tabla de la base de datos se detallan en el **ANEXO I.**

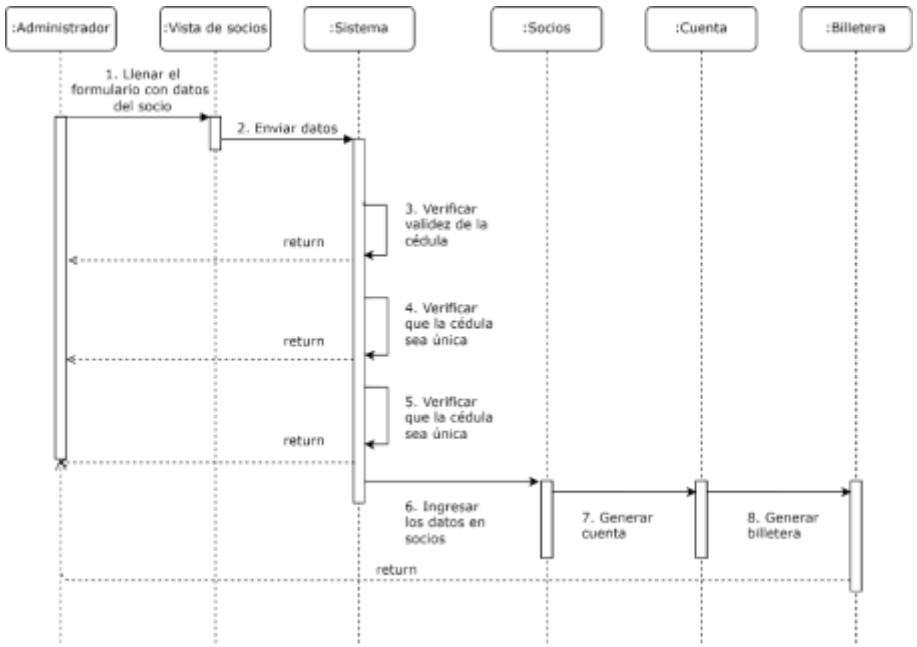


Figura 10-3: Diagrama de secuencia para el ingreso de un socio

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

3.2.2.7. Diagramas de estado

Los diagramas de estado representan un flujo de acciones que se realizan dentro del sistema, simulando el comportamiento de este. En la **Figura 11 – 3** se ejemplifica un diagrama de estado del sistema, el resto de los diagramas correspondientes a las operaciones que se realizan sobre cada tabla de la base de datos se detallan en el **ANEXO J.**

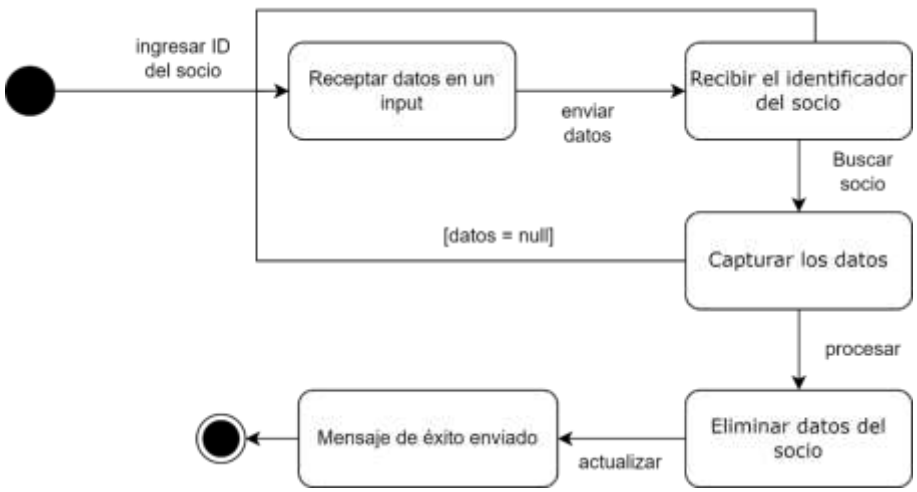


Figura 11-3: Diagrama de estado para la eliminación de un socio

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

3.2.2.8. Diagramas de colaboración

Los diagramas de colaboración modelan el comportamiento dinámico del sistema mostrando la interacción entre todos los objetos, muestra los vínculos que tienen los objetos entre sí ya sea para intercambiar mensajes o realizar operaciones. En la **Figura 12 – 3** se ejemplifica un diagrama de colaboración del sistema, el resto de los diagramas correspondientes a las operaciones que se realizan sobre cada tabla de la base de datos se detallan en el **ANEXO K.**

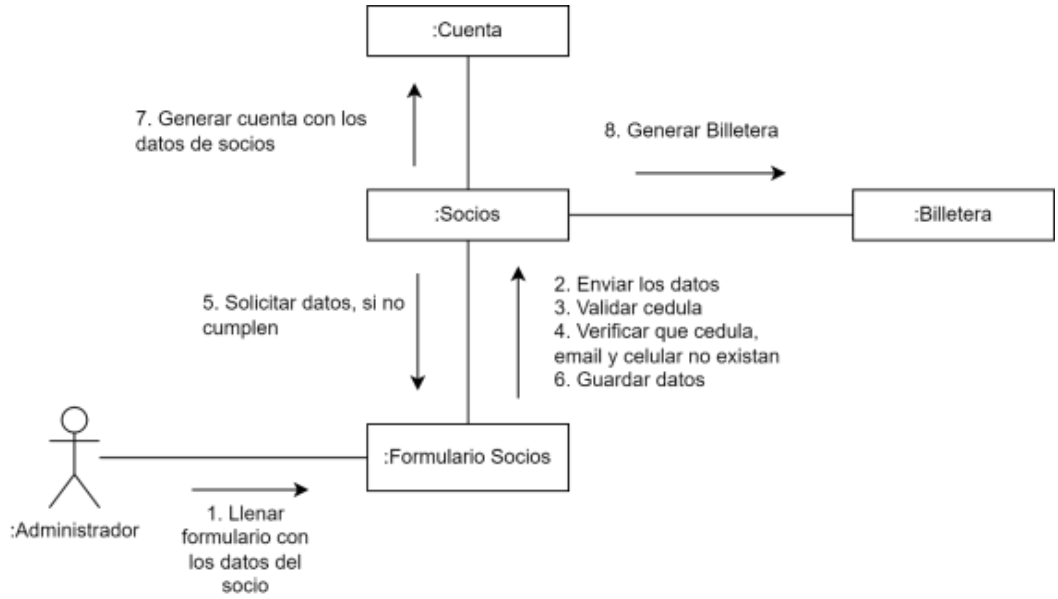


Figura 12-3: Diagrama de colaboración para el ingreso de un socio

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

3.2.3.Fase de construcción

Para cumplir con los requerimientos funcionales definidos por el cliente mediante la definición de cada uno de los casos de uso del sistema, el desarrollo del sistema se segmenta en tres partes: la primera parte contiene la implementación de la API de votaciones, en la segunda parte corresponde a la implantación de los contratos inteligentes y la tercera parte corresponde al Front-End (interfaz gráfica) con el desarrollo de la Dapp de votaciones.

En la Api de votaciones se han desarrollado cuatro métodos de solicitudes HTTP los cuales son: GET, POST, PUT y DELETE, a cada uno de estos métodos se realizó la debida verificación de los datos y la autenticación de usuario. Cómo resultados obtenidos un total de 40 archivos, los cuales se segmenten entre los archivos que el modelo de la base de datos, los casos de uso, los controladores, las rutas y el *middleware*. Todo lo anterior se ha desarrollado tomando en consideración el estilo arquitectónico de *Clean Architecture* creado por Robert C. Martin.

Clean Architecture es un conjunto de estándares que tiene como objetivo desarrollar arquitecturas en capas que faciliten la escritura de código de calidad que funcione mejor, sea fácil de mantener y tenga menos dependencias a medida que crezca el proyecto. Esta arquitectura se puede aplicar sin importar el lenguaje en el que codifique.

En cuanto a los archivos de la app-votaciones contiene un total de 12 archivos entre ellos: controlller, css, extensiones, imágenes, js, login, pages, plantilla, resources, .htaccess, index, index1.

3.2.4.Fase de Transición

Para realizar el despliegue de la aplicación se define el diagrama de despliegue. En él se define todos los componentes del sistema y su interacción como se observa en la **Figura 13-3,** pertenece al **ANEXO O**, anexo que provee más diagramas para el apoyo del despliegue de la aplicación.

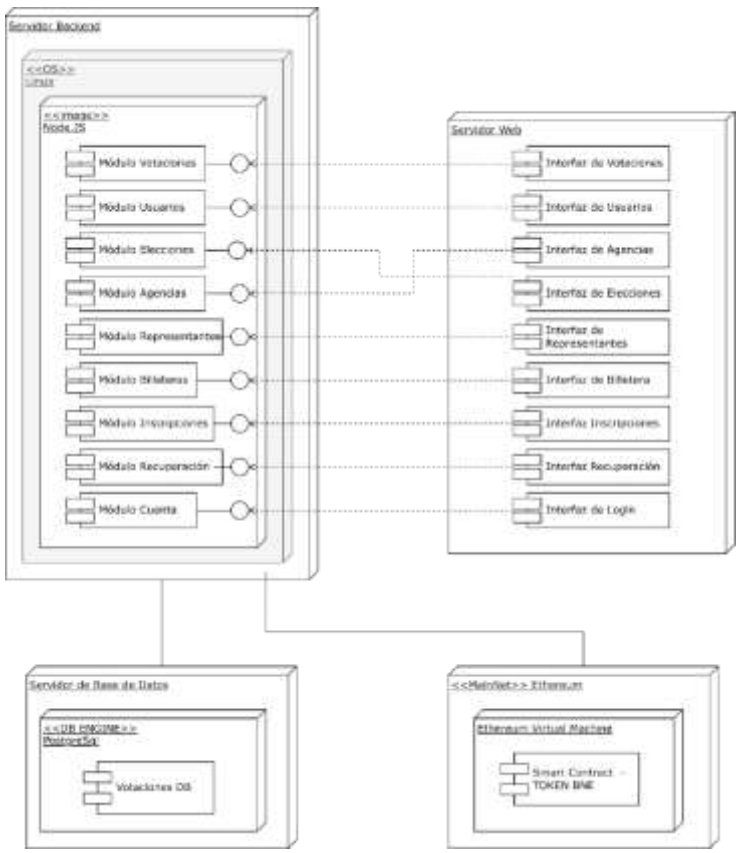


Figura 13-3: Diagrama de despliegue de la aplicación descentralizada

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

El despliegue de la aplicación descentralizada se realiza en la nube de Amazon Web Services, se usa el servicio de Amazon Lightsail que permite aprovisionar instancias de máquinas virtuales para el despliegue de aplicaciones web. Primero, se despliega la base de datos, para ello en el panel de administración del Lightsail se configura el despliegue de la instancia de PostgreSQL con una capacidad de 2 vCPU, 40 GB de almacenamiento SSD y 1 GB RAM, características que se observan en la **Figura 14-3**

Figura 14-3: Instancia de base de datos de AWS Lightsail

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

Posteriormente, se levanta el servidor para alojar el Backend de la aplicación, pero antes en el archivo de configuración se configura la conexión a la base de datos como se ilustra en la **Figura 15-3.**

Figura 15-3: Archivo de configuración para la conexión a la instancia de base de datos

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

A continuación, se aprovisiona el servidor de base de datos, para ello se utiliza una imagen ya configurada de Linux con NodeJs con una capacidad de hardware de 1 vCPU, 20 GB SSD de almacenamiento y 512 GB RAM como se muestra en la **Figura 16-3.**

Figura 16-3: Instancia de servidor web proveída en AWS Lightsail

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

Se debe agregar que antes de ejecutar la instancia del Backend, se provee una serie de comandos a ejecutarse en el aprovisionamiento de la instancia, comando que se ilustran en la **Figura 17-3.**

Figura 17-3: Comandos ejecutados en la instancia del Backend

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

Para el despliegue del Frontend, se realiza una construcción del proyecto usando el comando *yarn build* proporcionado por el gestor de paquetes, el resultado es una serie de archivos estáticos listos para desplegarse. Usando el servicio de Amazon S3, como se muestra en la **Figura 18- 3** se crea un contenedor para almacenar los archivos estáticos y publicarlos mediante una ruta.

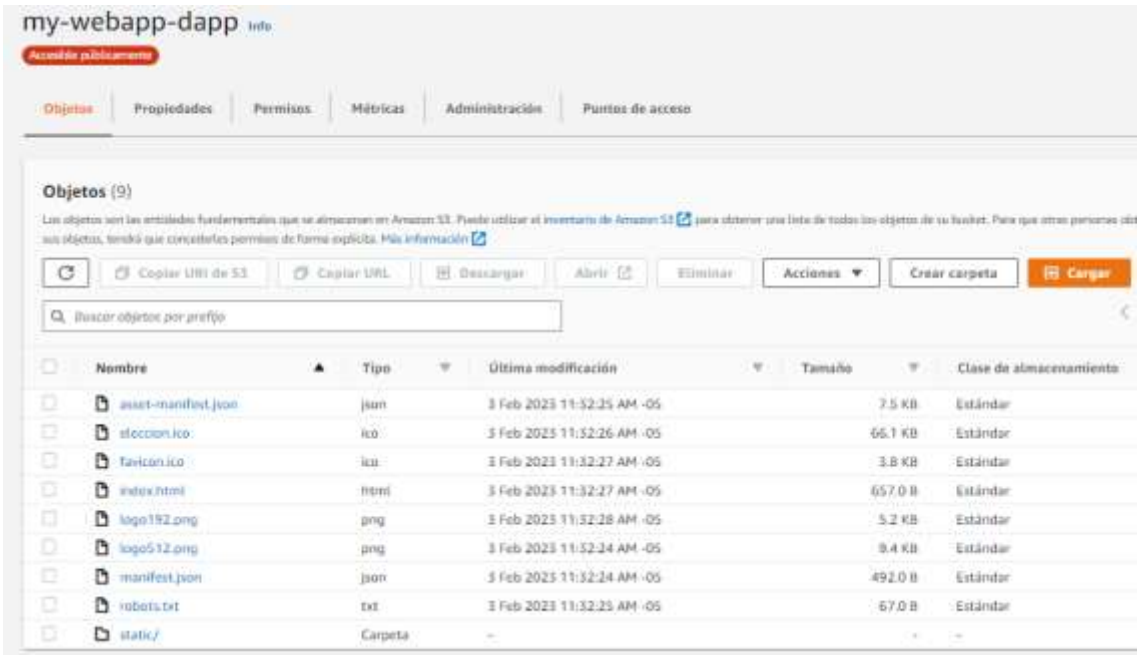


Figura 18-3: Contenedor de almacenamiento para guardar los archivos estáticos del frontend

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

Por otra parte, el despliegue del contrato inteligente se lo realiza con la herramienta truffle, para ello en el archivo de configuración del proyecto se configura la red donde se va a desplegar, el id de la red, la cantidad de gas a utilizar en el despliegue y otros atributos que se detallan en la **Figura 19-3.**

```
networks: {
  goerli: {
    provider: () => new HDWalletProvider(
      process.env.MNEMONIC,
      `https://goerli.infura.io/v3/${process.env.INFURA_API_KEY}`),
    network_id: 5,
    gas: 5500000,
    confirmations: 2,    // # of confs to wait between deployments. (default: 0)
    timeoutBlocks: 200,  // # of blocks before a deployment times out  (minimum/default: 50)
    skipDryRun: true     // Skip dry run before migrations? (default: false for public nets )
  },
},
```

Figura 19-3: Archivo de configuración de red de despliegue.

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

Usando los comandos que provee la librería de Truffle se compila el contrato, se lo prueba, se los ejecuta y al final se despliega, como resultado se otorga el hash de transacción que indica la

ubicación del bloque donde se halla el contrato inteligente. Usando el explorador de Blockchain Etherscan se puede consultar la ubicación del contrato inteligente y otros parámetros que se observan en la **Figura 20-3**

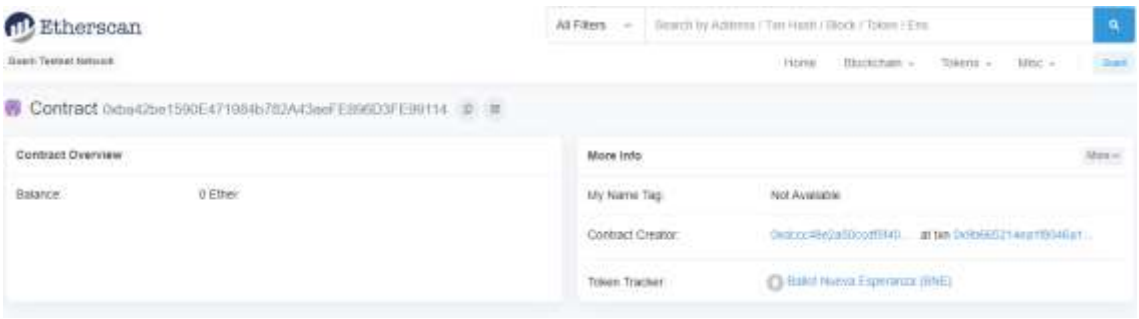


Figura 20-3: Transacción donde esta desplegado el contrato inteligente

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

Por último, el uso de todos los servicios mencionados dio como resultado la infraestructura de la **Figura 21-3,** se detalla la interacción de todos los servicios de la nube de Amazon Web Services, tales como: el uso de redes privadas virtuales, grupos de seguridad, almacenamiento de objetos S3, servicio de DNS, servicio de redes de distribución de contenido para el Frontend, etc. Además, la infraestructura posee la característica de alta disponibilidad debido al uso del escalamiento horizontal y el alojamiento en 2 zonas de disponibilidad.

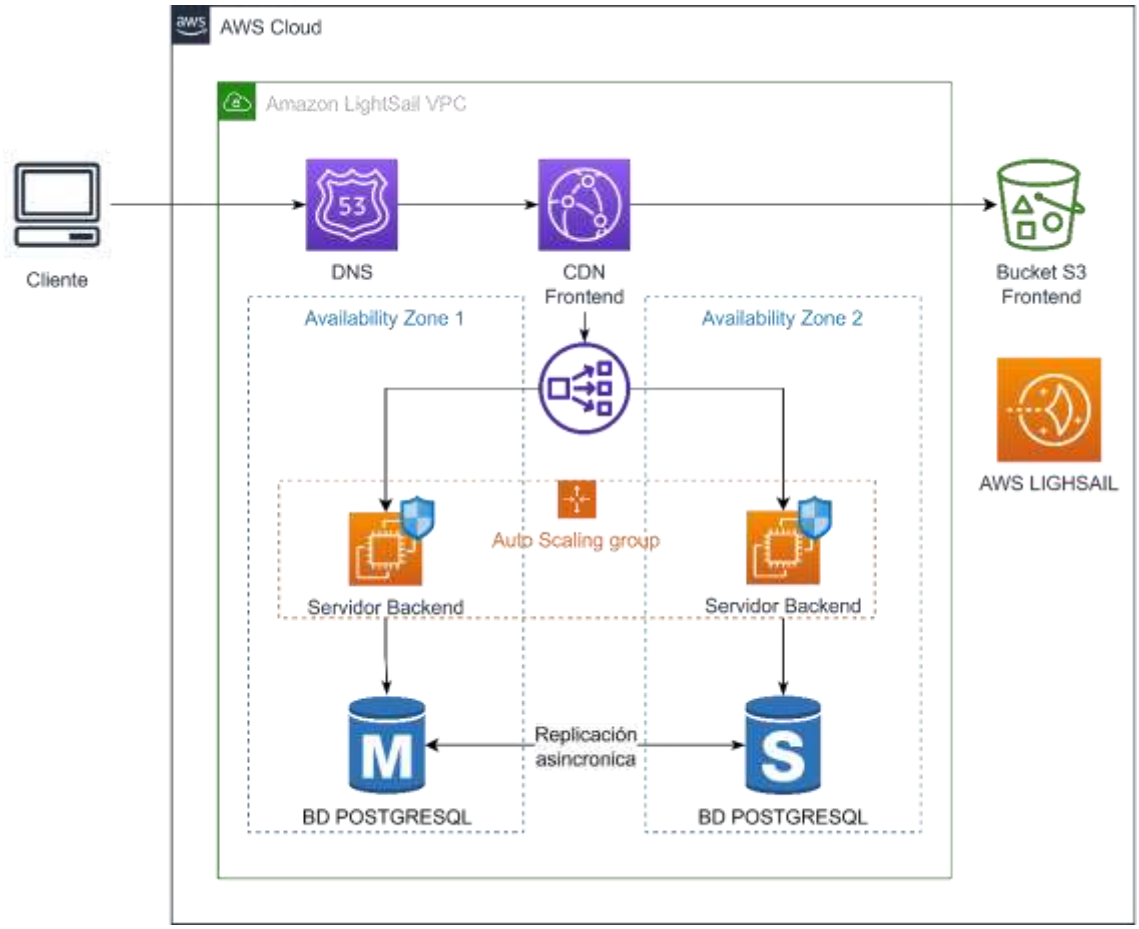


Figura 21-3: Infraestructura del sistema de votaciones

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

CAPÍTULO IV

4. RESULTADOS

El presente capítulo se analiza, evalúa y describe los resultados obtenidos sobre la utilización de los recursos y seguridad de la aplicación descentralizada de votaciones.

4.1. Eficiencia de desempeño

Dentro de la eficiencia de desempeño se mide la subcaracterística de utilización de recursos.

4.1.1. Utilización de Recursos

En el siguiente aparatado se evalúa el uso de la CPU, el uso de la memoria RAM y el uso del gas en las transacciones.

4.1.1.1. Uso de la CPU

Para evaluar el indicador de uso del CPU se considera el porcentaje de tiempo del CPU para realizar una determinada tarea, para ello, se utiliza el monitor de rendimiento que proporciona el sistema operativo anfitrión para obtener los datos. En la **Figura 1-4,** se ejemplifica la recolección de datos para el caso de uso de emitir un voto, el resto de los datos recolectados se encuentran detallados en el **ANEXO P.**

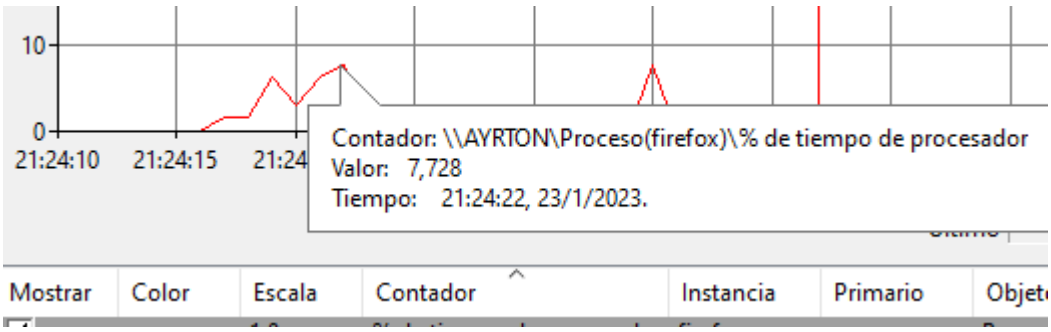


Figura 1-4: Diagrama de línea para porcentaje de tiempo de procesador para emitir un voto

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

4.1.1.2. Uso de la memoria RAM

Para evaluar el indicador se considera el tamaño en Megabytes (por sus siglas MB) usado para realizar una determinada tarea, para obtener los datos se utiliza el administrador de tareas proporcionado por el navegador anfitrión. En la **Figura 2-4**, se ejemplifica la recolección de datos para el caso de uso de ingresar una agencia, el resto de datos recolectados se encuentran detallados en el **ANEXO P.**

Figura 2-4: Cantidad de memoria RAM usada para ingresar una agencia

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

4.1.1.3. Uso del Gas

Para evaluar el indicador se considera la cantidad de GWEI usados para realizar una determinada tarea, para obtener los datos se utiliza el explorador de la red principal donde se aloja el contrato inteligente. Cabe resaltar que se eligen solo las tareas donde se involucra la comunicación con la red principal de Ethereum. En la **Figura 3-4,** se ejemplifica la recolección de datos para el caso de uso de emitir un voto, el resto de los datos recolectados se encuentran detallados en el **ANEXO P.**

Figura 3-4: Reporte de la transacción de uso del gas al emitir un voto

Realizado por: Avalos Ayrton, Manzano Edwin, 2023

4.2. Resultados obtenidos de la utilización de recursos

En este apartado se presenta los resultados para la subcaracterística de utilización de recursos y sus respectivos indicadores o criterios de evaluación en el uso de CPU, memoria RAM y del GAS.

4.2.1. Uso de la CPU

El indicador aceptable para el porcentaje de tiempo de procesador es la aproximación al valor de cero. En la **Tabla 1-4,** se presenta la escala asignada para medir el porcentaje de tiempo de procesador.

Tabla 1-4: Niveles de puntuación para el uso de CPU

Escala asignada (%)	Nivel de puntuación	Grado de satisfacción
0 – 27,5	Cumple con los requisitos	Muy satisfactorio
27,6 – 50,00	Aceptable	Satisfactorio
51,00 – 87,50	Mínimamente aceptable	Insatisfactorio
87,60 – 100	Inaceptable	

Fuente: (IEEE Std 2011c)

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

Para determinar la utilización de recursos y eficiencia en ejecutar las tareas del sistema de votaciones, en la **Tabla 2-4** se presenta la recolección de datos al medir el uso del CPU en varios casos de uso del sistema.

Tabla 2-4: Resultados obtenidos para el porcentaje de tiempo de procesador

Caso de uso	Uso del CPU (%)
Ingresar agencia	20,316
Buscar agencia	47,730
Eliminar una agencia	50,234
Actualizar una agencia	6,267
Ingresar usuario	42,181
Actualizar usuario	7,945
Buscar usuario	12,512
Eliminar un usuario	7,842
Registrar cuenta de un usuario	26,604
Buscar cuenta de un usuario	7,819
Actualizar datos de la cuenta del usuario	9,404
Iniciar sesión	6,573
Recuperar contraseña	6,237
Ingresar notificación	3,128
Actualizar notificación	4,622
Buscar una notificación	3,119
Ingreso masivo de socios	32,930
Crear una billetera	3,116
Buscar una billetera	6,283
Registrar una elección	7,820
Buscar una elección	12,477
Eliminar una elección	4,704
Actualizar una elección	3,131
Registrar una lista	15,659
Buscar una lista	40,159
Eliminar una lista	17,257
Actualizar una lista	10,764
Registrar una inscripción	17,120
Actualizar una inscripción	10,999
Buscar una inscripción	28,253
Generar reporte de votantes	25,085
Generar reporte de resultados de la elección	31,174
Emitir voto	7,728
Fondear token de votación	23,479
Fondear recursos de votación	12,578
Ingresar justificación	15,649
Actualizar justificación	14,050
Buscar justificación	15,699
Promedio	**16,280**

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

En la recolección y análisis de los datos correspondientes al porcentaje de tiempo de procesador se obtiene como promedio un 16,28 %. En otras palabras, en un intervalo de 5 segundos el 16,18% del tiempo el procesador se dedica a ejecutar los procesos del sistema de votaciones. De acuerdo con la **Tabla 1-4,** el porcentaje promedio se ubica en la escala [0 – 27,5], cumpliendo los requisitos y con un grado muy satisfactorio.

4.2.2. Uso de la memoria RAM

Está subcaracterística de la eficiencia desempeño tiene una calificación más alta entre menos memoria RAM utilice en cada una de las actividades. En la **Tabla 3-4**, se detallan los indicadores para medir el uso de la memoria RAM.

Tabla 3-4: Indicadores de evaluación de uso de memoria RAM

Calificación	Uso	Valor cualitativo
100%	[0-150] MB	Excelente
90%	[151-250] MB	Muy bueno
75%	[251-350] MB	Bueno
50%	[351-450] MB	Aceptarme
20%	[451-550] MB	Regular
0%	[551 -∞] MB	Malo

Fuente:(Gómez, Arcos-Medina y Pástor 2020)

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

Con el propósito de representar los resultados de las actividades específicas para medir la utilización de la memoria RAM, la **Tabla 4-4** presenta el uso de memoria RAM de cada tarea efectuada.

Tabla 4-4: Promedios obtenidos de memoria RAM

Caso de uso	Uso de la RAM (MB)
Ingresar agencia	150
Buscar agencia	171
Eliminar una agencia	181
Actualizar una agencia	152
Ingresar usuario	108
Actualizar usuario	133
Buscar usuario	141
Eliminar un usuario	133
Registrar cuenta de un usuario	116

Buscar cuenta de un usuario	140
Actualizar datos de la cuenta del usuario	147
Iniciar sesión	114
Recuperar contraseña	129
Ingresar notificación	146
Actualizar notificación	151
Buscar una notificación	139
Ingreso masivo de socios	168
Crear una billetera	157
Buscar una billetera	145
Registrar una elección	158
Buscar una elección	151
Eliminar una elección	151
Actualizar una elección	208
Registrar una lista	181
Buscar una lista	186
Eliminar una lista	182
Actualizar una lista	188
Registrar una inscripción	191
Actualizar una inscripción	187
Buscar una inscripción	197
Generar reporte de votantes	204
Generar reporte de resultados de la elección	212
Emitir voto	184
Fondear token de votación	196
Fondear recursos de votación	209
Ingresar justificación	195
Actualizar justificación	212
Buscar justificación	196
Promedio	**166,026**

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

Tras realizar el análisis de la métrica de uso memoria RAM perteneciente a la subcaracterística de la utilización de recursos, se obtuvo un promedio de 166,026 MB, con referencia a las diferentes actividades realizadas, además, de acuerdo con los indicadores de evaluación la DAPP se ubica en la escala de [151-250] MB, lo que significa que se encuentra en un rango de muy bueno, representado con una valoración del 90%

4.2.3.Uso del GAS

El indicador aceptable para el uso del GAS al realizar una transacción es la aproximación a 0 GWEI, ya que la cantidad de GWEI consumidos representa la cantidad de recursos financieros

para que la Ethereum Virtual Machine consolide una transacción en la Blockchain. La **Tabla 5-4** presenta la escala asignada para medir el uso de GAS.

Tabla 5-4: Niveles de puntuación para el uso de GAS

Escala asignada (WEI)	Nivel de puntuación	Grado de satisfacción
0 - 15	Cumple con los requisitos	Muy satisfactorio
16 – 30	Aceptable	Satisfactorio
31 – 45	Mínimamente aceptable	Insatisfactorio
46 - ∞	Inaceptable	

Fuente: (ISO/TR 23576 2020)

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

Para determinar la utilización de recursos y eficiencia en realizar transacciones en la Blockchain, la **Tabla 6-4** presenta la recolección de datos al medir el uso del GAS en los procesos que interactúan con la red principal de Ethereum.

Tabla 6-4: Resultados obtenidos para el uso de GAS

Caso de uso	GWEIs	WEI
Registrar una elección	0,000000024	24
Fondear recursos de votación	0,000000017	17
Fondear token de votación	0,000000016	16
Emitir voto	0,000000015	15
Promedio	**0,000000018**	**18**

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

En la recolección y análisis de los datos correspondientes al porcentaje de tiempo de procesador se obtiene como promedio un **0,000000018 GWEI** en su equivalente a 18 WEI. Se determina que la cantidad de GWEI promedio utilizada para realizar una transacción en la Blockchain se encuentra en la escala de [16 – 30] WEI, con un nivel de puntuación aceptable y un grado de satisfactorio.

4.3. Seguridad

Para medir cada una de las subcaracterísticas de la seguridad de la norma ISO/IEC 25010 se utiliza una combinación de encuestas, criterios de evaluación y métricas establecidos por la metodología GQM, descrita en el **ANEXO D**, la encuesta fue aplicada a un grupo de seis tecnicos que trabajan en el área de TI de la Cooperativa, los resultados se aprecian en la **Tabla 7-4.**

Tabla 7-4: Resultados obtenidos para los criterios de seguridad

	1	2	3	4	5	6	Promedio
C1	1	1	1	0	0	0	0,5
C2	1	0	1	0	0	1	0,5
C3	1	1	1	1	1	1	1
C4	0,5	1	0,5	1	1	0,5	0,75
I5	1	1	1	1	0	1	0,83
I6	1	1	1	0	0	0	0,5
I7	1	1	1	1	1	1	1
NR8	0	0	0	0	0	0	0
NR9	1	1	1	1	1	1	1
NR10	1	1	1	1	1	1	1
NR11	0	0	0	0	0	0	0
R12	1	1	1	1	1	1	1
R13	0	0	0	0	0	0	0
A14	1	1	1	1	1	1	1
A15	1	1	1	1	1	1	1

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

A cada subcaracterística se le asigno una ponderación para conocer el nivel de seguridad de la DAPP en el área de votaciones. La **Tabla 8-4** detalla los diferentes porcentajes (%) asignados.

Tabla 8-4: Ponderación de la seguridad

Subcaracterísticas	**Porcentaje (%)**
Confidencialidad	25
Integridad	25
No-Repudio	15
Responsabilidad	15
Autenticidad	20
Total	**100**

Fuente: (Calabrese et al. 2017)

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

4.3.1. Análisis de resultados Seguridad

La **Tabla 9-4** detalla el promedio total de cada una de las sus características de seguridad. Se considera que las subcaracterísticas con mayor puntuación son la autenticidad e integridad mientras que el no repudio y responsabilidad son las subcaracterísticas con menor valoración.

Tabla 9-4: Resultados de las subcaracterísticas de la seguridad

Subcaracterísticas	Promedio sobre 1	Porcentaje	Ponderación
Confidencialidad	0,83	20,83	25
Integridad	0,94	23,61	25
No-Repudio	1	15	15
Responsabilidad	1	15	15
Autenticidad	1	20	20
Total		**94,44**	**100**

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

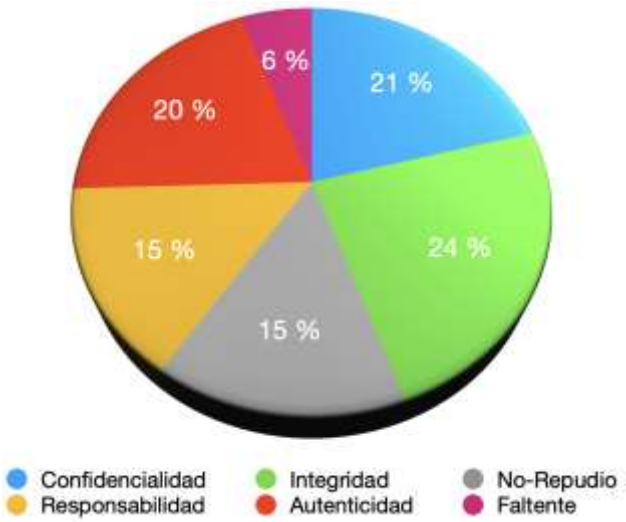


Gráfico 1-4: Representación de las subcaracterísticas de seguridad que posee la DAPP

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

El **Grafico 1-4** muestra que la confidencialidad alcanza un 20,83% del 25% máximo, mientras que la responsabilidad y el No Repudio tienen un porcentaje del 15%. La integridad registra un porcentaje del 23,61% y la autenticidad alcanza un 20%.

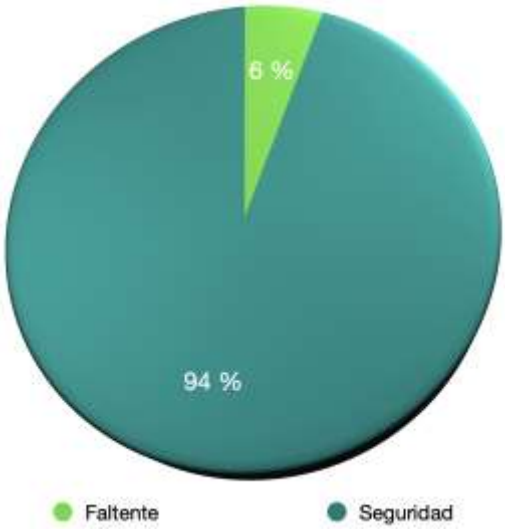


Gráfico 2-4: Nivel de seguridad de la DAPP

Realizado por: Manzano Edwin, Ayrton Avalos, 2023

De acuerdo con los resultados representados en el **Gráfico 2-4,** se puede concluir que el nivel de seguridad del sistema de votaciones es del 94%, mientras que el faltante alcanza un 6%.

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

El presente capítulo describe las conclusiones y recomendaciones que conlleva el cumplimiento de los objetivos

5.1. CONCLUSIONES

- Para poder comunicar una aplicación descentralizada con la Blockchain se necesita de métodos de invocación remota, entre los más importantes se tiene al método de llamada de procedimiento remoto y la invocación de método remoto. En el desarrollo del sistema de votaciones se usa el método de llamada de procedimiento remoto, ya que se encuentra implementado en la librería Web3.js y usa la codificación de JSON volviéndolo más versátil de implementar y manipular.
- El proceso electoral dentro de la Cooperativa de Ahorro y Crédito Nueva Esperanza tiene como objetivo elegir los representantes de los consejos de administración y de vigilancia, donde participan los socios habilitados por cada agencia que conforma a la Cooperativa. Para ello, la entidad financiera hace uso de los procesos electorales tradicionales, dividiendo el proceso en la etapa de planificación, inscripción de representantes, nombramiento de juntas seccionales y receptoras del voto, etapa de ejecución de las elecciones, y etapa de cierre y consolidación de resultados. Así mismo, se debe planificar la logística, presupuesto y recursos necesarios para realizar las elecciones.
- El desarrollo de la aplicación descentralizada de votaciones usa la metodología de desarrollo RUP para implementar los módulos principales tales como: usuarios, elecciones, votos, candidatos y reportes. La principal ventaja de usar RUP es generar una documentación clara y detallada de cada fase del proceso de desarrollo, lo que facilita la revisión y el seguimiento del proyecto, mientras que la principal desventaja es el alto consumo de tiempo y recursos, especialmente si se requiere una gran cantidad de documentación y seguimiento riguroso.
- Usando el estándar de calidad de la ISO/IEC 25010 para medir la utilización de recursos se determina: el porcentaje de tiempo de procesador (uso del CPU) cumple con los requisitos y posee un grado muy satisfactorio, el uso del gas con un promedio de 18 WEI posee un nivel de puntuación aceptable y un grado de satisfactorio y el uso de memoria RAM posee un promedio de 166,026 MB, lo que significa que se encuentra en el valor cualitativo de muy bueno.

- Usando el estándar de calidad de la ISO/IEC 25010 bajo el enfoque de GQM, para la variable de seguridad se obtiene un nivel de seguridad del 94% considerando las subcaracterísticas de Confidencialidad, Integridad, No-Repudio, Responsabilidad y Autenticidad, por otra parte, la seguridad faltante alcanza un 6%.

5.2. RECOMENDACIONES

- Explorar otras alterativas de Blockchain diferentes a Ethereum para implementar una DAPP, debido a las oportunidades, mejoras y precios que pueden llegar a ofrecer.
- Desarrollar una versión móvil disponible en la tienda de aplicaciones de los smartphones para mejorar la accesibilidad y participación de los socios en el proceso eleccionario.
- Utilizar los servicios que ofrecen los proveedores de la nube para desplegar aplicación en producción, de esta manera solo se paga por los recursos que se están utilizando y se provee una infraestructura confiable para ejecutar la DAPP.
- Se recomienda el uso de los ORM como Sequelize para mejorar la interacción entre el servidor backend y la base de datos tanto en producción y desarrollo, además permite que el backend sea agnóstico de una base de datos.
- Promover la utilización de normas para asegurar la calidad del proceso y del producto de software.

GLOSARIO

Smart Contract: programa informático que hace cumplir y ejecuta acuerdos entre 2 actores, sin intermediarios y lo hace de forma automática

DAPP: Es una aplicación informática que funciona en un sistema de computación distribuido

GAS: Es la unidad de medida utilizada para medir el trabajo Fuente Ethereum para realizar transacciones o cualquier interacción dentro de la red.

EVM: Ethereum Virtual Machine, es una máquina virtual que funciona dentro del ecosistema de Ethereum, permite la ejecución de programas y Smart contracts.

P2P: La red Peer to Peer se conoce en español como red entre par.

ETH: Es la moneda utilizada dentro de la red de Ethereum para pagar por el uso de los recursos de los ordenadores descentralizados.

GWEI: El precio del gas, es una denominación de ETH; cada Gwei equivale a 0,000000001 ETH (10-9 ETH).

WEI: es la denominación más pequeña de ether, la moneda utilizada para facilitar las operaciones transaccionales en la red Blockchain de Ethereum

FRONTEND: la parte de una aplicación que se encarga de la interacción con el usuario y su visualización. Es el aspecto visible y tangible de una aplicación, y es lo que los usuarios interactúan directamente.

BACKEND: es la parte de una aplicación que se encarga de las tareas o funciones que no son visibles directamente para el usuario como el almacenamiento y recuperación de datos, la lógica de negocio, el procesamiento de datos y la comunicación con otros sistemas.

BIBLIOGRAFÍA

AGUILAR, L., 2008. *FUNDAMENTOS DE PROGRAMACIÓN. Algoritmos, estructura de datos y objetos. Cuarta edición.* Cuarta edición. Madrid: McGRAW-HILL/INTERAMERICANA DE ESPAÑA, S. A. U.

AMAZON, 2023. Información general sobre Amazon Web Services Documento técnico de AWS.

ARLOW, J. y NEUSTADT, I., 2005. *UML 2 and the Unified Process: Practical Object-Oriented Analysis and Design*. 2nd. S.l.: s.n.

ARROYO GUARDEÑO, D., DÍAZ VICO, J. y HERNÁNDEZ ENCINAS, L., 2019. *¿Qué sabemos de? Blockchain* [en línea]. S.l.: CSIC Consejo Superior de Investigaciones Científicas. [consulta: 3 junio 2022]. ISBN 9788400104788. Disponible en: https://elibro.net/es/ereader/espoch/111431?page=1.

BANNET, J., PRICE, D., RUDYS, W., SINGER, J. y S., D., 2004. Hack-a-vote: Security issues with electronic voting systems | IEEE Journals & Magazine | IEEE Xplore. *IEEE Security & Privacy* [en línea]. [consulta: 22 mayo 2022]. Disponible en: https://ieeexplore.ieee.org/abstract/document/1264851.

BLOCKCHAIN FEDERAL ARGENTINA, 2019. Protocolos de consenso. [en línea]. [consulta: 4 junio 2022]. Disponible en: https://bfa.ar/blockchain/protocolos-de-consenso.

CAI, W., WANG, Z., ERNST, J.B., HONG, Z., FENG, C. y LEUNG, V.C.M., 2018. Decentralized Applications: The Blockchain-Empowered Software System. *IEEE Access*, vol. 6, ISSN 21693536. DOI 10.1109/ACCESS.2018.2870644.

CALABRESE, J., ESPONDA, S., PASINI, A. y PESADO, P., 2021. CACIC 2020 - Organizado por el Dto. Ingeniería e Investigaciones Tecnológicas UNLaM y la RedUNCI. ,

CALABRESE, J., MUÑOZ, R., PASINI, A., ESPONDA, S., BORACCHIA, M. y PESADO, P., 2017. Asistente para la evaluación de características de calidad de producto de software propuestas por ISO/IEC 25010 basado en métricas definidas usando el enfoque GQM. *XXIII Congreso Argentino de Ciencias de la Computación*,

COULOURIS, G., 2017. *Distributed systems : concepts and design* [en línea]. 5th ed. S.l.: Pearson India, New Delhi, India y 2017. [consulta: 15 octubre 2022]. ISBN 9789332575226. Disponible en: https://www.worldcat.org/es/title/1322929649.

CUENCA, M. y MEZA, D., 2019. El voto electrónico en el ecuador; perspectivas desde crecientes avances tecnológicos. *DSpace de Uniandes* [en línea]. [consulta: 22 mayo 2022]. Disponible en: https://dspace.uniandes.edu.ec/handle/123456789/10022.

DEBUS, J., 2017. Consensus Methods in Blockchain Systems. *Frankfurt School of Finance & Management* [en línea], [consulta: 17 octubre 2022]. Disponible en: www.fs-blockchain.decontact@fs-blockchain.dewww.facebook.de/fsblockchain.

DRESCHER, D., 2017. *A NON-TECHNICAL INTRODUCTION IN 25 STEPS Blockchain Basics: A Non-Technical Introduction in 25 Steps* [en línea]. S.l.: s.n. [consulta: 9 octubre 2022]. ISBN 978-1-4842-2604-9. Disponible en: www.apress.com/9781484226032.

EDIX, 2022. Framework: qué es, para qué sirve y algunos ejemplos. *Edix* [en línea]. [consulta: 18 octubre 2022]. Disponible en: https://www.edix.com/es/instituto/framework/.

ETHEREUM, 2016. web3.js - Ethereum JavaScript API — web3.js 1.0.0 documentation. [en línea]. [consulta: 18 octubre 2022]. Disponible en: https://web3js.readthedocs.io/en/v1.8.0/index.html.

ETHEREUM, 2021. Solidity — Solidity 0.8.17 documentation. [en línea]. [consulta: 17 octubre 2022]. Disponible en: https://docs.soliditylang.org/en/v0.8.17/.

FOLLOW MY VOTE, 2021. About Us - Follow My Vote. [en línea]. [consulta: 22 mayo 2022]. Disponible en: https://followmyvote.com/about-us/.

GARCIA, N., 2019. *Implementación de un sistema de votación electrónica basado en la tecnología Blockchain para las elecciones estudiantiles en la Universidad de Córdoba* [en línea]. S.l.: Universidad de Córdoba. [consulta: 20 mayo 2022]. Disponible en: https://repositorio.unicordoba.edu.co/bitstream/handle/ucordoba/3496/Garc%C3%ADaVilladiegoNeifer.pdf?sequence=1&isAllowed=y.

GÓMEZ, J., ARCOS-MEDINA, G. y PÁSTOR, D., 2020. Application of Genetic Algorithms Technique in the Generation of Academic Schedules. *KnE Engineering* [en línea], vol. 2020, [consulta: 28 enero 2023]. ISSN 2518-6841. DOI 10.18502/KEG.V5I1.5927. Disponible en: https://knepublishing.com/index.php/KnE-Engineering/article/view/5927.

GÓMEZ, M. del C., CERVANTES, J. y GONZÁLEZ PÉREZ, P., 2019. *Fundamentos de Ingeniería de Software* [en línea]. 1. Naucalpan: UNIVERSIDAD AUTONOMA METROPOLITANA. [consulta: 22 octubre 2022]. ISBN 978-607-28-1659-6. Disponible en: http://www.cua.uam.mx/pdfs/conoce/libroselec/Fundamentos_Ing_SW-VF.pdf.

HABER, S. y STORNETTA, W.S., 1991. How to Time-Stamp a Digital Document. *Journal of Cryptology*, no. 2,

HAVERBEKE, M., 2018. *Eloquent JavaScript*. 3era Edición. S.l.: s.n. ISBN 1593279507.

HERNÁNDEZ TREJO, N., 2011. El paradigma de la votación electrónica: el caso del Distrito Federal. *Revista de Administración Pública* [en línea], vol. Volumen XLVI, no. Nº3, [consulta: 9 octubre 2022]. Disponible en: https://www.researchgate.net/publication/333659296_El_paradigma_de_la_votacion_electronica_Revista_de_Administracion_Publica_INAP.

IBÁÑEZ JIMÉNEZ, J., 2018. Blockchain : Primeras cuestiones en el ordenamiento español. *Blockchain : Primeras cuestiones en el ordenamiento español* [en línea], [consulta: 3 junio 2022]. Disponible en: https://books.google.com.co/books?hl=es&lr=&id=S3ZiDwAAQBAJ&oi=fnd&pg=PA11&dq=blockchain+españa+&ots=LhBKpFt-PP&sig=bfsgLrXfr2K6uf2eKrW1P2dB8Qw&redir_esc=y#v=onepage&q=blockchain españa&f=false%0A.

IBM, 2021. Beneficios de blockchain. [en línea]. [consulta: 25 junio 2022]. Disponible en: https://www.ibm.com/mx-es/topics/benefits-of-blockchain.

IEEE STD, 2011a. ISO/IEC 25010 - Eficiencia de desempeño. *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models* [en línea]. [consulta: 23 octubre 2022]. Disponible en: https://iso25000.com/index.php/normas-iso-25000/iso-25010/21-eficiencia-de-desempeno.

IEEE STD, 2011b. ISO/IEC 25010 Seguridad. *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models* [en línea]. [consulta: 23 octubre 2022]. Disponible en: https://iso25000.com/index.php/normas-iso-25000/iso-25010/25-seguridad.

IEEE STD, 2011c. ISO/IEC 25040:2011 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Evaluation process. . marzo 2011.

ISO/TR 23576, 2020. ISO - ISO/TR 23576:2020 - Blockchain and distributed ledger technologies — Security management of digital asset custodians. [en línea]. [consulta: 24 enero 2023]. Disponible en: https://www.iso.org/standard/76072.html.

KAMIL, M., BIST, A.S., RAHARDJA, U., SANTOSO, N.P.L. y **IQBAL, M., 2021.** Covid-19: Implementation e-voting Blockchain Concept. *International Journal of Artificial Intelligence Research*, vol. 5, no. 1, ISSN 2579-7298. DOI 10.29099/IJAIR.V5I1.173.

KARLA, B., CHAMBILLA, B., PARA OPTAR EL, C. y **PROFESIONAL, T**., 2016. UNIVERSIDAD NACIONAL JORGE BASADRE GROHMANN-TACNA Facultad de Ingeniería Presentada por. ,

KASIREDDY, P., 2021. The Architecture of a Web 3.0 application. *The Architecture of a Web 3.0 application* [en línea]. [consulta: 13 octubre 2022]. Disponible en: https://www.preethikasireddy.com/post/the-architecture-of-a-web-3-0-application.

KASPERSKY, 2021. Polys online voting system. [en línea], [consulta: 22 mayo 2022]. Disponible en: https://mwc.kaspersky.com/files/Polys/Polys%20-%20online%20voting%20system%20-%20Whitepaper.pdf.

KRUTCHEN, P., 2003. *The Rational Unified Process – An Introduction (3rd edition)* . 3rd. S.l.: s.n.

LUCAS, J., 2019. Qué es NodeJS y para qué sirve. *OpenWebinars.net* [en línea]. [consulta: 18 octubre 2022]. Disponible en: https://openwebinars.net/blog/que-es-nodejs/.

MALDONADO, J., 2021. Truffle, la mayor herramienta de desarrollo para Ethereum. [en línea]. [consulta: 18 octubre 2022]. Disponible en: https://es.cointelegraph.com/explained/truffle-the-biggest-development-tool-for-ethereum.

MARTÍNEZ, A. y MARTÍNEZ, R., 2000. Guía a Rational Unified Process. [en línea], [consulta: 20 octubre 2022]. Disponible en: https://www.researchgate.net/publication/268005509.

MCCUBBIN, G., 2022. Intro to Web3.js · Ethereum Blockchain Developer Crash Course | Dapp University. [en línea]. [consulta: 18 octubre 2022]. Disponible en: https://www.dappuniversity.com/articles/web3-js-intro.

MDN CONTRIBUTORS, 2022. JavaScript | MDN. [en línea]. [consulta: 17 octubre 2022]. Disponible en: https://developer.mozilla.org/es/docs/Web/JavaScript.

MICROSOFT, 2022. Documentation for Visual Studio Code. [en línea]. [consulta: 4 junio 2022]. Disponible en: https://code.visualstudio.com/docs.

NAKAMOTO, S., 2009. Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario. [en línea], [consulta: 22 mayo 2022]. Disponible en: www.bitcoin.orgTraducidoalEspañoldebitcoin.org/bitcoin.pdfporAngelLeón-www.diariobitcoin.com.

OPENJS FOUNDATION y **NODE.JS**, 2022. Acerca | Node.js. [en línea]. [consulta: 18 octubre 2022]. Disponible en: https://nodejs.org/es/about/.

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN., 2011. Requerimientos y evaluación de sistemas y calidad de software (25010)). ,

POSTGRESQL GLOBAL DEVELOPMENT GROUP, 2022. PostgreSQL 15.1 Documentation The PostgreSQL Global Development Group. *PostgreSQL 15.1 Documentation* [en línea], [consulta: 20 noviembre 2022]. Disponible en: https://www.postgresql.org/.

PRIETO DE LOPE, R.A., 2015. *SGBD e instalación: administración de bases de datos (UF1469)* [en línea]. S.l.: IC Editorial. [consulta: 20 noviembre 2022]. ISBN 9788416433360. Disponible en: https://elibro.net/es/lc/espoch/titulos/44145.

PRINCE, A., JOLÍAS, L. y **LACABANNE, F**., 2012. Voto electrónico en Argentina. White Paper. [en línea]. Disponible en: http://bcn.cl/2ejeq.

QATAWNEH, M., QUZMAR, A. y **AL-MAAITAH, S.,** 2022. BLOCKCHAIN-BASED E-VOTING SYSTEM FOR ELECTIONS IN JORDAN. *Journal of Theoretical and Applied Information Technology* [en línea], vol. 100, no. No5, [consulta: 19 octubre 2022]. ISSN 1992-8645. Disponible en: https://www.researchgate.net/publication/359759254.

REACT, 2022. React - Una biblioteca de JavaScript para construir interfaces de usuario. [en línea]. [consulta: 4 junio 2022]. Disponible en: https://es.reactjs.org/.

REDHAT, 2019. El concepto de IDE. [en línea]. [consulta: 18 octubre 2022]. Disponible en: https://www.redhat.com/es/topics/middleware/what-is-ide.

REMIX, 2022. Remix - Ethereum IDE & community. [en línea]. [consulta: 4 junio 2022]. Disponible en: https://remix-project.org/.

RENIU, J., 2011. Algunas certezas (pocas) sobre la introducción del voto electrónico. *Revista de Administración Pública, INAP* [en línea], vol. Volumen XLVI, no. Nº 3, [consulta: 9 octubre 2022]. Disponible en: https://www.researchgate.net/publication/333659296_El_paradigma_de_la_votacion_electronica_Revista_de_Administracion_Publica_INAP.

RODRIGUEZ, N., 2018. Historia de la tecnología Blockchain: Guía definitiva. *Historia De La Tecnología Blockchain: Guía Definitiva* [en línea]. [consulta: 22 mayo 2022]. Disponible en: https://101blockchains.com/es/historia-de-la-blockchain/.

ROJO, M.I., 2019. *Blockchain, fundamentos de la cadena de bloques.* S.l.: Ediciones de la U. ISBN 9789587920031.

ROOSE, K., 2022. Qué es la web3: lo que debes saber - The New York Times. [en línea]. [consulta: 3 junio 2022]. Disponible en: https://www.nytimes.com/es/interactive/2022/03/29/espanol/web3-que-es.html.

RUMBAUGH, J., JACOBSON, I. y **BOOCH, G.,** 1999. *The Unified Software Development Process*. S.l.: s.n.

SALIMITARI, M. y **CHATTERJEE, M.,** 2018. A Survey on Consensus Protocols in Blockchain for IoT Networks. [en línea], [consulta: 17 octubre 2022]. DOI 10.48550/arxiv.1809.05613. Disponible en: https://arxiv.org/abs/1809.05613v4.

SHANKER, M., 2019. Use Case: Smart Contract for Lease Agreements using Blockchain Technology. *International Journal of Scientific Research in* _____ *Research Paper. Computer Science and Engineering*, vol. 7, no. 6, ISSN 2320-7639. DOI 10.26438/ijsrcse/v7i6.19.

SHARAN, K., 2018. Java Remote Method Invocation. *Java APIs, Extensions and Libraries* [en línea], [consulta: 19 octubre 2022]. DOI 10.1007/978-1-4842-3546-1_6. Disponible en: https://link.springer.com/chapter/10.1007/978-1-4842-3546-1_6.

SMITH, R., 2009. International Experiences of Electronic Voting and Their Implications for New South Wales. [en línea], Disponible en: https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/Reports/iVote%20reports/Internati

onal_Experiences_of_Electronic_Voting_and_Their_Implications_for_New_South_Wales_Report_2009.pdf.

STEINMETZ, R. y **WEHRLE, K.,** 2005. 2. What Is This "Peer-to-Peer"? *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* [en línea], vol. 3485 LNCS, [consulta: 4 junio 2022]. ISSN 16113349. DOI 10.1007/11530657_2. Disponible en: https://link.springer.com/chapter/10.1007/11530657_2.

SWAN, M., 2018. Blockchain for Business: Next-Generation Enterprise Artificial Intelligence Systems. *Advances in Computers*, vol. 111, ISSN 0065-2458. DOI 10.1016/BS.ADCOM.2018.03.013.

UNIVERSIDAD DE ALICANTE, 2003. Sesión 1: Introducción a RMI. *Universidad de Alicante* [en línea]. [consulta: 23 octubre 2022]. Disponible en: http://www.jtech.ua.es/j2ee/2003-2004/modulos/rmi/sesion01-apuntes.htm.

VOATZ, 2017. How It Works - Voatz How Voatz works for voters and administrators. [en línea]. [consulta: 22 mayo 2022]. Disponible en: https://voatz.com/how-it-works/.

WASKOM, M., 2021. 11 librerías para crear visualizaciones de datos. *Journal of Open Source Software*, vol. 6, no. 60, DOI 10.21105/JOSS.03021.

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE

UNIDAD DE PROCESOS TÉCNICOS

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 20/ 06 / 2023

INFORMACIÓN DE LOS AUTORES
Nombres – Apellidos: Ayrton Fidel Avalos Cuadrado – Edwin Stalyn Manzano Quinzo
INFORMACIÓN INSTITUCIONAL
Facultad: Informática y Electrónica
Carrera: Software
Título a optar: Ingeniero en Software
f. Analista de Biblioteca responsable: Ing. Fernanda Arévalo M.