



UNIVERSIDAD TECNOLÓGICA ECOTEC

FACULTAD DE INGENIERÍA

TÍTULO DEL TRABAJO:

TECNOLOGÍA BLOCKCHAIN APLICADA A UNA PLATAFORMA DE
VOTACIÓN ELECTRÓNICA: CASO DE ESTUDIO ECUADOR

LÍNEA DE INVESTIGACIÓN:

TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

MODALIDAD DE TITULACIÓN:

TRABAJO DE INTEGRACIÓN CURRICULAR

CARRERA:

INGENIERÍA EN SOFTWARE

TÍTULO A OBTENER:

INGENIERO EN SOFTWARE

AUTOR(A):

CHRISTIAN ADRIÁN LÓPEZ AGUIRRE

TUTOR(A):

PH.D. DIEGO PEÑA ARCOS

MGTR. LISSENIA ISABEL SORNOZA QUIJIJE

GUAYAQUIL – ECUADOR

2023

DEDICATORIA

Esta tesis está dedicada a:

A mis padres por su apoyo incondicional y cariño además de estar conmigo en todo momento. A mi hermano por sus ánimos y buenos deseos.

Finalmente, deseo expresar mi dedicación a todos mis compañeros, quienes me respaldaron y brindaron su apoyo en los momentos más desafiantes durante la ejecución del proyecto, así como por la comprensión ofrecida a diario.

AGRADECIMIENTO

Expreso mi más sincero agradecimiento a todas las personas que han contribuido de manera directa e indirecta en el desarrollo de esta investigación.

En especial, a mis profesores y asesores, por su invaluable guía, conocimientos compartidos y valiosas sugerencias que han enriquecido este trabajo y me han impulsado a ir más allá de mis límites.

Agradezco también a mis amigos y compañeros de estudio, por sus intercambios de ideas, debates y colaboración que han enriquecido mis perspectivas y enriquecido mi aprendizaje durante todo este tiempo.

Finalmente, mi agradecimiento a la Universidad Ecotec y a todos los docentes que formaron parte de mi proceso universitario y los que han sido parte de este proyecto y han dejado una huella en el camino académico y profesional. Sin su apoyo, este logro no habría sido posible.



ANEXO N° 7.1

**UNIDAD DE INTEGRACIÓN CURRICULAR
CERTIFICADO DE APROBACIÓN DEL TUTOR METODOLÓGICO Y CIENTÍFICO PARA LA
PRESENTACIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR**

Samborondón, 1 de diciembre de 2023

Magíster
Erika Ascencio Jordán
Decana de la Facultad
Ingenierías
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de integración curricular TITULADO: **“Tecnología Blockchain aplicada a una plataforma de votación electrónica: caso de estudio Ecuador”** según su modalidad PROYECTO DE INTEGRACIÓN CURRICULAR; fue revisado, siendo su contenido original en su totalidad, así como el cumplimiento de los requerimientos establecidos en la guía para su elaboración, Por lo que se autoriza al estudiante: **LOPEZ AGUIRRE CHRISTIAN ADRIAN**, para que proceda con la presentación oral del mismo.

ATENTAMENTE,

Firma 1

PhD. Diego Peña Arcos
Tutor(a) metodológico

Firma 2

Mgr. Lissenia Sornosa
Tutor(a) de la ciencia



ANEXO N°7.2

**UNIDAD DE INTEGRACIÓN CURRICULAR
CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS
DEL TRABAJO DE INTEGRACIÓN CURRICULAR**

Habiendo sido revisado el trabajo de integración curricular TITULADO: "Tecnología Blockchain aplicada a una plataforma de votación electrónica: caso de estudio Ecuador" según su modalidad PROYECTO DE INTEGRACIÓN CURRICULAR elaborado por LOPEZ AGUIRRE CHRISTIAN ADRIAN fue remitido al sistema de coincidencias en todo su contenido el mismo que presentó un porcentaje de coincidencias del (2%) mismo que cumple con el valor aceptado para su presentación que es inferior o igual al 10% sobre el total de hojas del Trabajo de integración curricular.

Adicional se adjunta print de pantalla de dicho resultado.

ATENTAMENTE,

Firma 1

PhD. Diego Peña Arcos
Tutor(a) metodológico

Firma 2

Mgtr. Lissenia Sornoza Quijije
Tutor(a) de la ciencia



TIC-2023S02- LOPEZ_AGUIRRE_CHRISTIAN_ADRIAN

2%
Textos
sospechosos



2% Similitudes
< 1% similitudes entre
comillas
< 1% Idioma no reconocido
0% Textos potencialmente
generados por la IA

Nombre del documento: TIC-2023S02-
LOPEZ_AGUIRRE_CHRISTIAN_ADRIAN.pdf
ID del documento: 3d52349e0a03eab1f56c3cd6c21d02a2c388a90
Tamaño del documento original: 5,1 MB

Depositante: DIEGO ANDRES PEÑA ARCOS
Fecha de depósito: 1/12/2023
Tipo de carga: interface
fecha de fin de análisis: 1/12/2023

Número de palabras: 36.253
Número de caracteres: 245.363

Ubicación de las similitudes en el documento:



Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	revistas.upt.edu.pe El impacto del Blockchain en la cadena de suministros de la I... https://revistas.upt.edu.pe/ojs/index.php/ingenieria/article/download/708/702	< 1%		Palabras idénticas: < 1% (153 palabras)
2	repositorio.utn.edu.ec Implementación de un sistema de votación electrónica pa... http://repositorio.utn.edu.ec/bitstream/123456789/12442/6/04_ISC_620_TRABAJO_DE_GRADO.pdf.bt 5 fuentes similares	< 1%		Palabras idénticas: < 1% (84 palabras)
3	Documento de otro usuario #44b272 👤 El documento proviene de otro grupo	< 1%		Palabras idénticas: < 1% (92 palabras)
4	www.euskadi.eus Voto electrónico. Voto electrónico en el mundo - Procesos elect... https://www.euskadi.eus/informacion/voto-electronico-voto-electronico-en-el-mundo/web01-a2hauk... 1 fuente similar	< 1%		Palabras idénticas: < 1% (76 palabras)
5	do.org Frameworks PHP basados en la arquitectura Modelo-Vista-Controlador pa... https://doi.org/10.26423/rctuv1011.703	< 1%		Palabras idénticas: < 1% (31 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	www.informadorpublico.com El voto electrónico en el mundo: De 295 países, sól... https://www.informadorpublico.com/Internacional/el-voto-electronico-en-el-mundo-de-295-paises-s...	< 1%		Palabras idénticas: < 1% (35 palabras)
2	repository.usta.edu.co https://repository.usta.edu.co/bitstream/handle/11634/42768/2022oscarsanabria.pdf?sequence=1	< 1%		Palabras idénticas: < 1% (21 palabras)
3	www.opinioncaribe.com Conozca los términos más utilizados durante el proces... https://www.opinioncaribe.com/2015/10/25/conozca-los-terminos-mas-utilizados-durante-el-proces...	< 1%		Palabras idénticas: < 1% (19 palabras)
4	www.revistas.ug.edu.ec https://www.revistas.ug.edu.ec/index.php/easi/article/download/1771/2600/5213	< 1%		Palabras idénticas: < 1% (13 palabras)
5	1library.co Prueba de Usabilidad Natalie González 84 - Anexo 1: Pruebas de usab... https://1library.co/article/prueba-usabilidad-natalie-gonzalez-anexo-1-pruebas-usabilidad.qm0525q	< 1%		Palabras idénticas: < 1% (15 palabras)

Fuentes mencionadas (sin similitudes detectadas)

Estas fuentes han sido citadas en el documento sin encontrar similitudes.

1	https://www.linkedin.com/pulse/vulnerabilidades-en-los-smart-contracts-dos-de-alfredo-b
2	https://online-tesis.com/tecnicas-de-recoleccion-de-datos-para-realizar-un-trabajo-de-inve
3	http://revistas.ulvr.edu.ec/index.php/yachana/article/view/851
4	https://doi.org/10.1590/1518-8345.1054.2777
5	https://doi.org/10.3390/app10124113

RESUMEN

En la actualidad, se encuentran disponibles varios sistemas de voto electrónico que ofrecen ventajas como ahorro ecológico, eficacia en el escrutinio y accesibilidad para electores en el exterior. Sin embargo, la inclusión de la tecnología en los procesos electorales también ha dado lugar a vulnerabilidades y ataques informáticos, lo que ha creado desconfianza y menor participación en dichos sistemas. Para abordar estas deficiencias, se propone el uso de la tecnología blockchain en conjunto con contratos inteligentes, los cuales, gracias a su estructura descentralizada e inmutable, brindan una solución.

El objetivo general de este trabajo de titulación consistió en desarrollar un sistema web para el voto electrónico basado en blockchain, asegurando la integridad de los datos y la confiabilidad en el proceso electoral. Se enfocó especialmente en el uso de contratos inteligentes para llevar a cabo el sufragio, el escrutinio y la emisión de resultados. Para alcanzar este propósito, se realizó una revisión bibliográfica orientada en el voto electrónico y la tecnología blockchain, explorando sus particularidades, funcionamiento y beneficios. También se abordaron los conceptos de contratos inteligentes y se asemejaron algunas plataformas blockchain que podrían utilizarse para resolver la problemática planteada. Adicionalmente, se obtuvo resultados de las pruebas de vulnerabilidades.

En conclusión, este proceso finalizó en un tiempo considerable, además que en la elaboración del sistema web se muestra que los objetivos planteados fueron cumplidos satisfactoriamente con el fin de brindar resultados favorables.

Palabras clave: voto electrónico, blockchain, contratos inteligentes, plataformas blockchain, proceso electoral.

ABSTRACT

Currently, there are several electronic voting systems available that offer advantages such as ecological savings, efficiency in vote counting, and accessibility for overseas voters. However, the integration of technology into electoral processes has also led to vulnerabilities and cyber-attacks, resulting in mistrust and decreased participation in these systems. To address these deficiencies, the use of blockchain technology in conjunction with smart contracts is proposed, which, due to their decentralized and immutable structure, provide a solution.

The general objective of this thesis was to develop a web-based system for electronic voting based on blockchain, ensuring data integrity and reliability in the electoral process. It focused specifically on the use of smart contracts to facilitate voting, vote counting, and result declaration. To achieve this purpose, a bibliographic review was conducted, focusing on electronic voting and blockchain technology, exploring their characteristics, functionality, and benefits. The concepts of smart contracts were also addressed, and several blockchain platforms that could be used to address the problem were compared. Additionally, vulnerability testing was performed to ensure the security and effectiveness of the system.

In conclusion, this process was completed within a considerable timeframe, and the development of the web-based system demonstrated that the stated objectives were successfully achieved, resulting in favorable outcomes.

Keywords: electronic voting, blockchain, smart contracts, blockchain platforms, electoral process.

ÍNDICE

INTRODUCCIÓN	11
Antecedentes	11
Planteamiento del problema	13
Pregunta científica	15
Objetivos.....	15
Objetivo General.....	15
Objetivos Específicos	15
Justificación.....	16
1. CAPITULO I: MARCO TEÓRICO.....	19
1.1 Marco Teórico Fundamental:.....	19
1.1.1 Introducción a Blockchain.....	19
1.1.2 Funcionamiento Básico de Blockchain.....	20
1.1.3 Blockchain y sus diferentes aplicaciones	25
1.2 Marco Teórico Conceptual.....	30
1.2.1 Tipos de Blockchain.....	30
1.2.2 Topología de red.....	31
1.2.3 Estructura de una cadena de bloques.....	34
1.2.4 Estructura Hash.	35
1.2.5 Elementos fundamentales en una red Blockchain.....	37
1.2.6 Smart contracts.....	42
1.2.7 Características de Blockchain.	46
1.2.8 Ethereum.....	47
1.2.9 Máquina Virtual de Ethereum.	49

1.2.10	Solidity.....	51
1.2.11	El voto electrónico y Blockchain.....	52
1.2.12	Características más relevantes en una votación.	53
1.3	Marco teórico: Situacional.....	54
1.3.1	Método de voto tradicional.....	54
1.3.2	Ventajas y desventajas del método tradicional.	55
1.3.3	Método de Voto Electrónico.....	56
1.4	Marco Teórico Contextual.....	57
1.4.1	Casos de Éxito.	57
1.4.2	Países con sistemas de voto electrónico implantados en el mundo.	58
2.	CAPITULO II: MARCO METODOLÓGICO.....	68
2.1	Metodología de investigación.	68
2.1.1	Enfoque de investigación.....	68
2.1.2	Alcance de la investigación.	69
2.1.3	Tipos de investigación.	71
2.1.4	Fuentes y técnicas para la recolección de información	73
2.2	Metodología por objetivos.	76
2.2.1	Analizar las problemáticas actuales del proceso de votación, incluyendo la logística, el gasto y la transparencia en el sistema electoral.....	76
2.2.2	Identificar los posibles desafíos y riesgos asociados con la automatización de los procesos electorales, como la seguridad de los datos y la protección de la privacidad de los votantes.	78
2.2.3	Definir el prototipo y simulación que pueda mostrar las características principales para llevar a cabo un proceso electoral.....	81
2.2.4	Probar el prototipo con respecto a seguridad y privacidad de los datos	83
2.3	Usabilidad.....	85

2.3.1	Análisis de la usabilidad.	86
2.3.2	Métodos de usabilidad.	86
3.	CAPITULO III: ANÁLISIS E INTERPRETACIÓN DE RESULTADOS.....	94
3.1	Descripción de los resultados.	94
3.1.1	Planificación.....	95
3.1.2	Recolección de datos.....	102
3.2	Análisis de resultados	106
3.2.1	Población.	106
3.2.2	Muestra.	106
3.2.3	Análisis de las respuestas obtenidas.	107
3.3	Resultados esperados.	130
4.	CAPITULO IV: PROPUESTA TECNOLÓGICA	135
4.1	Factibilidad Financiera.	136
4.2	Factibilidad Social.	137
4.2.1	Objetivos del plan de factibilidad Social.....	137
4.3	Factibilidad Técnica.	138
4.3.1	Metodología de desarrollo.	139
5.	CONCLUSIONES	182
6.	RECOMENDACIONES.....	184
7.	Bibliografía	185
8.	ANEXO.....	189
4.4	Anexo 1	190
4.5	Anexo 2	198

Índice de tablas

<i>Tabla 1: Reglas Heurísticas de Nielsen.....</i>	<i>89</i>
<i>Tabla 2: Definición de las preguntas del cuestionario por dimensión.</i>	<i>96</i>
<i>Tabla 3. Tabla comparativa de resultados de entrevistas.....</i>	<i>127</i>
<i>Tabla 4: Heurísticas violadas, problemas de usabilidad y las severidades encontradas en las pantallas del prototipo.....</i>	<i>130</i>
<i>Tabla 5: Requerimientos funcionales</i>	<i>145</i>
<i>Tabla 6: CU-GC-01 Registrar Candidato.....</i>	<i>148</i>
<i>Tabla 7: CU-GC-01 Modificar Candidato.....</i>	<i>149</i>
<i>Tabla 8: CU-GC-03 Eliminar Candidato.....</i>	<i>150</i>
<i>Tabla 9: CU-GC-04 Listar Candidatos.....</i>	<i>151</i>
<i>Tabla 10: CU-GE-01 Registrar Elección.....</i>	<i>153</i>
<i>Tabla 11: CU-GE-02 Iniciar Elección</i>	<i>154</i>
<i>Tabla 12: CU-GE-03 Finalizar Elección</i>	<i>155</i>
<i>Tabla 13: CU-GE-04 Modificar Elección.....</i>	<i>157</i>
<i>Tabla 14: CU-GE-05 Eliminar Elección.....</i>	<i>158</i>
<i>Tabla 15: CU-GE-05 Listar elecciones.....</i>	<i>159</i>
<i>Tabla 16: CU-GV-01 Registrar Votante</i>	<i>160</i>
<i>Tabla 17: Listado de votantes</i>	<i>161</i>
<i>Tabla 18: CU-CR-01 Mostrar Resultados</i>	<i>162</i>
<i>Tabla 19: CU-EV-01 Validar Votante.....</i>	<i>163</i>
<i>Tabla 20: CU-EV-02 Seleccionar Candidato.....</i>	<i>164</i>
<i>Tabla 21: CU-EV-03 Confirmar Voto</i>	<i>165</i>

Índice de Figuras

Figura 1. Estructura de un Blockchain.....	21
Figura 2. Tipos de redes: Centralizada Vs. Descentralizada Vs Distribuida.	33
Figura 3. Estructura de la cadena de bloques.....	34
Figura 4. Cadena Hash.....	36
Figura 5. Funcionamiento de un contrato inteligente.	46
Figura 6. Países con implantación de voto electrónico en el mundo.	58
Figura 7. Arquitectura del sistema. Elaborado por autor.	172
Figura 8. Diagrama Entidad-Relación.	173
Figura 9. Diagrama que representa el funcionamiento del patrón M.V.C.....	175
Figura 10. Pantalla Inicio sesión votante.....	177
Figura 11. Pantalla Inicio Sesión administrador.....	177
Figura 12. Dashboard principal del administrador.	178
Figura 13. Panel de gestión de elecciones.....	178
Figura 14. Panel para agregar candidato.....	179
Figura 15. Listado de votantes.....	179
Figura 16. Gestión de padrones electorales.	180
Figura 17. Pantalla - listado de resultados.....	180
Figura 18. Interfaz de resultados de votaciones.....	181
Figura 19. Prueba de creación de bloque y función hash.....	200
Figura 20. Prueba de un bloque de transacción.....	200
Figura 21. Prueba de carga y estrés.....	201
Figura 22. Resultado de promedio y media de peticiones en modo de carga.....	201

INTRODUCCIÓN

En el marco histórico y social del objeto de estudio, el surgimiento de la tecnología Blockchain está estrechamente ligado al desarrollo de la criptomoneda Bitcoin en el año 2009. La creación de Bitcoin por una entidad desconocida bajo el alias de Satoshi Nakamoto representó un hito que revolucionó la noción de dinero y las transacciones digitales. Blockchain, la tecnología subyacente que posibilita el funcionamiento de Bitcoin y otras criptomonedas, inicialmente se enfocó en asegurar la seguridad y la integridad de las transacciones financieras descentralizadas.

A medida que la tecnología Blockchain demostró su solidez y capacidad para mantener registros seguros e inmutables en el ámbito financiero, su aplicación se amplió hacia otras áreas, como el ámbito de la votación electrónica. Este avance sucedió en un contexto donde había un creciente interés por mejorar los sistemas electorales y aumentar la familiaridad en los procesos democráticos. Los desafíos vinculados a la seguridad, la transparencia y la confiabilidad de los sistemas convencionales de votación han sido temas de disputa e inquietud en diversas naciones, incluyendo Ecuador.

Desde una perspectiva social, la incorporación de la tecnología Blockchain en la plataforma de votación electrónica en Ecuador tiene como propósito abordar desafíos electorales específicos del país. La implementación de sistemas de voto electrónico busca potenciar la accesibilidad y la participación de los ciudadanos, especialmente aquellos que residen en el extranjero. Además, se busca disminuir la posibilidad de fraude y manipulación de resultados, lo que fortalecería la confianza de la población en el proceso electoral.

En el contexto histórico, el surgimiento de la tecnología Blockchain está estrechamente vinculado al desarrollo de la criptomoneda Bitcoin en 2009. La creación de Bitcoin por una entidad desconocida bajo el seudónimo de Satoshi Nakamoto fue un hito que cambió radicalmente la concepción del dinero y las transacciones digitales. Blockchain, la tecnología subyacente que permite el funcionamiento de Bitcoin y otras criptomonedas, tuvo inicialmente como objetivo principal avalar la integridad y seguridad de las transacciones financieras descentralizadas.

A medida que la tecnología Blockchain demostró su solidez y capacidad para mantener registros seguros e inalterables en el ámbito financiero, se comenzó a explorar su aplicación en otras áreas, como, por ejemplo, la votación electrónica. Este proceso de expansión ocurrió en un contexto en el que había un creciente interés por mejorar los sistemas electorales y reforzar la confianza en los procesos democráticos. Los retos concernientes con la seguridad, la transparencia y la confiabilidad de los sistemas convencionales de votación han sido motivo de debate y preocupación en varios países, Ecuador incluido.

En el contexto social, el preámbulo de la tecnología Blockchain en el sistema de votación electrónica a desarrollarse busca corregir problemas electorales particulares que afectan al país. La inscripción de sistemas de votación electrónica tiene como meta optimizar la accesibilidad y la participación de la población, con una orientación especial en los ciudadanos que viven en el extranjero. Asimismo, se procura reducir la posibilidad de fraude y manipulación de resultados, con el resultante y refuerzo de la confianza de la población en el proceso electoral.

Antecedentes

Durante un extenso período en Ecuador, las elecciones para diversas posiciones han seguido un enfoque convencional. A lo largo de muchos años, las personas solo han experimentado un método de votación, y aunque este enfoque tiene sus méritos, también presenta inconvenientes que abren la puerta a la consideración de nuevas alternativas y sistemas electorales que se adhieran a las regulaciones constitucionales y se ajusten a las condiciones actuales.

La automatización de los procedimientos electorales ha sido objeto de análisis y estudio en los últimos tiempos. Conforme al informe emitido en 2019 por la Organización de los Estados Americanos (OEA), titulado "Automatización Electoral: Un panorama de las experiencias en las Américas", se indica que varios países en la región han aplicado sistemas electrónicos de votación con el propósito de mejorar la claridad y eficacia en las votaciones. (Horni, 2021)

Por ejemplo, en el caso de Brasil, durante las elecciones presidenciales de 2018, se empleó el voto electrónico en más del 99% de las urnas, facilitando un recuento rápido y preciso de los sufragios. Por su parte, en Estonia, se ha implementado el voto en línea desde 2005, logrando altos niveles de participación ciudadana y reduciendo significativamente los gastos relacionados con las elecciones. Estos ejemplos ilustran el potencial de la automatización electoral para enriquecer el proceso de votación y consolidar la confianza en el sistema democrático. (Sánchez Herrera, 2021)

Dentro del escenario ecuatoriano, el método de votación actual enfrenta múltiples desafíos que impactan la transparencia y eficiencia del sistema democrático. Demandando una logística y despliegue costosos en términos de

recursos humanos y materiales, este proceso genera un efecto adverso en la ecología. La ausencia de transparencia y vigilancia ha contribuido a la abstención y a la falta de participación ciudadana, creando la posibilidad de posibles manipulaciones y corrupción en las elecciones. La introducción de aplicaciones seguras en los procesos electorales persigue modernizar y simplificar la democracia, pero enfrenta desafíos relacionados con agendas políticas, la confiabilidad de los ciudadanos y la seguridad nacional. La reticencia ante el cambio y la ausencia de seguridad en las aplicaciones pueden ocasionar demoras y restringir la modernización de los procesos electorales. Abordar estos inconvenientes es fundamental para consolidar la claridad, confianza y legitimidad del proceso democrático. (Llamas Covarrubias, Llamas Covarrubias, & Llamas Covarrubias, 2021)

Dentro del entorno actual, surge la relevancia de explorar alternativas y sistemas electorales que se adapten a los retos contemporáneos y se alineen con las disposiciones constitucionales. Se pone de relieve el potencial de automatizar los procedimientos electorales para mejorar la claridad y eficiencia, como se ha observado en experiencias de otros países. Además, se resalta la condición actual de las elecciones en Ecuador, incluyendo problemas vinculados a la logística, costos, insuficiente supervisión y probables manipulaciones.

Es innegable que la tecnología blockchain proporciona seguridad y precisión al compartir y guardar datos de forma instantánea en un registro inmutable, accesible únicamente por usuarios autorizados. Esta característica les brinda la capacidad de examinar cada detalle de la transacción desde su inicio hasta su conclusión, contribuyendo a instilar confianza en esta innovadora tecnología (IBM, 2022).

Planteamiento del problema

El procedimiento actual de votación implica una planificación y movilización significativa de recursos humanos y materiales, lo cual da lugar a un gasto económico considerable. Estos recursos se consumen en grandes cantidades durante un intervalo de tiempo limitado, lo que genera inquietudes sobre el impacto medioambiental. Otro aspecto a considerar es la supervisión insuficiente y la posibilidad de manipulación, lo cual ha generado desconfianza y una participación ciudadana reducida en ciertos casos. Existe la necesidad imperante de asegurar que todos los individuos, incluyendo aquellos con discapacidades, personas en zonas remotas o ciudadanos en el extranjero, tengan acceso equitativo y sencillo al proceso de votación. Una plataforma de votación electrónica podría simplificar la participación de estos grupos, garantizando que sus voces sean tomadas en cuenta durante el proceso electoral.

El proceso convencional de recolección y recuento manual de votos puede ser lento y susceptible a errores. Una plataforma de votación electrónica podría optimizar la eficiencia en el recuento de sufragios, ofreciendo resultados más veloces y exactos, lo cual contribuiría a la certeza y rapidez en la publicación de los resultados electorales. Además, ayudaría a minimizar el peligro de estafa electoral y manipulación de votos, ya que podría implementar sistemas avanzados de seguridad y autenticación que dificulten las prácticas fraudulentas.

Por lo tanto, es fundamental alcanzar una situación ideal mediante la implementación de un sistema de votación moderno y seguro que reduzca los costos económicos y disminuya el impacto ambiental. Además, este sistema debe infundir confianza en la ciudadanía, asegurando la transparencia y la integridad de los resultados electorales, fomentando así una mayor participación ciudadana en el proceso de votación y, en última instancia, su aceptación. A través de esta

investigación, se busca mitigar las amenazas a la seguridad nacional al garantizar salvaguardias contra posibles ataques cibernéticos y asegurando la invulnerabilidad del sistema electoral.

Aunque se aspira a la introducción de aplicaciones seguras en los procesos electorales como un medio para modernizar y agilizar la democracia, hasta ahora se ha notado que esta aspiración enfrenta desafíos derivados de intereses políticos, que pueden incluir manipulación política, resistencia al cambio y corrupción. Estos factores ejercen un impacto negativo en la confianza de los ciudadanos en el proceso electoral y generan dudas en torno a la transparencia y la integridad de los resultados. Además, se ha reconocido la posibilidad de amenazas a la seguridad nacional debido a procesos electorales susceptibles a ataques cibernéticos.

La meta es lograr un sistema de votación electrónica seguro, eficaz y confiable que disminuya los costos y tenga un impacto ambiental menor en comparación con el proceso tradicional. Este sistema debe inspirar confianza en los ciudadanos, aumentar la participación en las elecciones y garantizar la transparencia e integridad de los resultados electorales. También debe prevenir posibles amenazas a los datos que se manejan en todo el proceso, asegurando una sólida protección contra ataques cibernéticos.

Todo el asunto de investigación y desarrollo se llevará a cabo con la creación de un prototipo de plataforma de votación electrónica con énfasis en la seguridad, eficiencia y transparencia. Se aplicarán medidas de autenticación y encriptación para asegurar la invulnerabilidad del sistema y prevenir manipulaciones. Se incentivará la participación ciudadana en el proceso de desarrollo y se llevarán a cabo pruebas piloto y de estrés controladas para evaluar la efectividad del prototipo. Además, se diseñará una interfaz accesible y amigable para todos los ciudadanos. Se establecerán sistemas de supervisión y auditoría para avalar la transparencia y la rectitud de los resultados electorales. La plataforma abordará la necesidad de acceso universal al voto, permitiendo la participación de personas con discapacidades y personas en áreas remotas o en el extranjero. Además, se

trabajaré en la reducción del riesgo de fraudes y manipulaciones a través de protocolos de seguridad y la adopción de estándares reconocidos en el desarrollo de proyectos. En conjunto, el prototipo aspira a modernizar y acelerar el proceso democrático, fortaleciendo la confianza de los ciudadanos en el sistema electoral.

Ubicando bajo perspectiva de lo mencionado, el prototipo de votación electrónica emerge como una oportunidad para modernizar y acelerar la democracia, fortalecer la confianza de la ciudadanía en el sistema electoral y fomentar la transparencia en los procedimientos electorales a nivel nacional. La adopción de esta plataforma representa un paso significativo hacia una sociedad más participativa, inclusiva y confiable en el ejercicio de su derecho al voto.

Pregunta científica

¿Cuál es el nivel de seguridad de la tecnología Blockchain aplicada a una plataforma de votación electrónica?

Objetivos

Objetivo General

Evaluar la seguridad de la tecnología Blockchain implementada en una plataforma de votación electrónica para determinar la viabilidad, eficiencia e integridad de los datos garantizando la transparencia de los votos.

Objetivos Específicos

- Analizar las problemáticas actuales del proceso de votación, incluyendo la logística, el gasto y la transparencia en el sistema electoral.
- Identificar los posibles desafíos y riesgos asociados con la automatización de los procesos electorales, como la seguridad de los datos y la protección de la privacidad de los votantes.
- Definir el prototipo y simulación que pueda mostrar las características principales para llevar a cabo un proceso electoral.
- Probar el prototipo con respecto a seguridad y privacidad de los datos

Justificación

La responsabilidad del Consejo Nacional Electoral en la organización y supervisión de procesos electorales es crucial para asegurar la transparencia y confiabilidad de los resultados. En este sentido, es esencial explorar si la integración de la automatización en sus procedimientos puede ser una solución eficaz para abordar las deficiencias relacionadas con los métodos convencionales de votación.

El procedimiento actual de votación conlleva un gasto económico elevado debido a la planificación y movilización de recursos humanos y materiales. Estos materiales se consumen en grandes cantidades durante un lapso breve, lo que suscita inquietudes sobre el impacto en el medio ambiente. Además, la insuficiente supervisión y la posibilidad de manipulación han ocasionado la desconfianza y una reducida participación ciudadana en ciertos casos.

Un factor de gran importancia radica en que los sistemas de votación tradicionales enfrentan desafíos como el fraude, errores de conteo y la ausencia de supervisión adecuada. Estos desafíos han generado dudas y inexactitud de confianza en los resultados electorales en otras circunstancias. Esto resulta en la desconfianza por parte de los ciudadanos y en una menguada participación en años recientes, incluso llevando a una considerable parte de la población a abstenerse. La transparencia implica que los resultados electorales reflejen de forma precisa y justa la voluntad de los votantes, y que los procesos involucrados en el proceso electoral sean accesibles y comprensibles para todas las partes involucradas.

Dentro del proceso electoral en vigor, la transparencia es esencial para garantizar que no se produzcan manipulaciones o irregularidades que puedan distorsionar los resultados.

Los ciudadanos necesitan tener la certeza de que su voto será contabilizado correctamente y que los resultados finales serán precisos y reflejarán su elección. Un efecto fundamental del proceso electoral actual es la desconfianza que puede surgir entre los ciudadanos. Factores como la supervisión insuficiente, la posibilidad

de manipulación y los casos de corrupción pueden mermar la confianza de los votantes en la integridad de los resultados electorales. Los intereses políticos y la corrupción también desempeñan un papel importante que impacta en el proceso electoral en curso. La manipulación de los resultados electorales con fines políticos o la interferencia indebida en el proceso pueden socavar la integridad y la transparencia del mismo.

La adopción de elecciones mediante esta tecnología presenta ventajas notables, destacando entre ellas la economía y la sostenibilidad ambiental al reducir el consumo de papel y materiales necesarios para llevar a cabo las votaciones. Además, se logra reducir la corrupción en el proceso electoral, lo que representa el beneficio más significativo en esta coyuntura. Estos sistemas de votación basados en redes blockchain se caracterizan por su transparencia total y la capacidad de contar los votos prácticamente al instante. Por medio de un sistema de votación digital respaldado por una cadena de bloques, que debería ser privada para asegurar la supervisión de los resultados, se establece una plataforma que brinda a los votantes la seguridad de unas elecciones justas y transparentes. Indudablemente, "La transparencia es un pilar fundamental en la tecnología Blockchain, ya que está intrínsecamente incorporada en su naturaleza" (Rivero, 2018). Por esta razón, la utilización de sistemas y redes fundamentados en esta poderosa tecnología comienza a vislumbrarse como una opción genuina y sólida para superar las vulnerabilidades presentes en los sistemas actuales.

MARCO TEÓRICO
CAPITULO I

CAPITULO I: MARCO TEÓRICO

1.1 Marco Teórico Fundamental:

1.1.1 Introducción a Blockchain.

El blockchain es una tecnología de registro distribuido en la cual se guarda la secuencia de transacciones en una cadena de bloques, y cada nodo en el sistema cuenta con una copia completa de esta cadena. Cada bloque en la cadena contiene transacciones que han sido validadas y verificadas por los nodos de la red blockchain. Para llevar a cabo una nueva transacción, el usuario necesita una cartera digital, además de su dirección pública y la dirección del receptor. Todos los bloques están enlazados entre sí mediante el cálculo de su hash, lo que garantiza que no haya modificaciones posibles, asegurando la inmutabilidad y la imposibilidad de manipular la información.

La característica fundamental del blockchain es su descentralización. En lugar de depender de una entidad central, como un banco o una institución gubernamental, el blockchain opera en una red descentralizada de nodos. Cada nodo tiene una copia completa de la cadena de bloques y participa en la validación y verificación de las transacciones.

No se trata solo de descentralizar la información, se trata de poseerla. Cada concentrador de conexión puede almacenar casi una instancia del sistema Blockchain, que se fortalece permanentemente para que todos los concentradores sean consistentes (Muruganandam & Natarajan, 2022). En el propio término Blockchain se puede encontrar la descripción de cómo funciona esta tecnología: los datos se almacenan en bloques diferentes, que luego se conectan para formar una cadena de datos controlados, por tanto, es posible describir tres pasos principales para su funcionamiento: Primero, el cambio de información entre los participantes de Blockchain, lo que facilita el cifrado; en segundo lugar, después de que estas transacciones hayan sido verificadas por la red Blockchain, se combinan en un bloque de datos bloqueados; y finalmente,

estos bloques están vinculados a los anteriores con una clave hash, creando así una cadena de bloques (Demestichas, Nikolaos, Alexakis, & Evgenia, 2020)

1.1.2 Funcionamiento Básico de Blockchain.

El ejercicio de voto constituye una herramienta de gran relevancia en la toma de decisiones en diversas naciones, empresas y organizaciones, especialmente en situaciones que involucran información delicada o elecciones que podrían tener un impacto significativo en el rumbo de un país. En la actualidad, es común observar que estas entidades que dirigen y coordinan procesos electorales emplean principalmente dos enfoques para llevar a cabo sus procedimientos de votación.

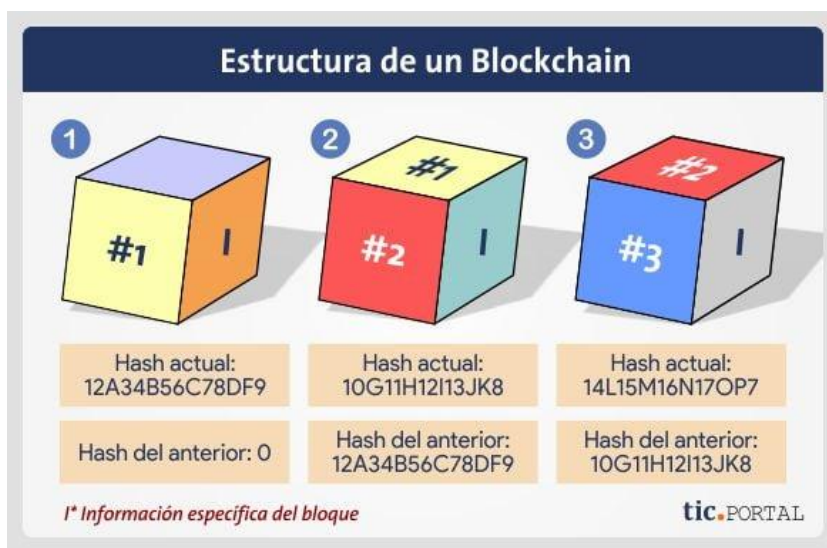
Estos métodos son: la utilización de software diseñado para facilitar la planificación y ejecución de votaciones, o la adhesión a medios más convencionales como el voto físico en papel. Aunque el voto en papel contribuye a la capacidad de auditoría de las elecciones, presenta vulnerabilidades en lo que respecta a seguridad y planificación. Además, circunstancias como la propagación global del Covid-19 y las restricciones de movimiento que trajo consigo han generado cambios en las metodologías de votación en muchas empresas y organizaciones. En este contexto, el voto en papel ya no es tan efectivo y, en muchos casos, se ha vuelto inviable. Por lo tanto, el voto electrónico emerge como una opción viable para estas circunstancias.

El término "voto electrónico" hace referencia al empleo de dispositivos electrónicos en el transcurso de un proceso de elección. Para que un sistema de votación sea catalogado como voto electrónico, es esencial que al menos la introducción de los votos esté digitalizada.

El sistema de votación electrónica (voto electrónico) diseñado para abordar la problemática expuesta en la sección de definición de problema de este documento se basa en una arquitectura respaldada por la tecnología Blockchain. Esta tecnología se sustenta en una red de nodos entre pares (P2P), donde un nodo puede cumplir el rol de cliente y servidor simultáneamente, compartiendo una estructura de datos sin requerir una autoridad centralizada.

Esta estructura de datos recibe el nombre de "libro mayor" o "ledger" en inglés, y se compone de bloques que almacenan información sobre transacciones o intercambios de bienes en la red. Cada bloque posee su propio hash, que es un código generado a partir de los contenidos del bloque, y además guarda el hash del bloque precedente.

Figura 1. Estructura de un Blockchain



Nota. Información del contenido de la estructura de un bloque

El gráfico previamente presentado ofrece una visión panorámica de la estructura y los términos esenciales que conforman la cadena de bloques.

Esta característica confiere a la Blockchain su cualidad de inmutabilidad, ya que alterar todos los bloques almacenados en la mayoría de los nodos de la red sería una tarea ardua. La Figura 1 ilustra cómo se enlazan las transacciones presentes en los bloques de la Blockchain, proporcionando un ejemplo visual de este proceso.

En los siguientes apartados, se abordará de manera específica el funcionamiento de la cadena de bloques, focalizándose en los elementos más destacados que conforman un bloque. Con el auxilio de la Figura 1, se busca fortalecer la explicación y simplificar la comprensión.

La tecnología Blockchain es reconocida como una base de datos que registra valores y transacciones. Sin embargo, su propósito sobrepasa la noción de ser meramente una vasta base de datos, ya que constituye una base de datos distribuida que habilita la transferencia segura de información.

La innegable fortaleza de la Blockchain se radica en su capacidad para resistir vulnerabilidades ante ataques cibernéticos, prescindiendo de la dependencia de un antivirus robusto o un cortafuegos sólido. "Blockchain se autodefende gracias a su propia estructura o arquitectura, que, como su nombre sugiere, se presenta como una cadena de bloques, y cada bloque puede contener varios tipos de información" (Porxas & Cornejo, 2018). Por lo tanto, los bloques se componen de tres elementos primordiales e ineludibles:

La estructura de un bloque puede desglosarse en tres componentes esenciales. En primer lugar, nos encontramos con la "información", que abarca los pormenores relacionados con la transacción, como el remitente, el receptor, la cantidad involucrada, entre otros, tal como se observa en el contexto de Bitcoin. Seguidamente, se halla el "Hash", que constituye un número único e irrepetible que actúa a modo de identificación del bloque. Cada bloque ostenta su propio hash, el cual es generado a partir de la información particular del bloque. En consecuencia, cualquier modificación en la información del bloque daría lugar a una alteración en el hash, invalidando de este modo la cadena.

Una de las causas subyacentes que confieren a la Blockchain su resiliencia frente a ataques informáticos deriva de la inalterabilidad del hash. Si un usuario intenta alterar la información en su copia de la base de datos, la comunidad de la red detectaría esta acción, y su versión de la base de datos quedaría invalidada. En otras palabras, la salvaguarda y autenticación de los documentos en Blockchain provienen de los propios usuarios, no de intermediarios.

Adicionalmente, en la red Blockchain, numerosos nodos vigilan en permanencia el comportamiento de la red. Cada usuario dispone de una copia íntegra e idéntica de la red, y las transacciones están acotadas en términos de fechas, horarios, participantes y volúmenes. Los usuarios gestionan la red y existen dos razones primordiales por las cuales se suman a ella: algunos la emplean para

acceder a los servicios de la red, mientras que otros, denominados "mineros", asumen la responsabilidad de crear nuevos bloques. Conforme se llevan a cabo contratos o transferencias, la información se acumula en nuevos bloques (Porxas & Cornejo, 2018).

Una vez asimilados los componentes de un bloque, se torna posible comprender por qué la cadena de bloques es inmodificable y resiliente a intrusiones. Uno de los argumentos principales radica en el hash, tal como fue mencionado previamente. Este número es exclusivo e inmutable, dado que su generación depende de la información particular del bloque. Si se alterara el contenido o la información del bloque, ello resultaría en un cambio en el hash. En consecuencia, el bloque experimentaría una transformación y, en consecuencia, ya no encajaría en la cadena, invalidando la estructura en su totalidad (Porxas & Cornejo, 2018).

Otra razón se origina en la operativa de la red, ya que múltiples nodos observan constantemente su comportamiento. Cada usuario de la Blockchain ostenta una copia completa e idéntica de la red, que contiene información detallada acerca de fechas, horarios, participantes y volúmenes de transacciones. Gracias a esta supervisión constante, si un usuario intenta modificar la información de su copia, la comunidad de la red lo detectaría, y su versión de la base de datos resultaría anulada, quedando sin efecto. Esta característica es esencial, ya que la seguridad y la autenticación de los documentos en Blockchain son proporcionadas de manera directa por los usuarios mismos, sin intervención de intermediarios (Porxas & Cornejo, 2018).

A medida que se suscriben contratos o se efectúan transferencias en la red, surge la necesidad de almacenar dicha información en un nuevo bloque. Para añadir un bloque adicional, es necesario resolver un problema matemático de considerable complejidad. Para lograrlo, se requiere una capacidad de cómputo substancial, momento en el cual entran en juego los llamados "mineros", que aprovechan al máximo su poder de procesamiento en un intento de resolver el enigma. Una vez que un minero presume haber hallado la solución, el resto de la comunidad verifica su exactitud. Si se valida, el nuevo bloque se agrega a la cadena, consolidando la información y ejecutando la transacción. En recompensa por hallar la solución, el

minero recibe un pago, que en el caso de Bitcoin equivale a 12.5 bitcoins, y cada bitcoin posee un valor aproximado de 10,500 dólares.

Blockchain representa una tecnología de tipo P2P (Peer to Peer), lo que implica que las transacciones se llevan a cabo exclusivamente entre dos puntos, aunque resultan visibles para toda la red, y cada miembro posee una copia de tales transacciones. Esto excluye la necesidad de terceros y, por ende, reduce cualquier riesgo de alteración o intromisión en la red, garantizando una protección contra ataques informáticos. Para vulnerar o penetrar la red, sería necesario tener control sobre todos los registros existentes, lo cual implicaría alterar o modificar más del 70% de la red de forma simultánea, una tarea prácticamente irrealizable. Por lo tanto, cualquier intento de alterar aspectos en la red no pasa inadvertido para los nodos o los participantes, confiriéndole a la tecnología un nivel elevado de seguridad (Limanorum, 2018).

1.1.3 Blockchain y sus diferentes aplicaciones

El empleo de la tecnología blockchain está presenciando una amplia variedad de aplicaciones a nivel mundial, incluyendo en el contexto ecuatoriano, donde su implementación ha estado en gran medida enfocada en el ámbito de las criptomonedas. Estas criptomonedas, siendo activos digitales descentralizados, fundamentan su funcionamiento en la tecnología blockchain.

De acuerdo con un informe emitido por García en el año 2018, un conjunto de asesores de criptomonedas, conocidos como "criptoasesores", estableció los primeros cajeros automáticos de criptomonedas en Ecuador el 8 de febrero del mismo año. Estos dispositivos fueron concebidos para simplificar el proceso de compra y venta de criptomonedas, buscando formalizar y legitimar estas operaciones en el país. La introducción de cajeros automáticos representa un paso hacia la posibilidad de que un mayor número de individuos pueda acceder a dichos servicios de manera segura y conveniente.

El funcionamiento de estos cajeros automáticos se centra inicialmente en las criptomonedas Bitcoin, Dash y Pura. Se eligieron específicamente Dash y Pura debido a los costos de transacción relativamente bajos asociados con ellas, lo cual facilita el acceso a este servicio para un rango más amplio de personas.

No se debe pasar por alto que la utilidad de la tecnología blockchain no se limita únicamente al ámbito de las criptomonedas y sus correspondientes transacciones. Dicha tecnología está siendo explorada en diferentes sectores, tales como logística, finanzas, cadena de suministro, salud, y muchas otras áreas, debido a su capacidad inherente para aportar mayor seguridad, transparencia y capacidad de seguimiento en las operaciones.

La incorporación de cajeros automáticos de criptomonedas en Ecuador tiene un impacto de gran relevancia en la sociedad, ya que contribuye al fortalecimiento de la confianza entre los ciudadanos. En años recientes, ha existido una percepción equivocada que vincula las criptomonedas con esquemas piramidales y actividades

fraudulentas, lo que ha generado reticencia en muchas personas a involucrarse con este tipo de activos digitales.

La introducción de estos cajeros aspira a cambiar esta percepción negativa al establecer una plataforma más formal y legalizada para la compra y venta de criptomonedas en el país. Al ofrecer la capacidad de convertir dinero digital en físico, los interesados consiguen acceder a un servicio de mayor seguridad y confiabilidad.

Este enfoque no solo ayuda a desmitificar las criptomonedas, sino también a fomentar una mejor educación financiera y tecnológica en la sociedad ecuatoriana. A medida que los ciudadanos experimentan directamente el uso de estas tecnologías, estarán en mejor posición para comprender sus beneficios y aplicaciones legítimas. Es esencial resaltar que la adopción de cajeros automáticos de criptomonedas busca promover un entorno de mayor transparencia y legitimidad en el uso de estos activos digitales en Ecuador. De esta forma, se contribuye a salvaguardar a los ciudadanos de posibles engaños y a fortalecer el desarrollo de un ecosistema confiable en el país.

Este novedoso servicio de cajeros automáticos de criptomonedas brinda a los usuarios la capacidad de llevar a cabo transacciones con tres tipos distintos de criptomonedas. Para utilizar este servicio, el usuario requerirá la dirección o el código QR de su billetera digital donde desee recibir los tokens. En caso de no disponer de esta información, el cajero proporcionará una solución al imprimir una cartera de papel con una dirección y clave privada, permitiendo el acceso a las criptomonedas al escanear una serie de códigos QR.

Además, el cajero ofrece la opción de realizar ventas de criptomonedas. Para ello, el usuario puede emplear un dispositivo inteligente para ingresar la dirección de envío proporcionada por el cajero, con el objetivo de recibir el pago correspondiente por los tokens que se están vendiendo. Una vez realizada la transacción, el cajero verifica la operación y emite un comprobante, entregando el equivalente en efectivo.

Este servicio no solo ha sido implementado en la capital de Ecuador, sino que también ha sido adoptado por la multinacional DHL con el propósito de reforzar

la seguridad en la gestión de la información. La tecnología blockchain está siendo aplicada en ámbitos fundamentales como:

- Logística a nivel global.
- Trazabilidad y transparencia en la cadena de suministro.
- Procesos comerciales en logística.

A nivel mundial, el uso de la tecnología blockchain está ganando terreno y se está aplicando de diversas formas tanto en el ámbito privado como en el público. Un ejemplo destacado es la empresa Storj, que aprovecha esta tecnología para ofrecer una alternativa de almacenamiento de datos en una red peer-to-peer (P2P). En este esquema, los datos son distribuidos y guardados en múltiples miembros de la red, aumentando considerablemente la seguridad y evitando la centralización de la información en un solo dispositivo de almacenamiento. De esta manera, se domina el riesgo de exposición de datos en caso de vulnerabilidad en un único punto.

Igualmente, grandes corporaciones como British Airways, Apple y Maersk están entrando en el mundo de la adopción de la tecnología blockchain para la administración de identidades. Por ende, esto va a dar el paso a que los individuos puedan crear identidades digitales personales que sean resistentes a manipulaciones y usurpaciones. Estas modernas identidades digitales podrían eventualmente reemplazar los convencionales nombres de usuario y contraseñas usados en línea, fortaleciendo así la seguridad en la autenticación de usuarios y la firma de documentos digitales.

La implementación de la tecnología blockchain en estos contextos ilustra su flexibilidad y su capacidad para potenciar la seguridad y eficiencia en diferentes campos. Además, es evidente un claro interés por parte de las empresas en explorar las oportunidades que esta tecnología ofrece para transformar procesos y aumentar la confianza en la gestión de datos e identidades. Es crucial destacar que la aplicación de blockchain en estos escenarios específicos puede tener un impacto relevante en la protección y control de información en la era digital.

La característica de almacenamiento inmutable en la tecnología blockchain ha permitido su uso para preservar otros tipos de datos además de las transacciones de Bitcoin. Esto conduce a un registro distribuido imborrable que es significativamente más seguro que las bases de datos convencionales, ya que no necesita intermediarios para su gestión.

En el ámbito militar, se han experimentado diversas aplicaciones de la blockchain. La Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) está desarrollando una plataforma de mensajería segura denominada "Plataforma de Mensajería Segura". El objetivo de este proyecto es establecer una interfaz que permita la transferencia de mensajes a través de un protocolo seguro y descentralizado en varios canales.

Por otro lado, la Agencia de Información y Comunicaciones de la OTAM está considerando propuestas para llevar a cabo proyectos relacionados con el desbloqueo automático de armas o vehículos militares mediante la implementación de la tecnología blockchain.

Estas aplicaciones militares resaltan cómo la tecnología blockchain se aprovecha para reforzar la seguridad, trazabilidad y descentralización en entornos críticos como el sector militar. Al asegurar la inalterabilidad de la información y eliminar la necesidad de una entidad centralizada, se garantiza mayor protección y confiabilidad en las operaciones y comunicaciones militares.

El Blockchain es conocido por sus características principales, según la información provista por (Limanorum, 2018), que serán examinadas y definidas a continuación:

- **Cifrado:** La función principal del cifrado es garantizar que solo el remitente y el receptor de una transacción tengan acceso al contenido completo de esta. La criptografía asegura la privacidad de los datos involucrados en cada transacción.
- **Secuencia de operaciones en bloques:** Todas las transacciones de la red se agrupan y almacenan en bloques que, a su vez, se organizan de manera

cronológica. Esta serie de bloques forma un historial justo y demostrable de todas las operaciones realizadas en la red.

- **Inmutabilidad:** La seguridad de la tecnología Blockchain es sumamente alta debido a que la información registrada en los bloques no puede ser eliminada ni alterada. La distribución y estructura en cadena de los bloques aseguran que cualquier intento de modificación sea rápidamente detectado y rechazado por la red.
- **Confianza:** La red Blockchain opera mediante un protocolo de consenso que asegura la inclusión de información confiable sin necesidad de establecer confianza directa entre los nodos. Cada transacción debe cumplir con los estándares de la red para ser validada, lo que garantiza que únicamente información precisa y correcta sea registrada.
- **Transparencia:** La transparencia es una característica esencial de Blockchain. Los usuarios pueden acceder y verificar en cualquier momento los registros generados por las transacciones en la red. Esto brinda una visión completa de todas las operaciones efectuadas, contribuyendo a la confiabilidad e integridad del sistema.

1.2 Marco Teórico Conceptual

1.2.1 Tipos de Blockchain.

Se conocen que existen 3 tipos de Blockchain:

1.2.1.1 Blockchain pública

Desde una perspectiva fundamental, la accesibilidad es una característica distintiva de la tecnología Blockchain, ya que está al alcance de cualquier individuo sin imponer restricciones. Solamente se necesita una computadora con la capacidad adecuada y acceso a internet para acceder a ella. Resulta relevante resaltar que, en este tipo de plataforma blockchain, los usuarios interactúan de manera confidencial, lo que implica que sus identidades tienen la posibilidad de permanecer ocultas durante las transacciones y las actividades llevadas a cabo en la red. Este aspecto de privacidad agrega un nivel extra de salvaguardia y protección para los participantes. (Muñoz, 2023)

1.2.1.2 Blockchain Privada

En esta clasificación se puede decir que la Blockchain de tipo Privada se distingue de la pública en el sentido de que su acceso es restringido y se necesita permiso o aprobación de la red para ingresar. En esta variante de tecnología, una sola entidad es responsable del mantenimiento y operación, y los registros no se hacen públicos. La Blockchain Privada resulta especialmente adecuada cuando se busca un mayor control y confidencialidad en las transacciones, ya que solo se permite el ingreso a usuarios con autorización. Por contraste, la Blockchain Pública es más inclusiva y democrática, permitiendo la participación y contribución de cualquier individuo. (Muñoz, 2023)

1.2.1.3 Blockchains Federadas

En lo referente a Blockchains Federadas estas constituyen una fusión de las características presentes en las Blockchains Privadas y Públicas. En este tipo de cadena de bloques, el acceso es controlado y limitado por una sola entidad, mientras que los registros y las transacciones se mantienen descentralizados, asegurando así la integridad de la información. Esta entidad también tiene la responsabilidad de aprobar los contenidos que serán visibles en la red.

Bajo lo observado, las Blockchains Federadas amalgaman aspectos de control y descentralización, lo que las convierte en una elección adecuada para situaciones que requieren un nivel específico de limitación de acceso y aprobación, al mismo tiempo que buscan mantener la transparencia y la confiabilidad que brinda la descentralización de los registros. (Muñoz, 2023).

1.2.2 Topología de red.

La tecnología del Blockchain proporciona la capacidad de revolucionar los sistemas actuales al permitir el mantenimiento de bases de datos de manera descentralizada y distribuida por medio de un protocolo informático de código abierto. Esto implica que ya no es imprescindible depender únicamente de una "autoridad central" o entidad que posea y certifique la exactitud de la información, así como que actúe como intermediaria en las transacciones. En lugar de eso, el Blockchain crea una red de nodos que colaboran en la validación y registro de transacciones de forma segura y transparente, eliminando la necesidad de una entidad central para verificar la información. Esto despliega nuevas oportunidades para un sistema más confiable, transparente y descentralizado en varios sectores, incluyendo las finanzas, la logística, la salud y otros más.

La tecnología del Blockchain, conocida como Tecnología de Registro Distribuido (DLT, por sus siglas en inglés), permite establecer redes para compartir registros de transacciones electrónicas, análogos a los libros de contabilidad o bases de datos digitales compartidas. Lo que la hace única es que estos registros se encuentran distribuidos entre los participantes de la red, quienes son

responsables de su mantenimiento. En estas redes, cada nodo o usuario (computadora) tiene una copia original del registro, lo que les permite determinar si las operaciones planteadas por otros usuarios de la red pueden o no llevarse a cabo.

Asimismo, la tecnología Blockchain, también conocida como Tecnología de Red o Registro Distribuido, permite la creación de redes para compartir registros de transacciones electrónicas, de manera semejante a los libros de contabilidad o bases de datos digitales compartidas. La particularidad radica en que estos registros se distribuyen entre los participantes de la red, quienes asumen la responsabilidad de mantenerlos. Cada nodo o usuario de la red posee una copia original del registro, lo que les otorga la capacidad de verificar si las operaciones propuestas por otros usuarios pueden ser realizadas o no. Esta distribución descentralizada y simultánea certifica la transparencia y la confiabilidad en la red, dado que cada participante tiene la capacidad de validar las transacciones y confirmar su autenticidad. La tecnología Blockchain ofrece una ruta segura y exploratoria para el registro y validación de transacciones en múltiples sectores, y su impacto potencial es ampliamente reconocido en la industria.

Ciertamente, dentro de una estructura basada en la tecnología blockchain, cada una de las transacciones es validada y aprobada por los nodos activos en la red. Cada nodo tiene la capacidad de inspeccionar y ratificar las transacciones al contrastarlas con la copia individual que posee del registro compartido y descentralizado.

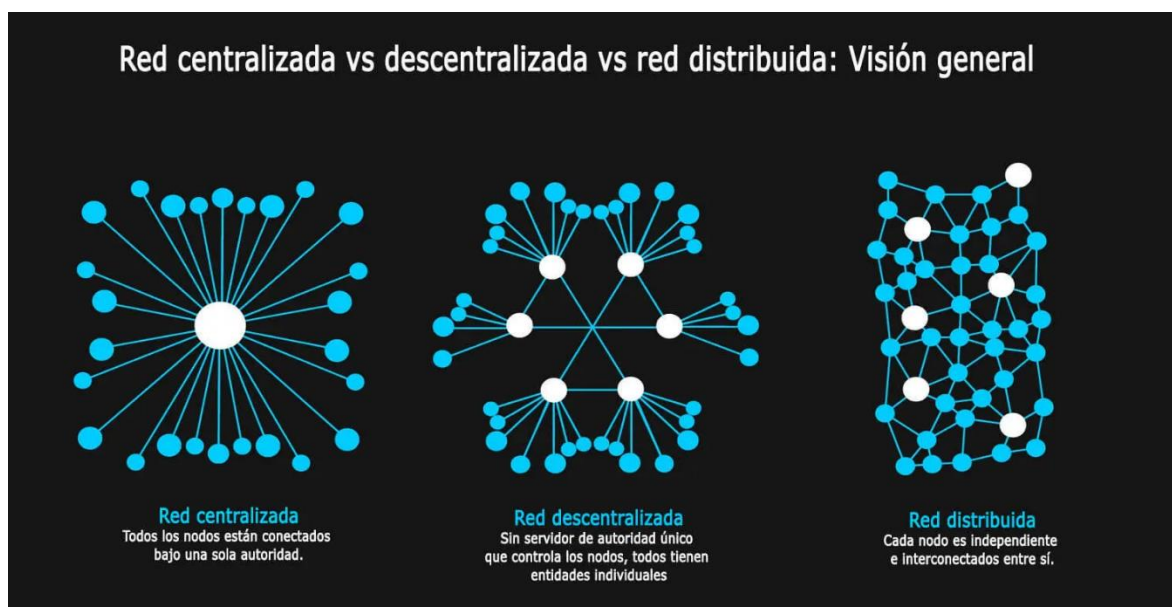
El proceso de consenso se lleva a cabo durante el procedimiento de validación. En términos sencillos, cuando la mayoría de los nodos están de acuerdo con una actualización del registro, como la inclusión de nuevas transacciones, dicha modificación se implementa automáticamente. Esto se ejecuta sin necesidad de intervención de una entidad central o de certificación de datos, tal como señaló Defelipe Díaz en 2018.

En la Figura 2, se exhibe la configuración de una red de naturaleza centralizada, que actualmente predomina en la mayoría de las redes en uso. En

contraparte, la tecnología blockchain se fundamenta en una estructura descentralizada, que define su funcionamiento. Esta topología descentralizada es la que se utilizará para diseñar la red a nivel nacional.

En el esquema de una red centralizada, existe un punto central de mando que supervisa y autoriza todas las operaciones y transacciones en la red. En este contexto, las decisiones y el acceso a la información son centralizados en una entidad única o autoridad.

Figura 2. Tipos de redes: Centralizada Vs. Descentralizada Vs Distribuida.



Nota: (Rodríguez, 2018) *La Mejor Guia Sobre La Tecnología Blockchain: Una Revolución Para Cambiar El Mundo*. Obtenido de 101blockchains:
<https://101blockchains.com/es/tecnologia-blockchain/>

1.2.3 Estructura de una cadena de bloques

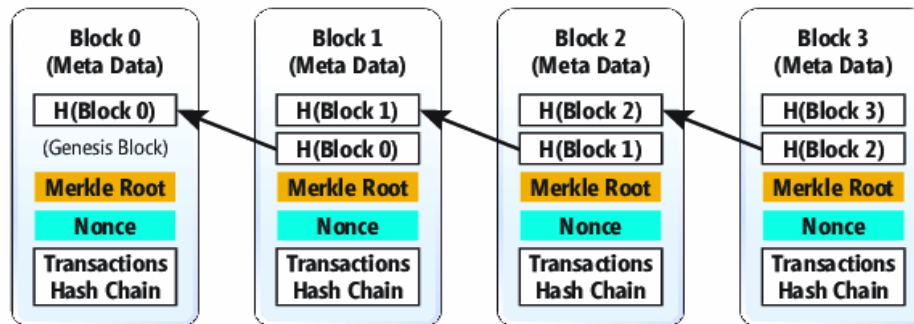
El término "cadena de bloques" fue inicialmente propuesto e introducido en 2008 a través de la implementación de Bitcoin, una criptomoneda pionera (Nakamoto, 2008). Esta innovadora tecnología ha atraído un creciente interés en los últimos años, abarcando diversos campos, incluido el ámbito académico. Aunque la criptomoneda es la aplicación de la cadena de bloques más reconocida, esta tecnología ha encontrado un lugar en una variedad de aplicaciones e industrias más allá del ámbito de las criptomonedas (Tinoco Plasencia, Juárez Trinidad, Gonzales Rosas, & Tamayo Franco, 2023)

Dentro del marco de la tecnología de cadena de bloques, los bloques de información se conectan mediante apuntadores hash, estableciendo una relación que enlaza cada bloque actual con el previo. Esta secuencia de bloques forma una línea continua que se extiende desde el bloque génesis, el primer bloque de la cadena.

La estructura de la cadena de bloques se replica en todos los nodos de la red, manteniendo así la sincronización. Cada nodo mantiene una copia integral de la cadena, y es responsable de verificar la validez de los bloques y las transacciones contenidas en ella.

En la Figura 3 se puede visualizar la configuración de una cadena de bloques y cómo los bloques están interconectados mediante las transacciones, construyendo así una secuencia fluida. Cada bloque incorpora un hash que representa su contenido, junto con el hash del bloque previo, asegurando de esta manera la inalterabilidad y la integridad de la cadena.

Figura 3. Estructura de la cadena de bloques.



Nota. Estructura de una cadena. Fuente (Waldman , 2018)

1.2.4 Estructura Hash.

Un hash consiste en una función matemática que convierte un conjunto de datos de cualquier tamaño en una cadena de caracteres de longitud fija. Dentro del ámbito de la tecnología blockchain, los hashes desempeñan un rol crucial en cuanto a la seguridad y la probidad de la cadena de bloques.

La estructura hash en la cadena de bloques se refiere a la manera en que los bloques se enlazan a través de los hashes. Cada bloque incorpora el hash del bloque previo en su información. Al crear un nuevo bloque, se introduce el hash del bloque anterior, perpetuándose este proceso. De esta manera, todos los bloques se unen en una secuencia continua, constituyendo la cadena de bloques.

Supongamos que tenemos una cadena de bloques compuesta por tres bloques. En cada uno de ellos se encuentra el hash del bloque anterior:

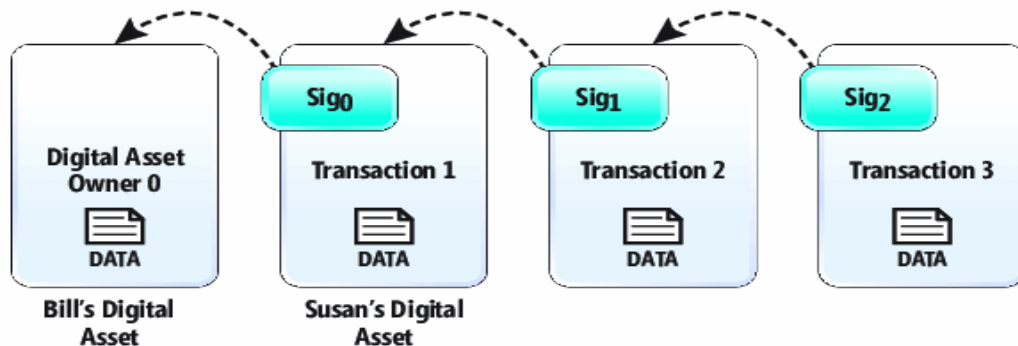
Bloque 1: Contiene sus propios datos y un hash que representa dichos datos.

Bloque 2: Incluye sus propios datos, un hash que refleja dicha información y, además, el hash del Bloque 1.

Bloque 3: Posee sus propios datos, un hash que refleja sus datos, y el hash del Bloque 2.

Si un atacante intentara modificar el contenido del Bloque 2, el hash de este se vería alterado. En consecuencia, el hash almacenado en el Bloque 3 ya no concordaría con el hash modificado del Bloque 2. Esto resultaría en una ruptura de la cadena de bloques, dado que los hashes no estarían conectados de forma correcta. Cualquier modificación en un bloque tendría impacto en todos los bloques subsiguientes, originando la inmutabilidad de la cadena y asegurando la detección de cualquier intento de alteración. Esta estructura hash en la cadena de bloques garantiza la seguridad, confiabilidad e inmutabilidad de la información en la cadena, elementos esenciales para mantener la integridad de la red blockchain.

Figura 4. Cadena Hash



La cadena hash de transacciones utiliza firmas digitales para trasladar la propiedad de un activo digital. Cada registro de transacción establece un enlace criptográfico hacia la transacción previa en la cadena hash. (Waldman , 2018)

En el ámbito de la cadena de bloques, la cadena hash de transacciones se destaca por su seguridad criptográfica y su capacidad para resistir manipulaciones. Cualquier alteración en la transacción inicial tendría consecuencias en el valor de 'Sig0', lo que, a su vez, implicaría la necesidad de actualizar el valor de hash

almacenado en la primera transacción y en todas las subsiguientes de la cadena hash.

Estos elementos de transacción se representan por medio de datos. Aunque los contenidos de cada transacción pueden variar en distintas aplicaciones de la cadena de bloques, para nuestros propósitos, resumiremos los datos subyacentes. Es crucial entender que la cadena de hash consiste en una secuencia de transacciones interconectadas mediante valores hash que provienen de las transacciones previas.

Específicamente en el contexto de las cadenas de bloques para criptomonedas, cada elemento de transacción incorpora una enumeración de las entradas y salidas de monedas digitales, junto con información adicional como la marca de tiempo y la posibilidad de incluir una comisión por la transacción. Estos detalles de entradas y salidas de monedas digitales son esenciales para representar fielmente un registro financiero detallado.

1.2.5 Elementos fundamentales en una red Blockchain.

1.2.5.1 Bloques

Un bloque dentro de la cadena representa un conjunto de transacciones válidas y datos complementarios que ha sido agregado a la secuencia. Cada bloque en la cadena, excepto el bloque inicial que da inicio a la secuencia, contiene los siguientes componentes:

- Un identificador alfanumérico, conocido como hash del bloque anterior, que establece la conexión con el bloque previo en la cadena.
- Un grupo de transacciones legítimas que han sido incorporadas en ese bloque. La cantidad de transacciones en cada bloque puede variar y es influenciada por distintos factores.

- Un segundo código alfanumérico, que representa el hash del bloque subsiguiente en la secuencia, creando así un vínculo con el siguiente bloque en la cadena.

En resumen, un bloque en la cadena de bloques es una unidad informativa que contiene transacciones y datos de referencia para mantener la conexión con los bloques precedentes y sucesivos en la cadena. Esto asegura la continuidad y la integridad del registro en la red blockchain

1.2.5.2 Nodos.

Un nodo en el contexto de Bitcoin hace referencia a un dispositivo o unidad central de procesamiento (CPU) conectado a la red de Bitcoin, que emplea un software para guardar y distribuir una versión actualizada de la cadena de bloques en tiempo real.

Cuando un bloque es válido y se añade a la cadena, esta información se difunde a todos los nodos presentes en la red, y cada uno de estos nodos agrega dicho bloque a su copia propia almacenada. De esta manera, todos los nodos en la red Bitcoin cuentan con una versión sincronizada y reciente de la cadena de bloques.

Este proceso de distribución y constante actualización de la cadena de bloques en cada nodo es lo que garantiza la seguridad y la integridad de la red. Cada nodo tiene la capacidad de validar y autorizar las transacciones contenidas en cada bloque, además de certificar que la información permanezca coherente en toda la red.

1.2.5.3 Protocolo P2P (peer to peer).

El Modelo P2P, también conocido como Peer-to-Peer (par a par), se trata de una estructura de red descentralizada donde los dispositivos (peers) se comunican directamente entre sí sin requerir una entidad central o un servidor intermediario. Cada dispositivo en esta red asume roles de cliente y servidor simultáneamente, compartiendo recursos y servicios de manera directa entre sí.

En el entorno de una red P2P, los dispositivos pueden abarcar desde ordenadores y teléfonos móviles hasta tablets y otros dispositivos conectados a la web. Estos elementos pueden intercambiar datos, ficheros, aplicaciones y recursos sin depender de una infraestructura centralizada.

En un sistema P2P, la interacción se lleva a cabo mediante la identificación y ubicación de los otros dispositivos en la red. Cada dispositivo puede localizar y enlazar con otros peers utilizando direcciones IP o nombres de host. Esta red carece de una entidad central que dirija o coordine las conexiones, lo que brinda mayor resistencia a fallas y dificulta su censura o ataque.

El Protocolo P2P tiene aplicaciones diversas, como el intercambio de ficheros, la mensajería instantánea, las plataformas sociales descentralizadas y las criptomonedas como Bitcoin. En el caso de Bitcoin, la red opera a través de un protocolo P2P, en el cual los nodos (peers) enlazan para compartir la cadena de bloques y validar las transacciones, sin necesidad de un servidor central que controle la red.

Este Protocolo P2P es el cimiento de registros distribuidos a nivel mundial llamados cadenas de bloques o Blockchain, siendo Bitcoin la más grande de ellas. Estas cadenas posibilitan transferencias de dinero directas y seguras entre individuos, sin la intervención de intermediarios como los bancos.

A diferencia de internet, que se enfoca en ser una red informativa, el blockchain funge como una red de valor o moneda. Además, se constituye como un entorno que facilita a todos acceder a la verdad, dado que cualquier información

registrada en la cadena se encuentra organizada y a disposición para su verificación.

En términos elementales, el blockchain es un código fuente de código abierto, lo que denota que cualquier persona puede descargarlo libremente, implementarlo y aprovecharlo para crear nuevas soluciones de administración de transacciones en línea. Esta tecnología brinda la opción de generar una amplia gama de aplicaciones y transformar diversos aspectos de la vida diaria.

La seguridad del blockchain radica en su encriptación, que opera con claves públicas y privadas, proporcionando una seguridad robusta en las transacciones. Con esta tecnología, ya no se precisa preocuparse por el correcto funcionamiento de cortafuegos o la presencia de individuos con malas intenciones.

1.2.5.4 Transacciones.

Dentro del marco del protocolo de transacciones en blockchain, la seguridad y confiabilidad desempeñan un papel crucial para asegurar la transferencia segura y precisa de unidades monetarias entre usuarios. En este protocolo, una transacción consta de dos elementos principales:

Destinatarios de la transacción: Estos representan el receptor de la información transferida y son esenciales para definir la dirección hacia la cual se dirige la transferencia de fondos. Cada destinatario de la transacción especifica la cantidad de información transferida desde el origen y la dirección destinataria. La precisión en estas especificaciones evita confusiones y errores en la transferencia de fondos.

Orígenes de la transacción: Los orígenes son los datos o fondos utilizados para realizar la transacción. Estos provienen de operaciones anteriores y sirven como base para establecer futuros destinatarios de transacciones. En otras palabras, los orígenes de una transacción actúan como una referencia que autentica la disponibilidad y legitimidad de los fondos antes de llevar a cabo la transferencia.

Esto asegura que los fondos empleados en la transacción sean legítimos y autorizados.

La estructura de destinos y orígenes en una transacción es vital para preservar la seguridad y la solidez del sistema blockchain. Cada transacción debe ser confirmada y validada por los nodos en la red antes de ser incluida en un bloque y agregada a la cadena de bloques. Esta validación se efectúa mediante algoritmos criptográficos que garantizan la autenticidad de las transacciones y evitan cualquier manipulación maliciosa.

Vale la pena destacar que la configuración y el funcionamiento de las transacciones en blockchain varían dependiendo de la criptomoneda o red en particular. No obstante, el concepto fundamental de destinos y orígenes sigue siendo una característica esencial para salvaguardar la seguridad y confiabilidad de las operaciones en el entorno del blockchain.

Las características de las transacciones se exponen a continuación:

Es posible combinar distintas operaciones de entrada y salida. Por ejemplo, una transacción puede involucrar diversos fondos originados en transacciones previas y distribuirlos de manera eficiente entre diferentes beneficiarios.

La suma total de las entradas debe ser igual o superior a la suma total de las salidas. En situaciones en las que un usuario carezca de transacciones previas que sumen exactamente la cantidad que desea enviar, es posible utilizar transacciones antiguas con un valor superior al necesario y luego efectuar la salida de los fondos deseados hacia el beneficiario. El saldo restante, es decir, la diferencia, también se incluirá en la transacción.

Tras realizar una transacción en el contexto del sistema blockchain, los usuarios pueden encontrarse con un excedente en sus orígenes, denominado "comisión". Esta comisión es opcional y resulta de configurar las entradas y salidas al crear la transacción.

La comisión surge cuando el valor de las entradas supera el de las salidas, generando un saldo extra. Básicamente, esta comisión constituye una “recompensa” que los usuarios pueden otorgar al nodo encargado de procesar la transacción. Al asignar una comisión, se motiva a los nodos de la red a procesar la transacción de manera más ágil y eficiente.

El propósito de la comisión radica en incentivar a los nodos a emplear sus recursos para procesar las transacciones de los usuarios. Esto fomenta la participación activa de los nodos en el funcionamiento de la red, ya que, al hacerlo, pueden recibir estas comisiones como reconocimiento.

Es esencial destacar que el usuario determina la cuantía de la comisión, que puede variar según la urgencia o prioridad para procesar su transacción. Cuanto mayor sea la comisión, mayor será la probabilidad de que los nodos seleccionen la transacción para ser incluida en un bloque, y, en consecuencia, se procesará con mayor rapidez.

1.2.6 Smart contracts.

El término "contrato inteligente" (smart contract) fue acuñado por Nick Szabo en 1994, mucho antes de la irrupción de las redes de blockchain. Szabo presentó la idea como un protocolo programable diseñado para gestionar transacciones y establecer las condiciones de un acuerdo. En esencia, un contrato representa una serie de disposiciones consensuadas entre partes con experiencia y constituye la manera convencional de formalizar relaciones, como garantías, pactos entre entidades o representaciones de derechos de propiedad. La innovación propuesta por Szabo radicaba en la traducción de estas cláusulas pactadas a código informático, para luego integrarlas en hardware o software capaces de ejecutarlas automáticamente. Esto conllevaría la ventaja de reducir la dependencia de intermediarios en las transacciones y minimizar las posibilidades de errores o excepciones no deseadas. (Cuvi Santacruz & Franco Cortázar, 2023)

En el contexto de una red blockchain, los contratos inteligentes adquieren el rol de fragmentos de código ejecutable que residen directamente en la propia red. Estos códigos se encuentran vinculados a direcciones únicas en la cadena. Cada contrato es registrado en relación a una transacción, lo que posibilita su ejecución automática e independiente en cada nodo de la red.

Los contratos inteligentes han ganado relevancia en el ámbito de la tecnología blockchain debido a su potencial para automatizar y asegurar diversos tipos de acuerdos y transacciones. A medida que operan en una red descentralizada y distribuida, estos acuerdos prescinden de la necesidad de intermediarios convencionales, lo que conlleva a la disminución de gastos y acelera los procedimientos comerciales. Además, la inalterable y transparente naturaleza de la cadena de bloques asegura la integridad y confiabilidad de los contratos, reduciendo al mínimo la posibilidad de manipulación o fraude.

Por lo tanto, los contratos inteligentes representan una innovación sustancial en el campo de las tecnologías de registro distribuido, ofreciendo una forma eficiente, segura y confiable de automatizar y ejecutar acuerdos en diversos sectores, desde las finanzas hasta la gestión de la cadena de suministro. Su capacidad para traducir reglas y condiciones en código ejecutable abre nuevas oportunidades para la transformación digital y la optimización de procesos en una amplia gama de industrias.

Los smart contracts representan una innovación revolucionaria que ha surgido en el contexto de la tecnología blockchain. Estos contratos inteligentes permiten la automatización y ejecución confiable de acuerdos de manera segura y transparente dentro de una red blockchain. Lo distintivo de los smart contracts radica en su capacidad para traducir términos y condiciones de un contrato tradicional en código de programación, el cual es ejecutado en la cadena de bloques.

La base conceptual de los smart contracts fue introducida por Nick Szabo en 1994, mucho antes de la aparición de las redes de blockchain. Szabo concibió estos

contratos como protocolos programables de transacciones que definen y regulan las condiciones acordadas entre las partes involucradas. En lugar de depender de intermediarios o terceros, los smart contracts se apoyan en la ejecución automática y descentralizada, eliminando así la necesidad de confiar en una autoridad central.

En esencia, los smart contracts representan la transposición de cláusulas contractuales en fragmentos de código ejecutable, los cuales son incorporados en la cadena de bloques. Cada smart contract es identificado por una dirección única dentro de la red y queda vinculado a una transacción específica. Esto facilita su ejecución autónoma y consistente en cada nodo de la red, sin necesidad de intervención humana.

Estos contratos inteligentes consiguen ser implementados en una extensa gama de aplicaciones. Por ejemplo, en situaciones de pérdidas causadas por desastres naturales, un smart contract puede activarse automáticamente para permitir a las partes afectadas reclamar la indemnización correspondiente. Los detalles específicos, como la cantidad a ser recibida y los motivos de la compensación, pueden ser especificados en el contrato.

Es esencial resaltar que una vez que un smart contract es desplegado en la red de blockchain, su código no puede ser alterado. Esto pone en relieve la importancia de garantizar la seguridad y la ausencia de errores en el momento de su desarrollo. En este sentido, se han llevado a cabo investigaciones detalladas para que los desarrolladores comprendan la taxonomía de las vulnerabilidades asociadas a los smart contracts, desde cómo manejar excepciones no previstas hasta cómo prevenir y mitigar posibles ataques, como los de denegación de servicio (DoS). (Bravo Cuero, 2023)

En conclusión, los smart contracts representan un avance significativo en la automatización y seguridad de los acuerdos en la era digital, transformando la manera en que se establecen, ejecutan y hacen cumplir los términos contractuales. Su potencial es vasto y su impacto en diversas industrias es cada vez más evidente,

ya que permiten eliminar intermediarios y fomentar la transparencia y confianza en las transacciones.

El análisis en profundidad de los costos asociados a la ejecución de los smart contracts ha sido objeto de una exploración exhaustiva. Un caso ejemplar es el de Ethereum, donde se introduce una unidad de medida denominada 'gas' (que se representa en su criptomoneda Ether, similar al Bitcoin) para equilibrar los cálculos que tienen lugar en diversas operaciones de la red al ejecutar los contratos inteligentes. Si un smart contract no ha sido optimizado adecuadamente, podría incurrir en un consumo desmesurado de gas, lo que se traduciría en gastos elevados para los creadores al momento de su ejecución.

En la red Ethereum, la ejecución de los contratos se lleva a cabo mediante el uso del 'código de la máquina virtual Ethereum', un lenguaje de bajo nivel diseñado para tal propósito. Sin embargo, la programación de estos contratos se realiza en un lenguaje de alto nivel similar a Javascript, conocido como Solidity. Dado que Ethereum opera como una blockchain de acceso público, cada segmento de código de cada contrato presente en la cadena se encuentra accesible públicamente, lo que permite que cualquier nodo en la red pueda examinar minuciosamente su código. Esto, a su vez, contribuye a que el comportamiento de estos contratos sea predecible y comprensible.

Más allá de estas funciones, los smart contracts presentan una versatilidad que les permite gestionar estados, llevar a cabo alteraciones en activos digitales, recibir y procesar entradas, interactuar con servicios externos y plasmar la lógica de negocios esencial para su correcto funcionamiento.

Una vez que estos contratos inteligentes son desplegados en la red, su accionar se pone en marcha a través de mensajes o transacciones dirigidas a su identificador único. Un aspecto crucial radica en que estos contratos deben ser intrínsecamente deterministas, es decir, un mismo conjunto de datos de entrada

siempre conlleva al mismo resultado de salida. La razón detrás de esta característica es garantizar que la ejecución de los contratos sea previsible y establecer salvaguardias contra posibles discrepancias entre los nodos de la red, lo que podría tener consecuencias negativas para el consenso que fundamenta la robustez de la blockchain.

Figura 5. Funcionamiento de un contrato inteligente.



Nota. Flujo de un contrato inteligente y su respectivo funcionamiento. (ihodl, 2017)

1.2.7 Características de Blockchain.

Las tres características clave de la blockchain que son importantes y relevantes para comprender su funcionamiento son las siguientes:

Descentralización: La blockchain opera en una red distribuida, donde múltiples nodos (dispositivos) mantienen una copia completa y actualizada de la cadena de bloques. No hay un mando central o entidad que controle toda la red. Esto hace que la blockchain sea resistente a fallos y más segura, ya que no hay un único punto de vulnerabilidad.

Inmutabilidad: Una vez que la información se registra en un bloque y es confirmada por la red, se vuelve prácticamente imposible de alterar. Cada bloque contiene un hash criptográfico del bloque anterior, lo que crea una cadena de bloques que está vinculada y asegura la integridad de los datos. Cualquier intento de modificar un bloque requeriría cambiar todos los bloques siguientes, lo que resulta altamente costoso y poco práctico.

Transparencia: Cada transacción registrada en la blockchain es visible para todos los nodos en la red. Todos los participantes tienen acceso a la misma información, lo que garantiza la transparencia de las operaciones. Además, cualquier persona puede verificar la autenticidad de una transacción y su registro en la cadena de bloques, lo que aumenta la confianza en el sistema.

1.2.8 Ethereum.

Ethereum, concebida por Vitalik Buterin, es una plataforma distribuida y descentralizada que, al igual que Bitcoin, se basa en la tecnología blockchain. A diferencia de Bitcoin, Ethereum no solo registra el histórico de transacciones en sus nodos, sino que también almacena el estado actual de las cuentas y permite la ejecución de programas, incluyendo los famosos "contratos inteligentes". (Domínguez Padilla, 2022)

Los nodos de la red Ethereum no solo contienen un registro completo de las transacciones, sino que también albergan un registro actualizado del estado de todas las cuentas. Esto habilita la ejecución de código y la creación de aplicaciones descentralizadas, conocidas como DApps.

En esencia, Ethereum se puede describir como un vasto sistema computacional que brinda amplias oportunidades para su uso, experimentación y modificación según las necesidades específicas de los usuarios. Además, Ethereum permite la creación de tokens personalizados, lo que significa que cualquier persona puede diseñar y ofrecer su propia moneda digital para ser utilizada por otros usuarios.

El objetivo fundamental de Ethereum es proporcionar una plataforma abierta y alternativa para desarrollar aplicaciones descentralizadas. A través de la tecnología blockchain, se facilita la creación de sistemas autónomos que operan sin una autoridad central y son controlados por la comunidad. Al igual que Bitcoin, Ethereum se caracteriza por ser una red descentralizada e inmutable, pero se diferencia por ser altamente configurable, lo que permite adaptar sus características para satisfacer diversas necesidades. (Domínguez Padilla, 2022)

La filosofía subyacente en el diseño de Ethereum abarca varios principios fundamentales que guían su desarrollo y funcionalidad:

Simplicidad: El protocolo de Ethereum busca mantener un diseño simple y eficiente tanto en el almacenamiento de datos como en el rendimiento temporal. El objetivo es que incluso un programador con conocimientos medios pueda efectuar la especificación completa sin complicaciones excesivas.

Universalidad: Ethereum suministra un lenguaje interno de alto nivel que admite a cualquier programador utilizarlo para construir diversos tipos de contratos inteligentes o incluso crear sus propias monedas personalizadas. La plataforma se presenta como una herramienta versátil que puede adaptarse a diferentes propósitos.

Modularidad: Las diferentes partes del protocolo de Ethereum se trazan con alta modularidad y separabilidad. Esto significa que se busca que el sistema sea flexible para admitir reformas sin que afecten negativamente otras partes del protocolo. Los cambios deben favorecer al sistema en su conjunto y no ser únicamente beneficiosos para una parte.

Agilidad: Aunque se debe tener cautela en las modificaciones a nivel alto del protocolo, si durante las pruebas de desarrollo se asemejan oportunidades o progresos, se deben aprovechar. Esto implica una actitud abierta a la mejora constante y la optimización del sistema.

Sin discriminación y sin censura: El protocolo de Ethereum no debe delimitar características de uso específicas. Los módulos reguladores deben estar diseñados para regular el daño y no para oponerse a aplicaciones no deseadas en particular. Cualquier programador puede elaborar una funcionalidad, inclusive si es un buda infinito, siempre que esté dispuesto a pagar la tarifa computacional correspondiente.

1.2.9 Máquina Virtual de Ethereum.

Ethereum es una plataforma de cadena de bloques que se destaca por su naturaleza altamente programable y su capacidad para ejecutar contratos inteligentes. A diferencia de otras cadenas de bloques que ofrecen un conjunto limitado de operaciones predefinidas, Ethereum brinda a los usuarios la libertad de construir sus propias operaciones y aplicaciones dentro de su infraestructura.

Este poder de personalización se logra gracias a la presencia de la Ethereum Virtual Machine (EVM), que es una máquina virtual con la habilidad única de gestionar códigos de cualquier complejidad. La EVM es programable en varios lenguajes de programación, incluidos Solidity (con similitudes a C y JavaScript) y Serpent (similar a Python), lo que permite a los desarrolladores crear contratos inteligentes de manera eficiente y versátil (Dhulavvagol , Bhajantri , & Totad, 2020)

La EVM es el núcleo central de Ethereum y representa el corazón de la plataforma. Actúa como un motor que conecta y coordina todos los nodos de la red, permitiendo que la ejecución de contratos inteligentes sea una realidad en toda la red distribuida.

Los contratos inteligentes son una de las características más destacadas de Ethereum. Estos contratos son códigos ejecutables amontonados en la cadena de bloques que facilitan y aseguran el cumplimiento de los términos establecidos en el contrato. Su capacidad para automatizar tareas, ejecutarse de forma rápida y ser altamente efectivos los convierte en elementos fundamentales para diversas aplicaciones descentralizadas.

Un contrato inteligente está compuesto por tres elementos principales: un balance, un almacenamiento y un código ejecutable. El balance se refiere a los fondos o activos digitales asociados al contrato, mientras que el almacenamiento guarda la información específica del estado del contrato. Cada vez que el contrato es invocado o llamado, se modifica el estado y los cambios se registran en la cadena de bloques de forma inmutable.

En el ecosistema de Ethereum, la base de datos se actualiza inagotablemente gracias a la colaboración de cientos de nodos conectados en una misma red. Estos nodos son computadoras que ejecutan la Ethereum Virtual Machine (EVM) y procesan las mismas instrucciones de forma distribuida. Este enfoque descentralizado permite mantener un consenso compartido y confiable en toda la cadena de bloques de Ethereum. (Dhulavagol , Bhajantri , & Totad, 2020)

De hecho, se puede concebir a Ethereum como una especie de "ordenador mundial", donde cada nodo en la red actúa como un componente de procesamiento. La ejecución de la EVM en estos nodos garantiza que todas las transacciones y operaciones en la cadena de bloques se realicen de manera coherente y transparente, asegurando la integridad y seguridad de la red.

Es importante resaltar que la plataforma de Ethereum en sí misma no tiene valor inherente. Al igual que otros lenguajes de programación, su utilidad y potencial dependen en gran medida de la creatividad y la visión de los emprendedores y programadores que trabajan en ella. Son ellos quienes, mediante el desarrollo de contratos inteligentes y aplicaciones descentralizadas, aprovechan al máximo la plataforma y les dan vida a sus posibilidades.

La capacidad de programar y personalizar contratos inteligentes en Ethereum abre un mundo de oportunidades para la creación de diversos servicios y soluciones descentralizadas. Empresas, startups y desarrolladores pueden innovar y ofrecer una amplia gama de aplicaciones, desde sistemas financieros y de identidad, hasta

juegos y mercados descentralizados. La riqueza y diversidad de estas aplicaciones es lo que impulsa el valor y la adopción de Ethereum como una plataforma blockchain líder.

1.2.10 Solidity.

Solidity es el lenguaje de programación más utilizado y popular para desarrollar Smart Contracts en la plataforma Ethereum. Al igual que otros lenguajes de programación, Solidity permite a los desarrolladores establecer contratos inteligentes que se ejecutan en la Ethereum Virtual Machine (EVM) y operan en la cadena de bloques de Ethereum. (Hegedűs, 2019)

Para iniciar un flujo en Solidity, se utiliza la palabra reservada "contract", que es análoga a la declaración de una clase en otros lenguajes de programación. Un contrato en Solidity es como un contenedor que puede contener diferentes elementos, como funciones, modificadores y variables. Estos elementos definen la lógica y el comportamiento del contrato inteligente.

Dentro de un contrato en Solidity, se pueden precisar funciones que determinan las acciones que el contrato puede llevar a cabo. Las funciones pueden recibir parámetros y devolver valores, permitiendo que el contrato interactúe con otros contratos o con usuarios de la red Ethereum.

Además de las funciones, Solidity admite el uso de modificadores, que son bloques de código que se ejecutan antes o después de una función. Los modificadores se utilizan para aplicar lógica adicional o restricciones a las funciones, lo que puede ayudar a mejorar la seguridad y la eficiencia del contrato.

Solidity también ofrece diferentes tipos de datos, como enteros, cadenas, arreglos y estructuras, que permiten a los desarrolladores manipular y almacenar información de manera eficiente dentro del contrato.

Una característica importante de Solidity es que admite la herencia de contratos, lo que significa que un contrato puede heredar propiedades y funcionalidades de otro contrato. Esto permite la reutilización de código y facilita la organización y la gestión de contratos más complejos.

1.2.11 El voto electrónico y Blockchain.

La sociedad ha experimentado una evolución significativa debido al avance de la tecnología, y esta ha influido y complementado el complejo comportamiento social. En este contexto, la posibilidad de implementar el voto electrónico en los procesos electorales es una opción, pero crear un sistema de este tipo no se limita a contar votos o permitir su emisión, sino que también debe respetar los principios fundamentales del voto, como su unicidad por persona, su carácter privado y secreto. (Lajpop Ajpacajá)

No todas las arquitecturas de software efectúan con los estrictos requisitos del voto electrónico, y es aquí donde el blockchain surge como una tecnología que satisface estos requerimientos. La tecnología blockchain se basa en la privacidad, seguridad y distribución de poder, entre otras características, lo que la convierte en una opción adecuada para garantizar la integridad y confidencialidad en los procesos de votación. (Lajpop Ajpacajá)

Implementar el voto electrónico con blockchain puede ofrecer una solución sólida para asegurar la autenticidad y la transparencia en los procesos electorales, lo que fortalece la confianza de los ciudadanos en el sistema democrático. Al tener en cuenta estos fundamentos y características, se puede avanzar hacia un sistema de voto electrónico más confiable y seguro.

1.2.12 Características más relevantes en una votación.

Voto único: Cada persona facultada para votar solo puede emitir un voto durante el proceso de votación.

Voto secreto: El voto es privado y nadie puede conocer el voto específico de un elector.

Integridad de los votos: Una vez emitido el voto, no puede ser alterado por ninguna entidad, asegurando que el resultado refleje la decisión del elector.

Integridad de la votación: El resultado total de la votación no puede ser modificado o manipulado.

Auditoría individual: Se debe avalar que los votos se cuenten de manera precisa y correcta.

Auditoría universal: Se debe aseverar que todo el proceso electoral, desde el inicio hasta el final, se realice de manera adecuada y transparente.

Cumplir con estos principios en el diseño de un sistema de voto electrónico es crucial para asegurar la confianza y la legitimidad de los resultados. La tecnología blockchain, con sus características de privacidad, seguridad y distribución de poder, se presenta como una opción prometedora para abordar estos desafíos y mejorar la transparencia en los procesos electorales. Al implementar el voto electrónico con blockchain, se puede avanzar hacia elecciones más seguras, confiables y accesibles para todos los ciudadanos.

1.3 Marco teórico: Situacional

1.3.1 Método de voto tradicional.

El voto tradicional es una de las formas más antiguas y ampliamente utilizadas en el mundo para elegir líderes y resguardar la democracia. En Ecuador, este método se lleva a cabo de la siguiente manera:

En primer lugar, la persona que va a ejercer su derecho al voto debe dirigirse al lugar designado como sitio de votación, donde preliminarmente se realizó el registro electoral. Este lugar es habilitado por el Consejo Nacional Electoral para que funcionen las mesas de votación.

En el proceso electoral, se cuenta con un sistema delineado para certificar que el voto sea transparente, legal y libre de manipulación. El votante debe pedir a la mesa de votación la papeleta de votación, que es el documento donde el ciudadano marca su predilección electoral.

Luego, el sufragante se dirige a la urna, donde ejerce su derecho al voto, marcando su elección en la papeleta. Después, se acerca a la urna y coloca su voto en ella. Esta etapa es fundamental para el usuario o ciudadano dentro del sistema.

El objetivo de este proceso es atestiguar que cada voto sea contado de manera justa y transparente, respetando la voluntad de los ciudadanos y garantizando la moralidad de los resultados. El voto habitual ha sido una piedra angular de la democracia en Ecuador y en muchos países del mundo, y sigue siendo un pilar importante para aseverar la participación ciudadana en el proceso electoral.

En el voto tradicional, el votante pierde el rastro total de su voto y confía en el sistema para que el voto sea registrado correctamente. La mesa de votación está compuesta por ciudadanos seleccionados por el Consejo Nacional Electoral a través de un sorteo, quienes actúan como jurados de votación. Su función es atender la mesa de votación, realizar los escrutinios correspondientes y entregar los resultados de las votaciones en los documentos electorales.

Al finalizar las votaciones, la mesa de votación abre la urna y viene a realizar el conteo de votos. Se presenta un conjunto de filas que contienen los nombres de los candidatos y diversas columnas destinadas a registrar los votos obtenidos por cada uno de los aspirantes. Este proceso forma parte del Escrutinio, en el cual intervienen los jurados de sufragio, las comisiones escrutadoras y el Consejo Nacional Electoral. Su propósito principal es llevar a cabo el cómputo de los sufragios, resolver tanto las cuestiones fácticas como jurídicas que se planteen basándose en las causas legales de reclamación, y realizar las declaratorias de elección correspondientes. Esencialmente, esta actividad pública implica la verificación y consolidación de los resultados de las votaciones. (Garzón Sherdek & Cahuasquí Cevallos, 2021).

1.3.2 Ventajas y desventajas del método tradicional.

El método tradicional del voto presenta diversas ventajas y desventajas que son importantes para tener en cuenta al compararlo con otros métodos de votación.

1.3.2.1 Ventajas del método tradicional del voto:

- **Confiable:** Este método ha sido utilizado durante mucho tiempo y ha demostrado ser confiable para contar los votos de manera precisa.
- **Transparencia:** Los votantes pueden presenciar el proceso de votación y conteo de votos, lo que aumenta la transparencia y la confianza en el sistema electoral.
- **Participación ciudadana:** Al acudir físicamente a los centros de votación, se promueve la participación ciudadana en el proceso democrático.
- **Inclusión:** Permite que personas de todas las edades y niveles de acceso a la tecnología puedan ejercer su derecho al voto.
- **Cultura democrática:** El voto tradicional ha sido parte de la cultura democrática en muchos países y es una tradición valorada por los ciudadanos.

1.3.2.2 Desventajas del método tradicional del voto:

Costoso: La organización y logística de las elecciones tradicionales pueden ser costosas, especialmente en países con grandes poblaciones.

Tiempo y esfuerzo: El proceso de votación y conteo manual de votos puede llevar tiempo y retrasar la divulgación de los resultados electorales.

Errores humanos: Preexiste la peripetia de errores humanos en el conteo de votos o en la concesión incorrecta de votos a los candidatos.

Desplazamiento físico: Requiere que los votantes se desplacen físicamente a los centros de votación, lo que puede ser inconveniente para algunas personas.

Dificultades en el extranjero: Para los votantes que se encuentran en el extranjero, puede ser difícil o costoso ejercer su derecho al voto en el sistema tradicional.

Estas ventajas y desventajas proporcionan un contexto importante para comparar el método tradicional del voto con otras opciones, como el voto electrónico o el voto por correo, y para evaluar cuál de ellos puede ser más adecuado para satisfacer las necesidades y exigencias de un proceso electoral justo y confiable.

1.3.3 Método de Voto Electrónico.

Para garantizar la legitimidad de cualquier método de votación, es esencial que el voto cumpla con ciertas circunstancias básicas de seguridad. Estas condiciones incluyen que el voto sea secreto, universal y único. El voto electrónico, al igual que otros métodos, está diseñado para cumplir con estos requisitos esenciales.

El voto electrónico hace uso de tecnología avanzada y sigue un proceso similar al método tradicional de votación. Es notable recalcar que los sistemas de voto electrónico no son algo nuevo, ya que se han intentado implementar durante varios años para resolver desafíos tecnológicos de gran importancia.

Las implementaciones de voto electrónico pueden variar considerablemente y pueden presentar diferentes grados de automatización en cada caso. Sin embargo,

el objetivo común es afirmar que el asunto electoral sea honesto, seguro y capaz de preservar la privacidad del voto de cada ciudadano.

1.4 Marco Teórico Contextual

1.4.1 Casos de Éxito.

El voto electrónico ha sido implementado y utilizado en varios países durante muchos años. Entre los países más destacados a nivel mundial que han mostrado un interés significativo en el voto electrónico se encuentran Brasil, India, Venezuela y los Estados Unidos. En Brasil, el voto electrónico se ha utilizado desde 1996 y ha sido aplicado en diversos procesos electorales a lo largo del tiempo. (Euskadi.eus, 2022)

Un ejemplo relevante del uso del voto electrónico en Brasil fue durante las elecciones presidenciales de 2010, en las cuales participaron 135 millones de votantes. El sistema demostró su eficiencia al permitir conocer los resultados en solo una hora y quince minutos después de que cerraron los colegios electorales.

La aceptación del sistema de voto electrónico en Brasil ha sido notoria, tanto que el país ha prestado sus máquinas de voto electrónico en forma de alquiler a otras naciones, como Paraguay y Ecuador, para que también puedan realizar procesos electorales utilizando esta tecnología.

El voto electrónico ha mostrado ser una alternativa efectiva para modernizar y agilizar el proceso electoral, además de garantizar mayor seguridad y transparencia en los resultados. Aunque ha sido exitoso en muchos países, también ha generado debates y consideraciones sobre aspectos como la ciberseguridad y la confiabilidad del sistema.

Voto Electrónico representa un importante avance en la forma en que los ciudadanos ejercen su derecho al voto y participan en el proceso electoral, fomentando una mayor eficiencia y participación ciudadana. (Euskadi.eus, 2022)

El voto electrónico ha sido implementado en varios países alrededor del mundo durante un período considerable, demostrando una notable adaptabilidad, eficacia y aceptación por parte de los votantes. Aunque no es un sistema perfecto y presenta algunas debilidades, también exhibe prerrogativas reveladoras en paralelo con el sistema tradicional de votación. Es por esta razón que varios países a nivel mundial han optado por utilizarlo en sus procesos electorales. Algunos de estos países son:

En Europa:

Bélgica es uno de los países que a nivel mundial tiene un método de voto electrónico más moderno, puede ser por el tiempo que lleva usando este régimen el cual se implementó “desde 1989, allí se empezó utilizando unas tarjetas de banda magnética en donde por medio de una pantalla donde los votantes realizaban su elección” (Euskadi.eus, 2022), esta información se almacenaba en las tarjetas y estas consecutivamente se depositaban en una urna que analizaba y computaba la información.

“Para 2010 comenzó un proceso de licitación para la selección de un nuevo sistema o actualización del ya existente, el sistema nuevo se basa en una urna electrónica con pantalla táctil y con posibilidad de imprimir un comprobante del voto en papel para la auditoria del resultado” (Euskadi.eus, 2022). El proceso de licitación buscaba mejorar y modernizar el sistema de votación, con el objetivo de incrementar la eficiencia y transparencia en el proceso electoral. La incorporación de la urna electrónica con pantalla táctil proporciona una manera más intuitiva y accesible para los votantes, permitiéndoles emitir su voto de forma rápida y sencilla. Asimismo, la opción de obtener un comprobante en papel ofrece una

capa adicional de seguridad y confiabilidad, ya que se puede utilizar para verificar y auditar los resultados de las elecciones posteriormente.

Una de las mejoras más significativas en los avances tecnológicos del sistema de voto electrónico se ha centrado en la trazabilidad del voto. En las elecciones del 25 de mayo de 2019, en los puestos de votación que utilizan el voto electrónico, se implementó un novedoso sistema que brinda a los votantes la certeza de que su voto es trazable y seguro (Euskadi.eus, 2022).

Cuando un votante emite su voto en la máquina de votación electrónica, esta genera una papeleta impresa encriptada que contiene la selección realizada por el votante. Esta papeleta es única para cada votante y está encriptada para salvaguardar la privacidad de su elección. Luego, el votante tiene la oportunidad de confirmar y validar su voto a través de un lector, lo que le permite verificar que la elección impresa en la papeleta coincide con su intención de voto. Una vez confirmado, el votante deposita la papeleta en una urna segura.

Este sistema de trazabilidad del voto proporciona una capa adicional de seguridad y confianza para los votantes, ya que pueden verificar personalmente que su voto fue registrado correctamente y que no ha sido alterado de ninguna manera. Además, al utilizar la encriptación, se garantiza que la información del voto se mantenga confidencial y segura durante todo el proceso electoral. (Euskadi.eus, 2021).

En el caso de Estonia, uno de los precursores en la ejecución del voto electrónico, su primera incursión en este procedimiento se remonta al año 2005. Siendo el primer país en permitir el voto a través de internet, Estonia indicó una visión innovadora en el campo de la tecnología electoral. En 2011, alrededor del 25% de los votantes ya había optado por ejercer su derecho al voto mediante este sistema electrónico (Euskadi.eus, 2022).

Una característica distintiva del método de voto electrónico en Estonia es la posibilidad de votar con anticipación, hasta seis días antes de la fecha oficial de las elecciones. Los votantes pueden pronunciar su voto de varias formas, y el voto que se tiene en cuenta para el conteo final es el último emitido, lo que ofrece flexibilidad a los ciudadanos para cambiar su decisión si así lo desean.

Con el pasar de los años, Estonia ha continuado renovando su sistema de voto electrónico. En las elecciones parlamentarias de 2019, aproximadamente el 44% de los votantes prefirió por ejercer su voto a través de este procedimiento, lo que manifiesta la creciente aceptación y confianza en el voto electrónico en el país. Para participar en el voto electrónico, los ciudadanos deben estar registrado anticipadamente como votantes y deben contar con un computador con conexión a internet, así como su documento nacional de identidad.

La experiencia de Estonia en la implementación del voto electrónico ha sido exitosa y ha sido un modelo para otros países que también consideran adoptar este sistema moderno y seguro para sus procesos electorales. La facilidad de acceso y la confianza en la seguridad del sistema han ayudado a su amplia aceptación por parte de los votantes estonios.

Bulgaria, en este país se realizaron las elecciones al parlamento para el 2021 con máquinas electrónicas, excepto en colegios con menos de 300 votantes registrados, hospitales y otras instituciones sociales, se presentaron fallas técnicas por su reciente implantación de este sistema, y por tal razón, “se tuvo que suspender el uso de dichas máquinas y utilizar papeletas como el método tradicional para 56 colegios electorales de los más de 12 mil” (Euskadi.eus, 2021).

En América los países que tienen un sistema de voto electrónico establecido son:

En Brasil, la ejecución del voto electrónico comenzó en el año 1995, cuando se certificó la Ley Electoral que sentó las bases para su adopción. Desde entonces, en 1996, se inició la implantación de las urnas electrónicas en el país.

Brasil ha sido uno de los líderes en América en la estandarización del voto electrónico como método de votación. Para el año 2002, se había conseguido alcanzar un importante hito, ya que el 100% de los votos presenciales fueron emitidos electrónicamente mediante las urnas electrónicas. Con el paso del tiempo, este sistema ha ido siendo más aprobado y confiable, y en las elecciones generales de 2010, cerca de cuatro millones de electores utilizaron urnas biométricas para ejercer su derecho al voto.

El proceso de voto electrónico en Brasil se ha ido generalizando en las elecciones, lo que ha llevado a un aumento en la confianza y la eficiencia del sistema electoral. El uso de urnas biométricas ha sido una de las mejoras implementadas, lo que ha permitido una mayor precisión en la identificación de los votantes y ha asistido a una mayor transparencia en el proceso de votación.

La experiencia de Brasil en la adopción del voto electrónico ha sido exitosa y ha establecido un precedente para otros países de América y del mundo que consideran implementar este moderno y seguro método de votación en sus procesos electorales. La rápida adopción del voto electrónico en Brasil es un claro ejemplo de cómo la tecnología puede mejorar y agilizar los procesos democráticos.

En las elecciones presidenciales de octubre de 2014, más de 23 millones de ciudadanos brasileños utilizaron la urna biométrica, lo que refleja el éxito y la aceptación de la tecnología del voto electrónico en el país. Desde entonces, todas las votaciones que se llevan a cabo en Brasil se realizan mediante el uso de esta tecnología, posicionándose como uno de los países más adaptados y adeptos a este método moderno.

En las últimas elecciones de 2018, nuevamente se utilizó el voto electrónico, aunque con una novedad importante. La impresión del voto, que previamente se realizaba

para garantizar la trazabilidad y la transparencia del proceso, fue eliminada debido a que no cumplía con uno de los elementos fundamentales del voto, que es la privacidad y secreto del sufragio.

Es interesante recalcar que Brasil ha mostrado una gran confianza en su sistema de voto electrónico, tanto así que presta sus máquinas a otros países para que puedan realizar sus procesos electorales utilizando esta tecnología. Esta iniciativa demuestra la credibilidad que tiene el método de voto electrónico en Brasil y su potencial para ser implementado en otros países que buscan modernizar y optimizar sus sistemas electorales.

Estados Unidos es uno de los países con una larga trayectoria en el desarrollo de métodos de voto electrónico y en la automatización del proceso de votación. Su historia en este campo se remonta a 1892, cuando debutó la primera máquina de votación conocida como Myers Automatic Booth. Esta máquina utilizaba palancas mecánicas, asignando una palanca a cada candidato, y fue instalada en las principales ciudades del país en la década de 1930. Para la década de 1960, aproximadamente la mitad de la población estadounidense ya utilizaba estas máquinas para ejercer su voto.

A medida que avanzaba el tiempo, Estados Unidos no se limitó a un único sistema de votación. Para 1980, ya se habían implementado cinco tipos de sistemas de votación en diferentes regiones del país. Estos sistemas incluían máquinas de palanca, tarjetas perforadas, papeletas de votación con o sin sistema de escaneo óptico y máquinas de grabación electrónica directa.

Es importante resaltar que la evolución del voto electrónico en Estados Unidos ha sido continua y ha experimentado diversos avances tecnológicos a lo largo de los años. El país ha adoptado diferentes sistemas de votación en función de las necesidades y capacidades de cada región, buscando siempre mejorar la eficiencia y precisión del proceso electoral.

A lo largo de su historia, Estados Unidos ha demostrado una fuerte inclinación hacia la automatización del proceso de votación, buscando proporcionar a los ciudadanos opciones tecnológicas para ejercer su derecho al voto.

En las elecciones presidenciales de 2012, aproximadamente el 40% de la población estadounidense optó por este método para ejercer su voto, lo que representa casi la mitad de los votantes en el país (Euskadi.eus, 2022). En los últimos años, se han llevado a cabo experimentos más innovadores, como el programa piloto en Virginia Occidental en 2018, donde se implementó la tecnología Blockchain en dos circunscripciones, admitiendo a los habitantes que estaban en el extranjero o en el ejército desplegar su voto.

En el caso de Venezuela, la implementación del voto electrónico comenzó en 1998 y se completó en 2004 con un sistema completo que permitía a las personas votar a través de pantallas táctiles, imprimir su voto y depositarlo en urnas electrónicas. Sin embargo, este método de votación ha sido objeto de controversia y sospechas de posible fraude. Por lo tanto, se han solicitado auditorías de países como Estados Unidos, Chile, Colombia, entre otros, para evaluar la integridad del proceso electoral.

En Asia los países que tienen un sistema de voto electrónico implantado son:

En Emiratos Árabes Unidos, la implementación del sistema de voto electrónico se inició en 2006 con el propósito de fomentar una mayor participación de las personas jóvenes en el proceso electoral. Debido a que el 88% de la población total es foránea y la población es predominantemente joven, se decidió adoptar tecnologías avanzadas para facilitar los trámites administrativos, incluyendo las elecciones.

El comité de elecciones ha realizado campañas en plataformas de redes sociales con la finalidad de instruir y fomentar el adecuado empleo del sistema de votación,

con especial enfoque en la juventud. En mayo de 2013, los dirigentes de los Emiratos Árabes Unidos fijaron como objetivo que todos los principios públicos deberían ser accesibles mediante dispositivos móviles en un plazo de unos años.

En las elecciones al Consejo Federal Nacional celebradas en 2015, 224,000 personas emitieron su voto utilizando el sistema totalmente electrónico, logrando una tasa de participación ciudadana del 35%. Durante este proceso electoral, se registró un aumento significativo del 119% en la participación, con un incremento destacado de la participación de la población femenina. Además, los resultados de las elecciones se conocieron en un tiempo récord, superando apenas los 30 minutos (Euskadi.eus, 2022).

La adopción del voto electrónico en Emiratos Árabes Unidos ha demostrado ser eficiente en promover la participación democrática, especialmente entre los jóvenes y la población extranjera. La rapidez y facilidad del proceso electrónico han contribuido a aumentar la participación ciudadana y agilizar la divulgación de los resultados electorales.

En Filipinas, el proceso de implementación del método de votación electrónica se inició en 2007. En 2008, se llevaron a cabo pruebas piloto utilizando urnas electrónicas y voto biométrico. Sin embargo, durante las elecciones de 2010, en las cuales se utilizó el método de voto electrónico, se presentaron denuncias por fallos en algunas de las máquinas utilizadas.

En 2013, se realizaron de nuevo elecciones parlamentarias con el mismo sistema de voto electrónico manejado en 2010, pero en esta ocasión no se reportaron sucesos. Subsiguientemente, en las elecciones generales de 2016, se volvió a emplear el voto electrónico, utilizando un total de 92,509 máquinas electrónicas para atender a los 55,736,801 votantes.

En este proceso electoral de 2016, se introdujo una idea, ya que las máquinas emitieron un impreso o comprobante del voto, lo cual permitió a los electores autorizar la precisión de su voto antes de sufragar. Esta medida buscaba mejorar la transparencia y confianza en el proceso electoral.

A lo largo de los años, Filipinas ha seguido avanzando en la adopción del voto electrónico, tomando en cuenta los resultados y experiencias previas para mejorar la confianza y eficacia del sistema de votación.

En India, el proceso de adopción del voto electrónico comenzó de forma progresiva a partir de 1989. A lo largo de los años, se fue implementando gradualmente en diferentes elecciones hasta alcanzar un hito significativo en el 2003, cuando se logró que el 100% de los votos fueran emitidos electrónicamente.

Una década después, en las elecciones generales de 2014, se introdujo una importante mejora en el sistema de votación electrónica. Se incorporó un nuevo método de verificación que permitía resolver una preocupación presente en votaciones anteriores: la falta de una forma efectiva de comprobar el voto emitido por el elector. Con esta innovación, se brindó a los votantes la posibilidad de obtener un comprobante de auditoría en papel que verificaba su elección antes de ser depositado en la urna.

Últimamente, en las elecciones ordinarias de 2019, el sistema de votación electrónica dio un paso más hacia la transparencia y la confiabilidad al incorporar el documento de auditoría en papel en el 100% de las máquinas de votación. Esto permitió que todos los votantes pudieran verificar personalmente su voto antes de finalizar el proceso electoral. Esta medida ha sido clave para fortalecer la integridad del proceso electoral en India y ha consolidado al voto electrónico como una opción segura y confiable para la ciudadanía.

METODOLOGÍA DEL PROCESO DE INVESTIGACIÓN

CAPITULO II

CAPITULO II: MARCO METODOLÓGICO

2.1 Metodología de investigación.

2.1.1 Enfoque de investigación.

(Lifeder, 2020) afirma que el enfoque de investigación cualitativa facilita un examen más individual y sistemático de la información, apoyado en ideas y opiniones acerca de un tema específico, posibilitando un análisis no estadístico de los datos. Luego se efectúa una interpretación específica pero coherente y bien fundamentada.

Adicionalmente, la manera en que se adquieren y analizan los datos suele ser más flexible, ya que no sigue rigurosamente las pautas de estos procedimientos. Este enfoque resulta beneficioso para comparar los resultados y las interpretaciones.

La investigación utiliza un enfoque cualitativo, dado que la información mencionada se compone de datos previamente analizados y escritos, obtenidos durante el proceso de entrevistas. Así, este proyecto se fundamenta con el propósito de adquirir datos de individuos que estén relacionados con el cambio en la forma en que los actores electorales pueden emitir sus votos en una plataforma de votación electrónica.

Para llevar a cabo este estudio en el terreno, se utilizará como base la recolección de información y opiniones a través de entrevistas, centradas en las personas involucradas en un proceso electoral. Estas personas incluyen estudiantes, profesores y profesionales en el área de la política.

Investigación detallada de casos específicos de implementación de sistemas de votación electrónica basados en blockchain en diferentes contextos, para comprender los desafíos, beneficios y lecciones aprendidas.

2.1.2 Alcance de la investigación.

El alcance de la investigación será de tipo exploratorio-diagnóstico, permitiendo una comprensión profunda y detallada de los fundamentos teóricos y prácticos de la tecnología Blockchain aplicada a una plataforma de votación electrónica en el contexto de Ecuador. En este sentido, se realizará una revisión exhaustiva de la literatura académica y fuentes especializadas para obtener un panorama completo de las aplicaciones y posibilidades de esta tecnología en el ámbito electoral.

En cuanto al tipo correlacional y explicativo, estos alcances dependen de la disponibilidad y accesibilidad de datos relevantes sobre casos reales de implementación de tecnología Blockchain en procesos electorales en otros países. En caso de contar con datos adecuados, se buscará establecer relaciones y correlaciones entre la adopción de la tecnología y sus efectos en la seguridad, transparencia y eficiencia del proceso electoral. Asimismo, se explorará la posibilidad de establecer explicaciones causales sobre cómo el desarrollo de este prototipo de la plataforma de votación electrónica basada en Blockchain impacta en la participación ciudadana y la confianza en el sistema electoral.

Se tiene la intención de desarrollar una plataforma web altamente parametrizable que contará con dos tipos de usuarios: administrador y votante. El administrador tendrá la capacidad de gestionar elecciones, candidatos y votantes, con funcionalidades para registrar, modificar, eliminar y consultar información. Por otro lado, el usuario votante podrá acceder al sistema, seleccionar el candidato de su preferencia y emitir su voto. Durante todo el proceso, se supervisará el progreso de las elecciones hasta su conclusión, proporcionando resultados rápidos y confiables.

Se llevará a cabo una revisión exhaustiva de la literatura académica y fuentes especializadas para adquirir un profundo conocimiento de los fundamentos teóricos y prácticos de la tecnología Blockchain y su aplicación en plataformas de votación electrónica. Dado que esta aplicación involucra aspectos políticos y datos sensibles, se analizará detalladamente la legislación electoral y las regulaciones vigentes en Ecuador para identificar los requisitos legales y los posibles desafíos que puedan

surgir al implementar una plataforma de votación electrónica basada en Blockchain. Además, se recopilan casos reales de implementación de esta tecnología en procesos electorales de otros países como referencias valiosas para comprender las lecciones aprendidas, los resultados obtenidos y los desafíos enfrentados en tales contextos.

Se evaluará el impacto de la tecnología en la seguridad y transparencia del proceso electoral, analizando cómo se garantiza la integridad de los votos y la protección contra posibles ataques cibernéticos o manipulaciones. Lograremos identificar los desafíos técnicos, legales y logísticos que podrían surgir durante la implementación de la plataforma de votación electrónica, así como las oportunidades para mejorar la participación ciudadana y la confianza en el sistema electoral.

El alcance de esta investigación se limitará a la evaluación teórica, práctica y análisis documental de la tecnología Blockchain aplicada a la votación electrónica en el contexto de Ecuador. Se realizará un prototipo que se encargará de simular un proceso electoral y así verificar que se cumpla con todo el proceso, se llevarán a cabo pruebas de seguridad, así como su despliegue a un ambiente de producción para verificar su funcionamiento, se recopilaron datos primarios de personas reales, ya que se enfoca en un estudio exploratorio y analítico de la temática. Además, se llevarán a cabo pruebas de implementación de la plataforma de votación electrónica basada en Blockchain, con el fin de recopilar datos primarios sobre su funcionamiento, eficiencia y seguridad. Se establecerán correlaciones entre la adopción de la tecnología Blockchain y los resultados obtenidos en términos de seguridad, transparencia y confiabilidad del proceso electoral.

Este enfoque más amplio admitirá conseguir una perspectiva más completa y detallada sobre la viabilidad y efectividad de la tecnología Blockchain en el contexto específico de Ecuador, proporcionando datos empíricos para respaldar las conclusiones y recomendaciones de la investigación.

2.1.3 Tipos de investigación.

2.1.3.1 Investigación Exploratoria

Este proyecto adoptará un enfoque exploratorio porque se recopilará documentación detallada sobre el funcionamiento de la tecnología Blockchain y los resultados y análisis obtenidos de las pruebas de usabilidad. Adicionalmente, se considerarán artículos y trabajos tanto originarios como internacionales para garantizar una perspectiva global en el desarrollo del proyecto. Se dará especial relevancia a escritos que aborden la implementación de sistemas de votación electrónica en diferentes partes del mundo y sus avances hasta la fecha. Además, se examinará la documentación relacionada con sistemas de votación electrónica basados en la tecnología Blockchain.

El enfoque exploratorio permite entender a fondo esta tecnología y sus aplicaciones, lo que es crucial antes de aplicarla en el proyecto de votación electrónica, con esto se valida conceptos y teorías relacionadas con la integración de Blockchain en la votación electrónica antes de una implementación completa, evitando costosos errores y optimizando la arquitectura del sistema. El objetivo principal es obtener una comprensión profunda de la temática y descubrir elementos novedosos y esenciales relacionados con seguridad y usabilidad que conlleva usar una tecnología segura para un proceso electoral.

2.1.3.2 Investigación Aplicada.

Posteriormente, la investigación se orientará hacia un enfoque aplicado, durante esta fase se proporciona la oportunidad de evaluar y medir el rendimiento real del sistema de votación electrónica basado en Blockchain en condiciones reales. Esto incluye la eficiencia, la velocidad y la seguridad del sistema, a la vez, urgen desafíos únicos y problemas específicos que solo se pueden identificar y abordar a través de la aplicación práctica. Esto incluye cuestiones de seguridad, escalabilidad y usabilidad.

La aplicación práctica permite adaptar la tecnología Blockchain a estos requisitos específicos y garantizar que el sistema cumpla con las necesidades de los usuarios y las regulaciones locales, a través de un enfoque aplicado, se pueden realizar ajustes y optimizaciones en tiempo real según los resultados y la retroalimentación obtenidos durante la implementación. Esto asegura que el sistema esté constantemente mejorando y adaptándose para alcanzar un rendimiento óptimo.

Con este enfoque se quiere aplicar la tecnología en un entorno simulado pero realista, se puede preparar al sistema y a los actores involucrados para escenarios reales de votación electrónica, mejorando la eficacia y la confianza en el proceso.

Se propondrán patrones de diseño para la estructura de los datos y el desarrollo de la interfaz, y se definirá la arquitectura del sistema. Una vez se tenga un prototipo funcional, se procederá a realizar pruebas para evaluar el funcionamiento básico del sistema. Se organizará una breve jornada de votaciones, simulando un escenario a pequeña escala similar a las elecciones presidenciales.

Después de finalizar la jornada de pruebas, se divulgarán los resultados y se analizará el rendimiento del sistema. Se propondrán cambios o mejoras en base a esta evaluación.

2.1.4 Fuentes y técnicas para la recolección de información

2.1.4.1 Definición de la población.

La población en este caso se compone de todos los posibles votantes y actores involucrados en el proceso de votación electrónica basado en blockchain. Esto incluye a los ciudadanos habilitados para votar en una elección presidencial de Ecuador. Con esto se definen criterios claros de inclusión y exclusión que determinen quiénes son considerados parte de la población y quiénes no. Por ejemplo, los ciudadanos de nacionalidad ecuatoriana mayores de edad y registrados para votar podrían estar incluidos, mientras que los menores de edad y ciudadanos extranjeros estarían excluidos.

2.1.4.2 Entrevista.

La elección de utilizar una entrevista como fuente de información para el desarrollo de esta plataforma de votación se basa en varios motivos estratégicos y que trae beneficios en todo el flujo de desarrollo del mismo, se consideran las siguientes razones:

Profundidad y Claridad en la Información: Una entrevista permite obtener información detallada y específica sobre el tema de la plataforma y la tecnología a usar. Se puede obtener respuestas claras y en profundidad sobre aspectos técnicos, funcionales y de diseño que pueden ser esenciales para la metodología.

Perspectiva de Expertos: Entrevistar a expertos en el campo de TI y la política puede proporcionar una perspectiva especializada y actualizada. Si nos enfocamos en esta población nos pueden ofrecer conocimientos y prácticas recomendadas que enriquecerán la metodología.

Validación de Hipótesis y Conceptos: La entrevista puede ayudar a validar las hipótesis o conceptos iniciales relacionados con la plataforma. Al obtener opiniones expertas, se pueden confirmar si las ideas propuestas son viables y eficaces.

Identificación de Desafíos y Soluciones Potenciales: Durante la entrevista, es probable que surjan desafíos o preocupaciones sobre la implementación de una aplicación en el contexto de la votación electrónica. Estos desafíos pueden ayudar a identificar áreas críticas y desarrollar soluciones adecuadas.

Adaptabilidad de la Metodología: Al obtener información cualitativa a través de entrevistas, puedes ajustar y adaptar la metodología según las ideas y sugerencias de los expertos. Esto asegura que la metodología sea sólida y efectiva en la práctica.

Contextualización y Personalización: Las entrevistas pueden proporcionar información contextual y personalizada sobre el entorno en el que se implementará la plataforma. Esto permite ajustar la metodología para que se adapte a las necesidades y desafíos específicos del contexto.

2.1.4.3 Análisis documental.

El análisis documental permite acceder a una amplia gama de documentos académicos, técnicos y científicos relacionados con la votación electrónica y la tecnología blockchain. Esto ayuda a establecer una sólida base teórica y conceptual para el desarrollo del aplicativo.

Es posible revisar de manera exhaustiva la literatura especializada sobre votación electrónica y blockchain. Esto incluye investigaciones previas, artículos, documentación de las tecnologías a usar, informes y otras fuentes relevantes que proporcionan información detallada y actualizada.

Adicionalmente, se pueden explorar casos de uso exitosos plataformas de votación electrónica basadas en blockchain en diversas partes del mundo. Estos casos de estudio proporcionan ideas, estrategias y enfoques efectivos que pueden inspirar y enriquecer este desarrollo.

2.1.4.4 Resultados e impactos esperados.

2.1.4.4.1 Resultados

- Mejorar las votaciones electorales presidenciales, automatizando el proceso de elecciones y brindando seguridad en el flujo de los datos
- Aumentar la seguridad al momento de emitir un voto, gracias a la tecnología blockchain que permite el cifrado de datos.
- Mantener el control de resultados que se van verificando en el proceso de votaciones.
- Emitir reporte de la elección electoral.
- Visualización del ganador de las elecciones, al finalizar el conteo de votos.

2.1.4.4.2 Impactos esperados.

- Certificar la seguridad y transparencia necesaria al instante de emitir un voto en el proceso electoral.
- Impedir la manipulación de la información de los votos por parte de terceros.
- Relativamente económico en comparación con el alto costo del material impreso utilizado en el proceso electoral.
- Que los votantes y candidatos sientan más confianza, utilizando el sistema de votaciones online, que realizando el proceso de forma manual.
- Acelerar el proceso de conteo de votos en las votaciones.

2.2 Metodología por objetivos.

La metodología por objetivos específicos es un enfoque que se centra en definir metas concretas y claras que se deben lograr en un proyecto o proceso. Estas metas específicas proporcionan una dirección clara y ayudan a medir el progreso y el éxito de la tarea en cuestión. A continuación, se describe cómo se implementó esta metodología:

2.2.1 Analizar las problemáticas actuales del proceso de votación, incluyendo la logística, el gasto y la transparencia en el sistema electoral.

Identificación de fuentes y datos relevantes: Se empezará recopilando información de diversas fuentes, como informes electorales, estudios académicos y opiniones de expertos en el campo. Esto nos permitirá obtener una visión integral de las problemáticas actuales relacionadas con la logística, el gasto y la transparencia en el sistema electoral.

Análisis de la logística electoral: Realizaremos un estudio detallado de la logística involucrada en el proceso de votación actual. Esto incluirá la identificación de los recursos humanos y materiales necesarios, los procedimientos de distribución y recolección de material electoral, y el tiempo requerido para llevar a cabo el proceso. También evaluaremos la efectividad de la logística actual en términos de eficiencia y costos.

Evaluación del gasto electoral: Analizaremos el gasto asociado al proceso electoral, incluyendo los costos de impresión de boletas, contratación de personal, transporte, alquiler de locales de votación, entre otros. Compararemos estos costos con alternativas tecnológicas, como la plataforma de votación electrónica que se va a desarrollar para determinar posibles ahorros y eficiencias.

Estudio de la transparencia en el sistema electoral: Investigaremos los mecanismos de supervisión y auditoría actuales en el proceso de votación para evaluar la transparencia del sistema. Analizaremos cómo se registran y verifican los votos, y

cómo se garantiza la integridad de los resultados. Además, revisaremos las medidas implementadas para prevenir fraudes y manipulaciones en el proceso.

Análisis comparativo: Realizaremos un análisis comparativo entre el proceso de votación actual y otras experiencias exitosas de implementación de votación electrónica en diferentes países. Esto nos permitirá identificar mejores prácticas y posibles soluciones a las problemáticas actuales.

Propuesta de recomendaciones: Con base en los resultados obtenidos, desarrollaremos un conjunto de recomendaciones para mejorar la logística, reducir el gasto y fortalecer la transparencia en el sistema electoral. Estas recomendaciones estarán orientadas a optimizar el proceso de votación, fomentar la participación ciudadana y garantizar la confianza en el sistema.

Resultados esperados

El resultado esperado es obtener una comprensión exhaustiva y documentada de la situación actual del sistema electoral, centrándose en la logística, los costos asociados y la transparencia del proceso. Esto se traducirá en una serie de recomendaciones sustentadas en datos y experiencias comparativas, que buscan mejorar la eficiencia, reducir el gasto y fortalecer la confianza en el sistema electoral. Estas recomendaciones estarán diseñadas para ser implementadas en la futura plataforma de votación electrónica, buscando así una modernización efectiva y confiable del sistema de votación.

2.2.2 Identificar los posibles desafíos y riesgos asociados con la automatización de los procesos electorales, como la seguridad de los datos y la protección de la privacidad de los votantes.

Revisión bibliográfica: Realizaremos una revisión exhaustiva de la literatura científica y técnica relacionada con la automatización de procesos electorales. Analizaremos estudios y casos de implementaciones previas en otros países para identificar los desafíos y riesgos comunes asociados con esta tecnología.

Análisis de vulnerabilidades: Realizaremos un análisis de vulnerabilidades potenciales en un sistema de votación automatizado. Investigaremos las posibles brechas de seguridad y las vulnerabilidades de los sistemas tecnológicos que podrían ser explotadas por actores maliciosos.

Simulaciones y pruebas de seguridad: Realizaremos simulaciones y pruebas de seguridad en un entorno controlado para evaluar la robustez del sistema de votación automatizado. Pondremos a prueba el sistema contra ataques cibernéticos e intentos de manipulación para identificar posibles debilidades.

Evaluación de la protección de datos: Analizaremos las medidas implementadas para garantizar la protección de los datos de los votantes. Revisaremos los protocolos de seguridad y encriptación utilizados para asegurar que la información de los votantes esté protegida de cualquier acceso no autorizado.

Evaluación de la confidencialidad de los electores: Investigaremos la salvaguarda de la privacidad de los votantes en un sistema de votación automatizado. Analizaremos las políticas y prácticas implementadas para asegurar que el sufragio de cada ciudadano sea confidencial y no pueda ser rastreado hasta el votante.

Evaluación del procedimiento de confirmación y examen: Examinaremos cómo se lleva a cabo la confirmación y examen del sistema de votación automatizado para garantizar la transparencia e integridad del proceso. Revisaremos los mecanismos de confirmación y las oportunidades para que los ciudadanos y las autoridades electorales puedan examinar el sistema.

Análisis comparativo: Realizaremos un análisis comparativo entre diferentes sistemas de votación automatizados utilizados en otros países para identificar desafíos comunes y soluciones implementadas.

Definir el prototipo y simulación que pueda mostrar las características principales para llevar a cabo un proceso electoral.

Definición de requisitos: Identificar y definir los requisitos y características principales que debe tener el prototipo de plataforma de votación electrónica. Esto incluirá aspectos como seguridad, usabilidad, transparencia y accesibilidad para garantizar una representación adecuada del proceso electoral, así como las tecnologías que se usarán para desarrollar el prototipo, las mismas que deben ser reconocidas y ayudar a la seguridad y fácil integración con varios servicios a futuro.

Tecnologías a usar:

- Blockchain
- Solidity
- ReactJs
- NodeJs
- AWS
- MySQL

Diseño de la arquitectura: Crear un diseño detallado de la arquitectura del prototipo, incluyendo la infraestructura tecnológica, el diseño de la base de datos, patrones de diseños, diagramas de flujos para identificar todo el proceso que tendrá la aplicación desde que los votantes y administradores entran a la plataforma, así como los componentes de seguridad necesarios para el funcionamiento seguro y confiable del sistema.

Desarrollo del prototipo: Implementar el prototipo de la plataforma de votación electrónica basado en el diseño de la arquitectura. Asegurarse de que todas las

características y requisitos definidos anteriormente se integren correctamente y funcionen de manera coherente.

Integración de mecanismos de seguridad: Incluir mecanismos avanzados de seguridad para resguardar la rectitud de los datos de los votantes y prevenir posibles ataques cibernéticos o manipulaciones en el sistema.

Creación de la simulación: Desarrollar la simulación interactiva utilizando el prototipo. Esta simulación debe permitir a los usuarios experimentar el proceso electoral completo, desde la inscripción de votantes hasta el anuncio de resultados, para mostrar de manera realista cómo funciona la plataforma en un proceso electoral real.

Pruebas y ajustes: Realizar pruebas exhaustivas del prototipo y la simulación para detectar posibles errores o fallos en el sistema. Realizar ajustes y mejoras según sea necesario para garantizar un funcionamiento fluido y confiable.

Validación con expertos: Obtener la validación y retroalimentación de expertos en tecnología, seguridad informática para asegurarse de que el prototipo y la simulación cumplan con los estándares requeridos y se ajusten a las necesidades del proceso electoral.

Resultados esperados

Al finalizar este proceso, se espera contar con un prototipo funcional de una plataforma de votación electrónica basada en tecnología blockchain y diseñada con un enfoque de seguridad. El prototipo debe representar de manera efectiva el proceso electoral, desde la inscripción de votantes hasta la revelación de los resultados finales. Además, la simulación interactiva asociada debe permitir a los usuarios experimentar y comprender de manera práctica cómo se desarrolla un proceso electoral utilizando esta plataforma.

La arquitectura detallada deberá mostrar una infraestructura tecnológica, una base de datos segura, patrones de diseño eficaces y un flujo de aplicación coherente. La

integración de mecanismos de seguridad avanzados será esencial para certificar la protección de los datos de los votantes y la desconfianza de posibles amenazas cibernéticas.

2.2.3 Definir el prototipo y simulación que pueda mostrar las características principales para llevar a cabo un proceso electoral.

La concepción para este prototipo y su simulación juega un papel fundamental en el marco del desarrollo de este proyecto de votación. Estos elementos resultan cruciales al permitir una representación práctica de las características y funcionalidades clave del sistema antes de su plena ejecución. Enseguida, se detalla un enfoque metodológico para la definición del prototipo:

Definición de Prototipo

Identificación de Requisitos del Prototipo:

En esta fase, se inicia con la identificación y establecimiento de los requisitos y atributos esenciales que el prototipo debe incorporar. Esto engloba cuestiones de seguridad, usabilidad, transparencia y accesibilidad.

Elección de Tecnologías Apropriadas:

El siguiente paso radica en la selección de las tecnologías idóneas para llevar a cabo la implementación. En el contexto de un sistema de votación electrónica, esto implica la selección de las herramientas y marcos de trabajo pertinentes para el desarrollo.

Elaboración de la Arquitectura del Prototipo:

Con la elección de tecnologías como fundamento, se procede a la creación de un diseño detallado de la arquitectura. Esto abarca la infraestructura tecnológica, la estructura de la base de datos y los patrones de diseño a aplicar.

Desarrollo del Prototipo:

La fase siguiente corresponde a la implementación del prototipo siguiendo el diseño arquitectónico. Las características y funcionalidades definidas en los requisitos se incorporan en el sistema.

Integración de Mecanismos de Seguridad Avanzados:

Se integran mecanismos de seguridad de vanguardia destinados a salvaguardar la integridad de los datos de los votantes y a prevenir eventuales amenazas cibernéticas o manipulaciones del prototipo.

Creación de la Simulación:

Se desarrolla una simulación basada de cómo se realiza una votación en la vida real, como punto de partida. La simulación se concibe como un entorno interactivo que permite a los usuarios experimentar la totalidad del proceso electoral, desde el registro de votantes hasta la presentación de los resultados.

Ejecución de Pruebas y Ajustes:

Se efectúan pruebas meticulosas de lo ya desarrollado y la simulación con el propósito de identificar posibles fallos o errores en el sistema. Cualquier inconveniente detectado se corrige, y se llevan a cabo ajustes según sea necesario.

Validación con Expertos:

La validación y la retroalimentación de expertos en tecnología y seguridad informática desempeñan un papel esencial para confirmar que el prototipo y la simulación cumplen con los estándares requeridos y se adaptan a las necesidades inherentes al proceso electoral.

Documentación y Presentación:

El proceso de desarrollo del prototipo y la simulación se documenta en su totalidad, incluyendo los pormenores técnicos y las enseñanzas extraídas. Posteriormente, se lo presenta junto con la simulación a las partes interesadas.

Iteración y Mejora:

En caso de ser necesario, se emprenden iteraciones en el prototipo y la simulación para abordar cualquier retroalimentación o recomendación de mejora obtenidas desde las entrevistas o encuestas que se realizaran.

2.2.4 Probar el prototipo con respecto a seguridad y privacidad de los datos

Identificación de requisitos de seguridad: Definir los requisitos de seguridad y privacidad que deben cumplirse en el prototipo, incluyendo medidas de autenticación, encriptación, control de acceso, anonimato de votantes y protección contra ataques cibernéticos.

Evaluación de la arquitectura de seguridad: Realizar una revisión detallada de la arquitectura del prototipo para evaluar si se han implementado adecuadamente los mecanismos de seguridad y si cumplen con los estándares requeridos.

Penetration testing (Pruebas de penetración): Realizar pruebas de penetración en el prototipo para identificar posibles vulnerabilidades y brechas de seguridad. Estas pruebas simulan ataques cibernéticos con el fin de evaluar la resistencia del sistema ante posibles amenazas. Se desarrollarán pruebas unitarias y de integración de los contratos inteligentes, estos son una característica esencial en esta tecnología, ya que permiten la automatización de transacciones y acuerdos entre partes sin la necesidad de intermediarios. Aquí entra en juego la calidad de las pruebas unitarias en los contratos inteligentes. Las pruebas unitarias admiten evidenciar si un módulo individual del contrato marcha como se espera, nivelando los posibles problemas. (Sánchez González, 2023)

Análisis de riesgos: Identificar y analizar los posibles riesgos relacionados con la seguridad y privacidad de los datos en el prototipo. Priorizar los riesgos en función de su impacto potencial y probabilidad de ocurrencia.

Evaluación de la privacidad de los datos: Analizar cómo se protege la privacidad de los datos de los votantes en el prototipo. Verificar que el sistema garantice el anonimato del voto y que la información personal de los votantes esté debidamente protegida.

Pruebas de carga, estabilidad y estrés: Realizar pruebas de carga y estabilidad para asegurar que el prototipo pueda manejar una alta concurrencia de votantes sin comprometer la seguridad y privacidad de los datos.

Revisión de políticas y procedimientos: Evaluar las políticas y procedimientos establecidos para la gestión y protección de datos en el prototipo. Asegurarse de que se cumplan con las normativas legales y estándares de privacidad.

Resultados esperados

Se espera haber identificado, implementado y probado de manera efectiva los requisitos de seguridad y privacidad en el prototipo de la plataforma de votación electrónica basada en tecnología blockchain. Esto implica:

Requisitos de Seguridad y Privacidad Bien Definidos:

Especificación clara de medidas de autenticación, encriptación, control de acceso y anonimato de votantes que cumplen con los estándares de seguridad y privacidad.

Arquitectura de Seguridad Evaluada y Validada:

Una arquitectura de seguridad revisada y validada que asegura la protección de los datos y garantiza la integridad y confidencialidad del proceso electoral.

Resultados de Pruebas de Penetración:

Un informe detallado de las pruebas de penetración que identifica vulnerabilidades y brechas de seguridad, junto con acciones correctivas para abordarlas.

Análisis de Riesgos y Mitigación:

Identificación de riesgos y un plan de mitigación para abordar los posibles problemas de seguridad, priorizando en función del impacto y probabilidad de ocurrencia.

2.3 Usabilidad.

La usabilidad abarca las condiciones que simplifican el proceso de votación para todos los involucrados en la red de votación, desde los administradores hasta los electores. También engloba las facilidades que el sistema ofrece para agilizar la votación. Este aspecto es de vital importancia, ya que la facilidad de acceso al sistema de votación puede aumentar de forma significativa la cantidad de personas que participan. La herramienta presenta una interfaz de usuario que es fácil de utilizar, intuitiva y clara. Además, aprovecha las comodidades conocidas de Internet, lo que permite a los usuarios participar en las elecciones desde cualquier dispositivo con acceso a la red. Con esto tenemos en cuenta que la usabilidad se refiere a la evaluación de cuán fácil es utilizar un producto tecnológico, considerando el nivel de satisfacción, el interés, la accesibilidad y la comprensión que el usuario tiene del producto generado. (Pailiacho Mena, Garcés Freire, & Balseca Manzano, 2022)

La usabilidad se configura como una cualidad indispensable para potenciar la efectividad, eficiencia y satisfacción en la interacción con el usuario. Este enfoque busca asegurar estrategias que posibiliten la entrada a los servicios informativos por parte de variados grupos de interés, teniendo en cuenta aspectos de accesibilidad y resguardo. La facilidad de uso se erige como un pilar fundamental para lograr esta

relación efectiva y eficiente con el usuario. (Pailiacho Mena, Garcés Freire, & Balseca Manzano, 2022)

2.3.1 Análisis de la usabilidad.

Siguiendo con el proceso de análisis, es esencial abordar el concepto de facilidad de uso, que se refiere a la simplicidad que una plataforma web brinda a los usuarios que la utilizan. En este sentido, las páginas web con buena facilidad de uso son aquellas cuyo diseño y desarrollo se centran en las necesidades de los usuarios, evitando complicaciones al utilizarlas.

Para llevar a cabo este análisis, aplicaré las "heurísticas de usabilidad", que implican identificar los principios heurísticos. En este caso, utilizaré los principios de la lista elaborada por Jakob Nielsen y los aplicaré en la aplicación para evaluarla.

2.3.2 Métodos de usabilidad.

Un método para evaluar la usabilidad puede ser descrito como un conjunto de procedimientos claramente definidos con el objetivo de adquirir información relevante sobre la interacción entre un software y el usuario final. Esto permite verificar cómo las características específicas de dicho software contribuyen a alcanzar un nivel determinado de usabilidad. Así, es posible identificar problemas de usabilidad al examinar en detalle las interfaces gráficas.

Jakob Nielsen, una figura destacada en el estudio de la usabilidad, nos explica que "la usabilidad es una característica que determina cuán fácil es para el usuario utilizar las interfaces gráficas de un producto de software en particular". Además, destaca que la usabilidad se basa en cinco aspectos principales (Nielsen, 2006)

- 1) **Facilidad de Aprendizaje:** El sistema debe permitir al usuario adquirir rápidamente el conocimiento necesario para interactuar cómodamente con él.
- 2) **Eficiencia:** Se refiere a la rapidez con la que el usuario puede llevar a cabo tareas en el sistema una vez que se ha familiarizado con este.

- 3) Memorabilidad: Hace referencia a qué tan fácil es para el usuario volver a interactuar con el sistema después de una etapa sin usarlo.
- 4) Manejo de Errores: El software debe evitar en la medida de lo posible que los usuarios cometan errores. En caso de errores, deben ser mínimos y el sistema debe permitir su recuperación, evitando la presencia de errores graves en el sistema.
- 5) Satisfacción: Indica qué tan placentera ha sido la experiencia de uso para el usuario durante su interacción con el sistema.

2.3.2.1 Evaluación Heurística.

Un método de evaluación, en el cual profesionales especializados en usabilidad evalúan si cada uno de los componentes de una interfaz gráfica para usuarios cumple con un conjunto de reglas heurísticas. Este método es ampliamente empleado dada su menor costo en comparación con otros enfoques. Según Nielsen, contar con un máximo de cinco expertos es adecuado para identificar la mayoría de los problemas de usabilidad presentes en una interfaz. (Nielsen, 2006).

El método de evaluación heurístico se basa en la utilización de un conjunto de principios de usabilidad que orientan a los evaluadores en cuanto examinan una interfaz en busca de problemas y deficiencias.

Se hallan numerosas reglas heurísticas utilizables, siendo que, dos expertos en usabilidad convocaron esas heurísticas en apenas diez reglas con el objetivo de proporcionar la evaluación situadas en práctica, nombradas de reglas Heurísticas de Nielsen.

Reglas Heurísticas Preguntas	Preguntas
H1 - Visibilidad del estado del sistema	¿Los usuarios son instruidos sobre el progreso del sistema con la respuesta oportuna y dentro de un tiempo admisible?
H2 - Correspondencia entre la interfaz del sistema y el mundo real	¿El sistema utiliza conceptos y lenguaje familiares a los usuarios en lugar de términos técnicos? ¿El sistema utiliza convenciones del mundo real y presenta las informaciones de manera natural y en orden lógico?
H3 - Control del usuario y libertad	¿Los usuarios pueden hacer lo que quieran y cuando lo desean?
H4 - Consistencia y estándares	¿Los elementos de diseño, como los objetos y las acciones, tienen el mismo significado o efecto en situaciones diferentes?
H5 - Prevención de errores	¿Los usuarios podrían cometer errores que no cometerían en mejores interfaces?
H6 - Reconocimiento en vez de recordación	¿Los elementos del proyecto, como los objetos, las acciones y las opciones, están visibles? ¿El usuario es forzado a recordar informaciones de una parte para otra del sistema?

H7 - Flexibilidad y eficiencia de utilización ¿Los métodos de las tareas son eficientes? ¿Los usuarios pueden personalizar las	¿Los métodos de las tareas son eficientes? ¿Los usuarios pueden personalizar las acciones frecuentes o los atajos?
H8 - Estética y diseño minimalista	¿Los diálogos contienen informaciones irrelevantes o raramente utilizadas?
H9 - Ayuda a los usuarios a reconocer, diagnosticar y recuperarse de errores	¿Los mensajes de error son expresados en lenguaje simple (sin códigos)? ¿Estos describen el problema exactamente y sugieren una solución?
H10 - Ayuda y documentación	¿Se suministra una ayuda apropiada? ¿Esa información es fácil de ser encontrada y enfocada en la tarea del usuario?

Tabla 1: Reglas Heurísticas de Nielsen

Esta se debe ejecutar de la siguiente manera:

Fase I: Cada elector, apoyándose en un conjunto de pautas heurísticas, analiza minuciosamente las interfaces visuales del software. Durante este proceso, registran cualquier problema identificado y será organizado según la norma de usabilidad no cumplida.

Fase II: Tras la evaluación individual del sistema por parte de los electores, se congregan para generar de manera convenida una única lista de inconvenientes de usabilidad, clasificándolos según el principio de usabilidad vulnerado.

Fase III: La lista de desafíos de usabilidad identificados en el paso previo será enviada a cada uno de los evaluadores, quienes evaluarán la frecuencia, gravedad

y nivel de criticidad de cada problema. Para este propósito, se utilizarán las escalas propuestas por Nielsen.

Escala de severidad para la evaluación heurística.

Puntuación	Severidad
1	No es un problema de usabilidad.
2	Es un problema estético. No tiene prioridad
3	Es un problema menor. Tiene baja prioridad.
4	Es un problema mayor. Tiene una alta prioridad para ser resuelto.
5	Catástrofe de usabilidad. Tiene que ser resuelto de inmediato

Fuente: (de Carvalho, Martinez Évora, & Zem-Mascarenhas, 2016)

Escala de frecuencia para la evaluación heurística.

Puntuación	Frecuencia
1	Presente con una frecuencia menor al 1%
2	Presente con una frecuencia entre 1% y 10 %
3	Presente con una frecuencia entre 11 % y 50 %
4	Presente con una frecuencia entre 51 % y 90 %
5	Presente con una frecuencia mayor a 90 %

Fuente: (de Carvalho, Martínez Évora, & Zem-Mascarenhas, 2016)

Las escalas significan lo siguiente:

Escala de Gravedad: Indica el nivel de complicación del problema de usabilidad identificado. Así, se pueden identificar obstáculos que afectan negativamente el desempeño óptimo de la interfaz del producto.

Escala de Frecuencia: Hace referencia al grado de aparición del problema de usabilidad detectado. Por ende, permite determinar cuáles problemas son más habituales o recurrentes en la interfaz del software.

Escala de Importancia: Se obtiene al combinar la gravedad y la frecuencia. De este modo, se puede determinar cuáles problemas tienen mayor relevancia y deben abordarse con prontitud para su pronta corrección.

Fase IV: En última instancia, luego de evaluar la lista de problemas de usabilidad en relación con su gravedad y frecuencia, los resultados serán entregados al líder

del equipo de desarrollo. Este líder calculará el promedio de los resultados y los organizará según su importancia.

ANALISIS EN INTERPRETACIÓN DE RESULTADOS
CAPITULO III

CAPITULO III: ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

3.1 Descripción de los resultados.

En este capítulo, nos centramos en la evaluación y análisis de resultados que nos dejó el test de usabilidad del sistema de votación electrónica a través del uso de los 10 principios heurísticos de Nielsen y a su vez, las respectivas entrevistas que se realizó en primer lugar a un profesional involucrado en los procesos electorales actuales y a una persona involucrada en TI para dar su punto de vista en cuanto a la tecnología Blockchain.

Empezaremos con los principios heurísticos, estos representan directrices fundamentales que se aplican a la usabilidad de sistemas e interfaces. La evaluación se basa en la interpretación y análisis de los resultados obtenidos a partir de un cuestionario diseñado en función de estos principios. A continuación, se exponen estos 10 principios heurísticos de Nielsen:

Visibilidad del estado del sistema: El sistema debe proporcionar retroalimentación clara sobre el estado del proceso de votación en todo momento.

Emparejamiento entre el sistema y el mundo real: Las acciones y opciones en el sistema deben corresponder intuitivamente con las acciones y expectativas del votante en el mundo real.

Control y libertad del usuario: Los votantes deben tener la capacidad de corregir errores, deshacer acciones y navegar de manera flexible por el proceso de votación.

Estabilidad y estándares: El sistema debe alcanzar estándares y convenciones de diseño reconocidos y mantener una interfaz y funcionamiento consistentes.

Prevención de errores: El sistema debe incluir características de diseño que ayuden a prevenir errores, como confirmaciones antes de acciones críticas.

Reconocimiento en lugar de recuerdo: El sistema debe minimizar la carga de memoria del votante, mostrando información relevante en el momento adecuado en lugar de requerir que recuerde información previamente vista.

Flexibilidad y eficacia de uso: El sistema debe ofrecer atajos y opciones avanzadas para usuarios experimentados sin abrumar a los usuarios novatos.

Diseño estético y minimalista: El sistema debe presentar información y opciones de manera clara y sin distracciones innecesarias.

Asistencia a los usuarios a examinar, precisar y recuperarse de errores: El sistema debe brindar mensajes de error claros y soluciones para ayudar a los votantes a superar problemas.

Ayuda y documentación: Se debe proporcionar acceso fácil a la información de ayuda y documentación para los votantes cuando sea necesario.

La evaluación de usabilidad se llevará a cabo a través de la aplicación de estos principios heurísticos, y se recopilarán datos a través de un cuestionario diseñado específicamente para este propósito.

3.1.1 Planificación

En esta etapa, se llevarán a cabo las siguientes actividades: la definición de la unidad de análisis y la creación del instrumento para la recolección de datos. La unidad de análisis seleccionada es: "Evaluar la usabilidad de un sistema de votación electrónica a través de los 10 principios heurísticos de Nielsen".

La actividad subsiguiente implica la creación de los instrumentos necesarios para recopilar datos. En este contexto, se han elaborado dos cuestionarios distintos basados en el enfoque propuesto por Nielsen y sus 10 principios heurísticos de usabilidad. Estos principios proporcionan directrices fundamentales para evaluar la habilidad de uso y la eficacia de un sistema de votación electrónica.

A continuación, se presenta la matriz que ha sido empleada para definir las preguntas que serán incluidas en el cuestionario de evaluación de usabilidad.

Tabla 2: Definición de las preguntas del cuestionario por dimensión.

Modelo	Dimensiones	Variables	Items
Modelo Heurístico De Nielsen	Visibilidad del estado del sistema	Mantener a cualquier usuario informado sobre lo que sucede	1) ¿Pudiste identificar fácilmente el estado actual del proceso de votación en la plataforma? 2) ¿Te resultó claro saber en qué etapa del proceso de votación te encontrabas en todo momento?
	Correspondencia entre el Sistema y el Mundo Real	Los usuarios comprenden la información sin necesidad de buscar el significado	3) ¿La terminología y los botones utilizados en la plataforma eran comprensibles y

			<p>correspondían con el proceso de votación real?</p> <p>4) ¿Le resultó fácil entender cómo transferir sus decisiones y preferencias reales a la plataforma?</p>
Control y Libertad para el Usuario	Posibilidad de poder deshacer y rehacer la acción		<p>5) ¿Sintió que tenía el control sobre el proceso de votación y podía realizar cambios antes de confirmar tu voto?</p> <p>6) ¿Pudo volver atrás o modificar su elección de voto de manera sencilla si así lo deseaba?</p>
Consistencia y Estándares	Diferentes situaciones o		<p>7) ¿Notó que existía</p>

	acciones significan lo mismo	consistencia en el diseño y la forma en que se presentaban las opciones a lo largo de la plataforma? 8) ¿La plataforma seguía un patrón estándar que facilitó su navegación y comprensión del proceso de votación?
Prevención de Errores	Eliminar condiciones que sean propensas al error	9) ¿La plataforma incluyó medidas para evitar que cometa errores durante el proceso de votación? 10) ¿Hubo alguna característica que le impidiera o advirtiera

			sobre posibles errores en su elección antes de confirmar el voto?
Reconocimiento en lugar de Recordar	Reducir la información que un usuario tiene que recordar		<p>11) ¿La plataforma presentó opciones o recordatorios visuales que le ayudaron a reconocer las acciones que debía realizar en lugar de tener que recordarlas?</p> <p>12) ¿Fue fácil para usted reconocer las opciones disponibles en cada paso del proceso de votación?</p>
Flexibilidad y Eficiencia de Uso	Permitir a los usuarios adaptar las acciones frecuentes		13) ¿Sintió que la plataforma le permitía votar de manera eficiente,

			<p>adaptándose a sus preferencias y necesidades?</p> <p>14) ¿La plataforma le ofreció opciones para personalizar su experiencia de votación y hacerla más eficiente?</p>
Estética y Diseño Minimalista	Priorizar el contenido y sus características		<p>15) ¿Encontró el diseño de la plataforma atractivo y fácil de entender durante el proceso de votación?</p> <p>16) ¿Considera que el diseño minimalista de la plataforma contribuyó a una experiencia de votación más clara y organizada?</p>

<p>Ayudar a los Beneficiarios a Registrar, Determinar y Recuperarse de Errores</p>	<p>Mensajes de error deben expresarse en un lenguaje sencillo</p>	<p>17) ¿La plataforma proporcionó mensajes claros y soluciones para ayudarle a entender y corregir posibles errores durante la votación?</p> <p>18) ¿Se sintió respaldado/a por la plataforma para corregir cualquier error que pudiera haber cometido durante el proceso de votación?</p>
<p>Ayuda y Documentación</p>	<p>Evitar que el usuario se pierda</p>	<p>19) ¿Encontró disponible alguna forma de ayuda o documentación que le asistiera en caso de</p>

			<p>necesitar información adicional durante la votación?</p> <p>20) ¿Considera que la información de ayuda disponible fue útil y fácil de acceder en caso de requerirla?</p>
--	--	--	---

3.1.2 Recolección de datos.

3.1.2.1 Encuesta (Test de usabilidad)

En esta fase, se procedió a la aplicación de dos cuestionarios utilizando la plataforma Google Forms a un grupo de 10 personas con diferentes ocupaciones. Los cuestionarios fueron dirigidos a un rango de edad entre 18 – 60 años que utilizaron el módulo de votante para ejercer su voto, mientras que el segundo se aplicó a 2 personas que hicieron uso del módulo de administrador para gestionar las elecciones.

En promedio, los cuestionarios tomaron aproximadamente 3 minutos y 30 segundos para ser completados por los electores y 6 minutos y 10 segundos para los administradores.

3.1.2.2 Entrevista I.

Se realizó la entrevista a una persona que ha participado dentro de procesos electorales en los últimos años y labora dentro del consejo nacional electoral como analista de participación política.

Resumen.

En esta entrevista se aborda la implementación de la tecnología en los procesos electorales, destacando su complejidad y el potencial de ofrecer ventajas en eficiencia y accesibilidad si se gestiona adecuadamente. Sin embargo, se resalta la importancia de abordar preocupaciones relacionadas con la seguridad y privacidad de los datos electorales.

Se enfatiza sobre la necesidad de garantizar la integridad del sistema electoral mediante la implementación de tecnologías que protejan los datos y prevengan posibles abusos de poder. La confianza en la tecnología electoral se construye a través de la participación ciudadana, supervisión independiente y revisiones constantes de los sistemas.

Se mencionan medidas como auditorías independientes y cifrado en seguridad de red como fundamentales para la transparencia y confiabilidad del sistema de votación electrónica. Además, se destaca la importancia de la confidencialidad y el anonimato de los electores, así como la necesidad de medidas de seguridad robustas y cumplimiento de normativas de privacidad.

Se abordan desafíos como la resistencia al cambio, costos y financiamiento, destacando la necesidad de colaboración entre partidos políticos, expertos en tecnología y la sociedad civil para asegurar elecciones justas y seguras. Se resalta la importancia de un enfoque integral que involucre a gobiernos, partidos políticos, organizaciones de la sociedad civil y otros actores relevantes.

Así mismo se habla sobre que la participación ciudadana, la colaboración y la facilitación del acceso a la información son clave para lograr un proceso electoral

inclusivo y equitativo. Se reconoce que la interoperabilidad y la colaboración son pilares clave para fortalecer la confianza del público y la democracia.

En última instancia, se destaca la importancia de la transparencia, participación ciudadana, seguridad, educación y mejora continua para abordar críticas y desconfianzas hacia la tecnología en los procesos electorales y construir confianza en la integridad de las elecciones. Se enfatiza el papel crucial de los partidos políticos en la toma de decisiones y discusiones sobre la implementación de sistemas de votación electrónica.

3.1.2.3 Entrevista II.

En esta segunda entrevista se hizo tuvo una reunión con una persona que tiene como cargo el de desarrollador de software y ha tenido algunos años de experiencia en el área, así como en el último año haber tenido la oportunidad de realizar desarrollos con Blockchain y así tener una mejor perspectiva de como se hace un desarrollo de tal magnitud.

En esta entrevista, se discute la aplicación de la tecnología blockchain en el contexto de elecciones o votaciones. Se destaca que la blockchain, al ser un sistema descentralizado y seguro, puede prevenir fraudes electorales gracias a su transparencia e inmutabilidad.

Se toca el tema sobre la importancia de la seguridad y la privacidad en la implementación de la tecnología blockchain en procesos electorales. Se menciona que la criptografía robusta es esencial para proteger la integridad de los votos y prevenir manipulaciones. A pesar de los temores legítimos sobre la vulnerabilidad ante ataques cibernéticos, se considera que la tecnología blockchain sería bien recibida si se abordan cuidadosamente los aspectos técnicos y de seguridad.

En términos de accesibilidad, se visualiza un sistema inclusivo y fácil de usar, con una interfaz intuitiva y opciones adaptables para garantizar la participación de todas las personas, incluidas aquellas con discapacidades.

La implementación de la tecnología blockchain podría hacer el proceso electoral más sencillo y conveniente, permitiendo a los ciudadanos votar desde sus hogares y aumentando la participación electoral. La posibilidad de confirmar de manera segura que el voto ha sido registrado correctamente añade un nivel adicional de confianza en el proceso.

La entrevista resalta que la capacidad de confirmar el voto de manera anónima y retirar el consentimiento, respaldado por medidas de seguridad robustas, preservaría la privacidad de los votantes. Además, se sugiere que la implementación de la tecnología blockchain podría aumentar la motivación para participar en elecciones y votaciones, especialmente debido a la conveniencia y la confianza en la integridad del proceso.

Aunque se reconoce que la educación sobre el funcionamiento del sistema es crucial, se considera que el diseño cuidadoso y un enfoque inclusivo pueden superar los desafíos asociados con la implementación de la tecnología blockchain en procesos electorales. En resumen, la tecnología blockchain se presenta como una herramienta prometedora para fortalecer la confianza y la integridad en los sistemas electorales.

3.2 Análisis de resultados

3.2.1 Población.

La población considerada para el desarrollo de este proyecto incluye a los ciudadanos ecuatorianos, en este caso la ciudad de Guayaquil-Ecuador, ellos participaron en el proceso de votación simulado del prototipo a desarrollar. Con esta población se realizó una encuesta, la cual consto de 13 preguntas sobre los principios de usabilidad de Nielsen

3.2.2 Muestra.

La muestra es exploratoria debido a que la población descrita anteriormente fue tomada de un cierto número de estudiantes, docentes y profesionales en el área de TI y la política con el objetivo de explorar ideas, conceptos o fenómenos en profundidad y con el enfoque principal de adquirir una comprensión inicial y profunda de la tecnología aplicada en este proyecto.

Esta muestra es a nivel de usabilidad ya que se hace referencia a un conjunto de usuarios seleccionados para participar en pruebas o evaluaciones de usabilidad. Esta es crucial para obtener retroalimentación significativa sobre cómo los usuarios interactúan con la plataforma y para identificar posibles problemas de usabilidad, a la vez ayuda a asegurar que las evaluaciones no estén sesgadas hacia un grupo específico de usuarios y que el producto sea accesible y utilizable para una variedad de personas.

3.2.3 Análisis de las respuestas obtenidas.

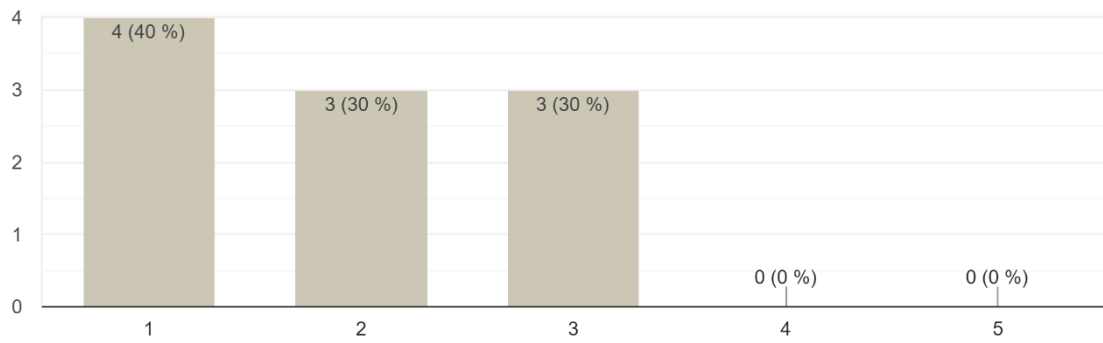
3.2.3.1.1.1 Análisis de encuesta.

Se obtuvieron 200 respuestas en total cubriendo los diez principios de Nielsen para medir la usabilidad.

Pregunta No.1 :

¿Pudiste identificar fácilmente el estado actual del proceso de votación en la plataforma?

10 respuestas

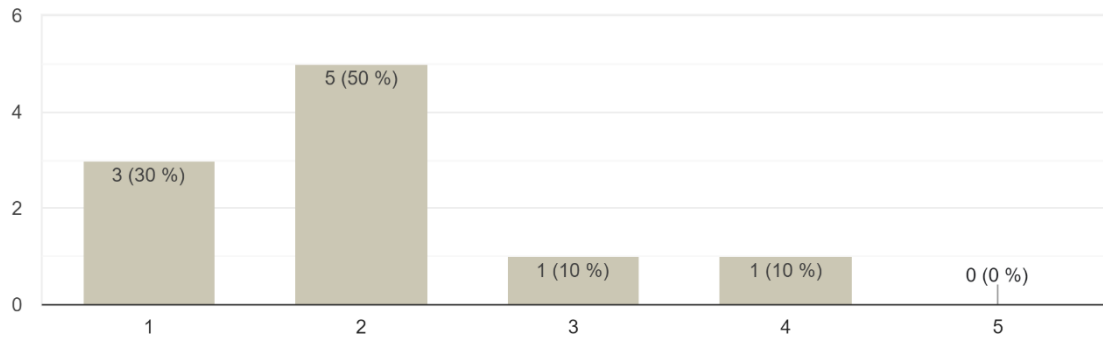


De acuerdo con los encuestados, en esta pregunta se puede interpretar que el 40% de encuestados han podido identificar de manera fácil como se maneja el estado del proceso de votación, el resto dio a conocer que es más un problema estético y que no tiene prioridad en ser implementado.

Pregunta No. 2:

¿Te resultó claro saber en qué etapa del proceso de votación te encontrabas en todo momento?

10 respuestas

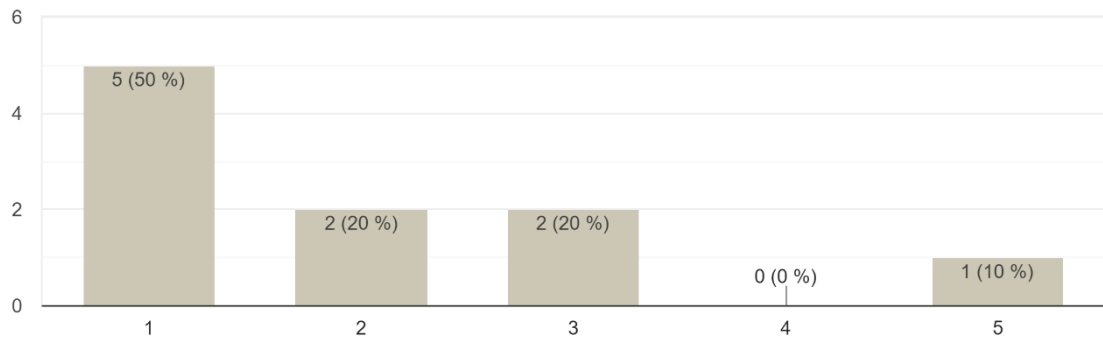


De acuerdo con los resultados, en esta pregunta se puede interpretar que el 30% de encuestados han tenido claro desde un inicio el cómo se maneja el proceso de votación en la plataforma, el 60% dio a conocer que es más un problema estético y que no tiene prioridad el ser implementado y con un 10% nos indica que es un problema mayor a su vez tiene una alta prioridad para ser resuelto.

Pregunta No. 3:

¿La terminología y los botones utilizados en la plataforma eran comprensibles y correspondían con el proceso de votación real?

10 respuestas

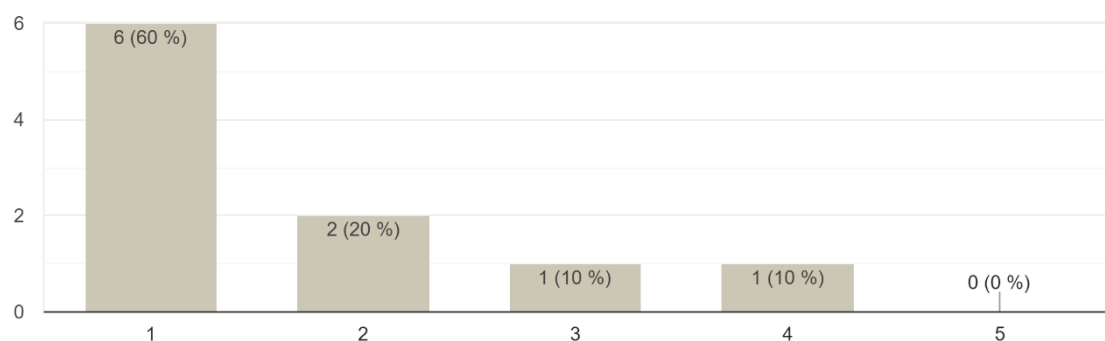


En relación con los resultados obtenidos de esta pregunta, se puede observar como el formato, terminología, gramática y los botones utilizados para cada proceso de votación eran comprensibles, ya que se cuenta con un 50%, un 40% indica que hay un problema de estética en ciertas zonas de la plataforma pero que no es algo prioritario su implementación. Así como existe un 10% que indica que los botones no eran lo suficientemente comprensibles para el proceso de votación.

Pregunta No.4:

¿Le resultó fácil entender cómo transferir sus decisiones y preferencias reales a la plataforma?

10 respuestas

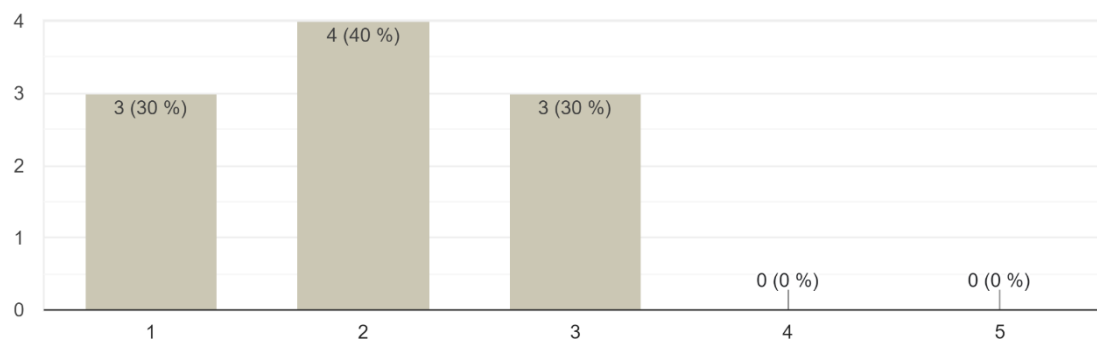


De acuerdo con el análisis de esta pregunta, se puede observar que el 60% de la población indica que le fue muy fácil tomar decisiones dentro de la plataforma, un 30% indica que es un problema menor, pero tiene baja prioridad y un 10% detalla que es un problema que debe ser resuelto lo más pronto posible.

Pregunta No.5:

¿Sintió que tenía el control sobre el proceso de votación y podía realizar cambios antes de confirmar tu voto?

10 respuestas

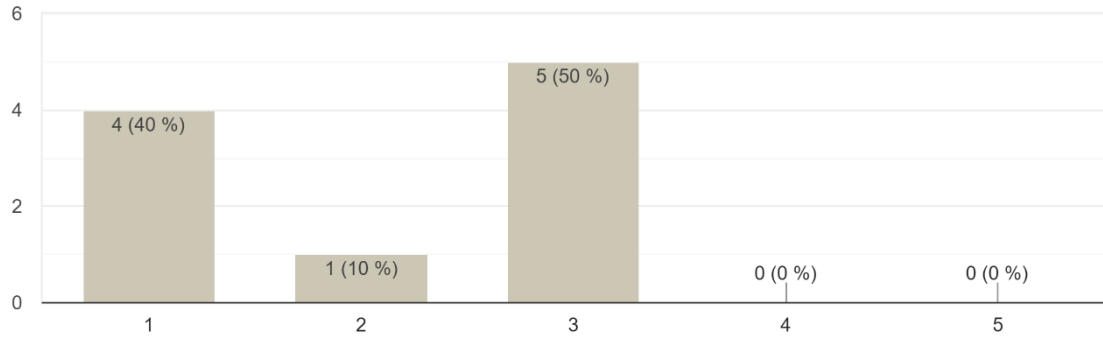


Para la pregunta que está relacionada con el proceso de ejercer el voto y el objetivo es verificar si la votante tenía el suficiente control sobre el proceso de votación y pueda realizar cambios antes de confirmar su voto: esto dio como resultado un 30%, pero hubo un 40% donde indica que es un problema estético. Adicional hubo un 30% donde se da a conocer que esta sección es un problema menor y tiene baja prioridad.

Pregunta No.6:

¿Pudo volver atrás o modificar su elección de voto de manera sencilla si así lo deseaba?

10 respuestas

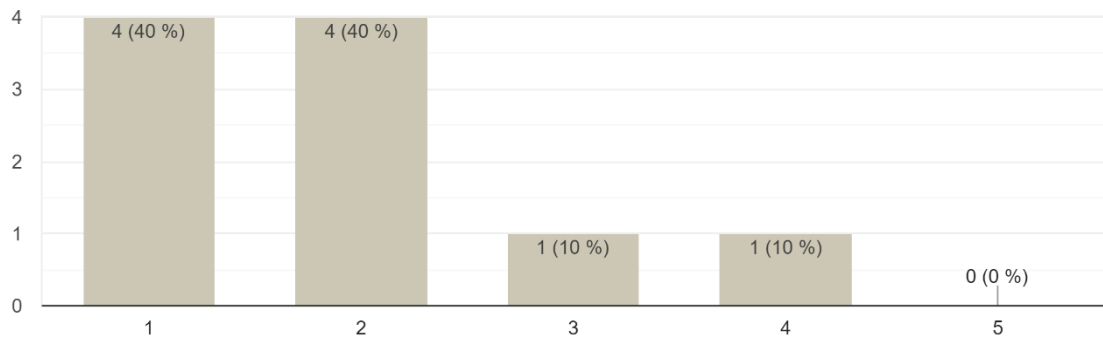


En base a los resultados obtenidos en la pregunta No.6 nos indica si el votante pudo volver atrás o modificar su elección de voto de una manera practica y sencilla. Un 40% de la población así lo certifica, en cambio hubo un 10% que detalla que este apartado puede mejorar, pero no es algo de prioridad. Así como el 50% de los encuestados indica que es un problema menor pero no es prioridad debido a que el proceso de votación transcurre con el flujo normal sin afectar su proceso.

Pregunta No.7.

¿Notó que existía consistencia en el diseño y la forma en que se presentaban las opciones a lo largo de la plataforma?

10 respuestas



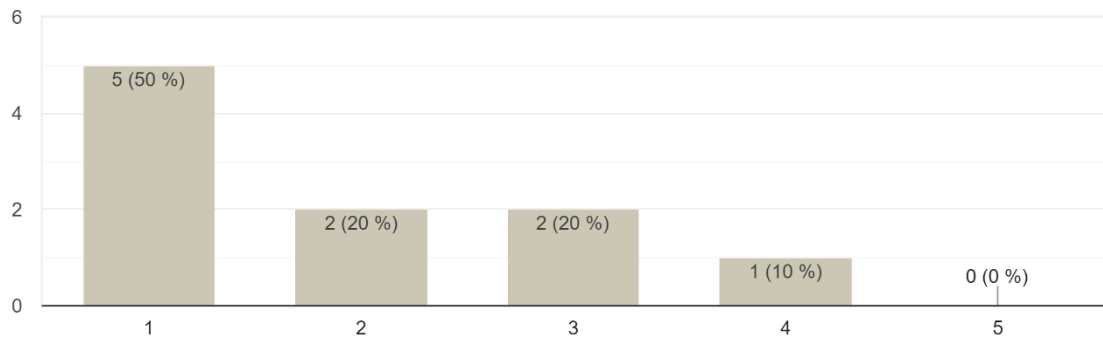
El análisis de los resultados de esta pregunta indica que la mayoría de los participantes perciben una consistencia en el diseño y la presentación de las opciones en la plataforma. El 80% de los encuestados (ocho de diez) proporcionó respuestas que indican que no consideran que sea un problema de usabilidad, con un 40% respondiendo con un "1" y otro 40% con un "2" en la escala del 1 al 5. Esto sugiere que la mayoría de los usuarios no perciben problemas significativos en la consistencia del diseño.

El 10% restante se dividió entre las respuestas "3" y "4", lo que indica que un pequeño porcentaje de los participantes considera que podría haber cierta inconsistencia en el diseño y la presentación de las opciones en la plataforma, aunque no la califican como un problema de usabilidad grave.

Pregunta No.8.

¿La plataforma seguía un patrón estándar que facilitó su navegación y comprensión del proceso de votación?

10 respuestas



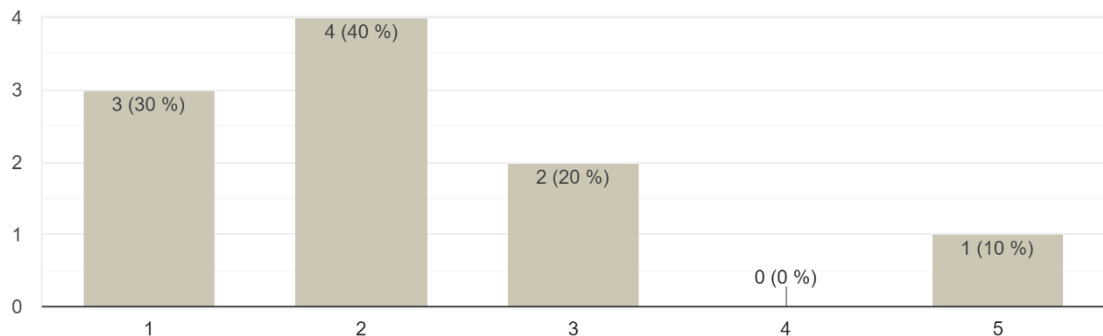
Los resultados indican lo siguiente: sugiere que la mayoría de los participantes percibieron que la plataforma seguía un patrón estándar que facilitó su navegación y comprensión del proceso de votación. Un 70% de los encuestados (cinco de diez) respondió con un "1" en la escala del 1 al 5, lo que indica que no consideran que sea un problema de usabilidad. Otro 20% respondió con un "2", lo que también refleja una percepción positiva.

Un 10% de los participantes respondió con un "3", lo que sugiere que algunos podrían haber experimentado cierta dificultad en la navegación y comprensión del proceso de votación, pero no lo calificaron como un problema importante de usabilidad. Solo una persona (10%) respondió con un "4", lo que indica una percepción de que la plataforma podría haber tenido problemas significativos en la estandarización y facilidad de navegación.

Pregunta No.9.

¿La plataforma incluyó medidas para evitar que cometa errores durante el proceso de votación?

10 respuestas



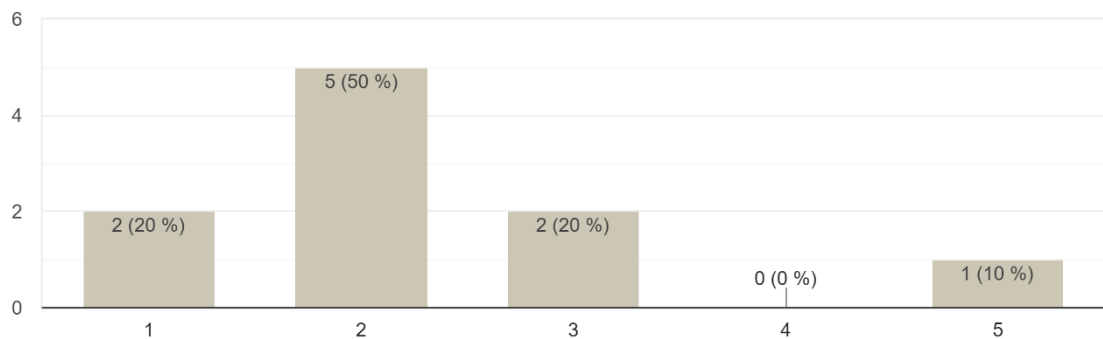
Indica que la mayoría de los participantes considera que la plataforma incluyó medidas para evitar cometer errores durante el proceso de votación. El 70% de los encuestados (siete de diez) proporcionó respuestas que sugieren que no perciben problemas significativos en este aspecto, con un 30% respondiendo con un "1" y un 40% con un "2" en la escala del 1 al 5. Esto indica una percepción general positiva de que la plataforma ha implementado medidas efectivas para prevenir errores.

Un 20% de los participantes respondió con un "3", lo que sugiere que algunos podrían haber experimentado cierta preocupación o confusión en relación con la prevención de errores, aunque no lo calificaron como un problema importante de usabilidad. Sin embargo, solo una persona (10%) respondió con un "5", lo que indica una percepción de que la plataforma podría haber tenido problemas significativos en la prevención de errores durante el proceso de votación y que debe ser implementado de manera rápida.

Pregunta No.10.

¿Hubo alguna característica que le impidiera o advirtiera sobre posibles errores en su elección antes de confirmar el voto?

10 respuestas



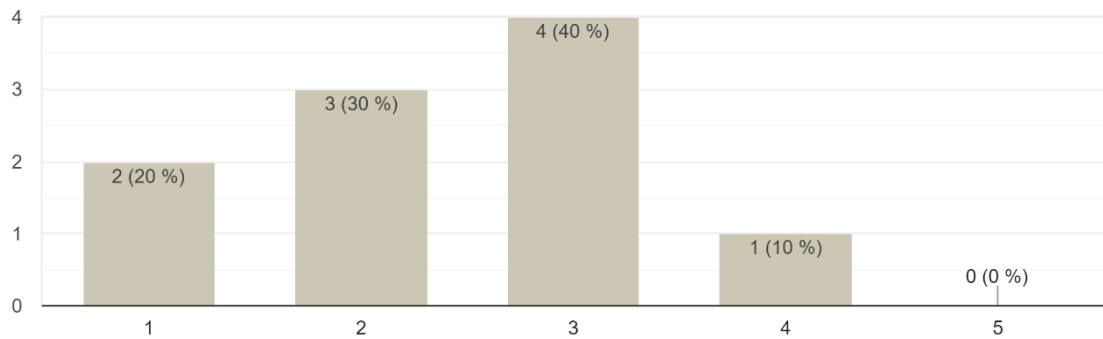
El análisis de los resultados de esta pregunta sugiere que la mayoría de los participantes considera que la plataforma incluyó características que les impidieron o advirtieron sobre posibles errores en su elección antes de confirmar el voto. Un 70% de los encuestados (siete de diez) proporcionó respuestas que indican que no perciben problemas significativos en este aspecto, con un 20% respondiendo con un "1" y un 50% con un "2" en la escala del 1 al 5. Esto indica una percepción general positiva de que la plataforma ha implementado características efectivas para prevenir errores antes de confirmar el voto.

Un 20% de los participantes respondió con un "3", lo que sugiere que algunos podrían haber experimentado cierta ambigüedad o falta de claridad en correlación con las peculiaridades de prevención de errores, aunque no lo calificaron como un problema importante de usabilidad. Sin embargo, solo una persona (10%) respondió con un "5", lo que indica una percepción de que la plataforma podría haber tenido problemas significativos en este aspecto al no evitar o advertir sobre posibles errores antes de confirmar el voto.

Pregunta No. 11.

¿La plataforma presentó opciones o recordatorios visuales que le ayudaron a reconocer las acciones que debía realizar en lugar de tener que recordarlas?

10 respuestas



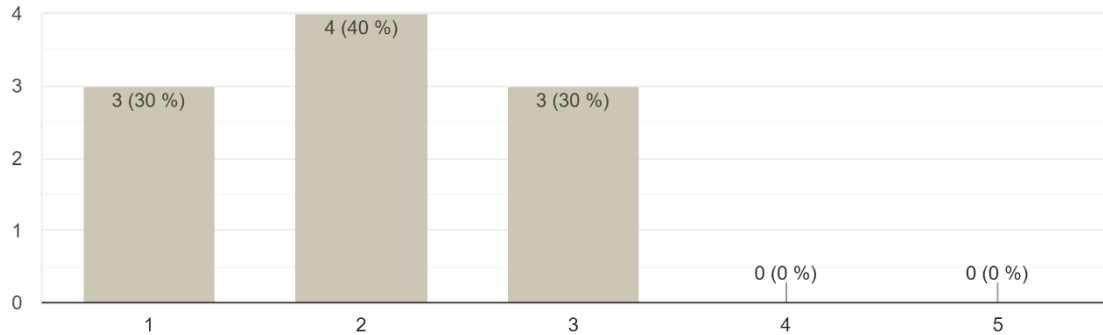
La mayoría de los participantes considera que la plataforma presentó opciones o recordatorios visuales que les ayudaron a reconocer las acciones que debían realizar en lugar de tener que recordarlas. El 70% de los encuestados (siete de diez) proporcionó respuestas que sugieren que no perciben problemas significativos en este aspecto, con un 20% respondiendo con un "1", un 30% con un "2" y un 20% con un "3" en la escala del 1 al 5. Esto indica una percepción general positiva de que la plataforma ofreció opciones visuales o recordatorios que facilitaron el reconocimiento de las acciones a realizar.

Sin embargo, un 10% de los participantes respondió con un "4", lo que indica que una minoría considera que la plataforma podría haber tenido problemas significativos en este aspecto, lo que se traduce en una alta prioridad para su resolución.

Pregunta No. 12.

¿Fue fácil para usted reconocer las opciones disponibles en cada paso del proceso de votación?

10 respuestas



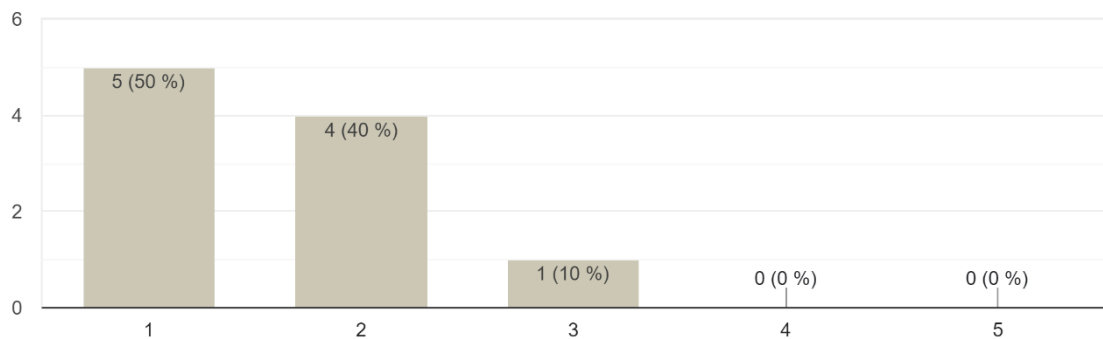
El análisis de los resultados de esta pregunta sugiere que la mayoría de los participantes considera que fue fácil reconocer las opciones disponibles en cada paso del proceso de votación. El 70% de los encuestados (siete de diez) proporcionó respuestas que indican que no perciben problemas significativos en este aspecto, con un 30% respondiendo con un "1" y un 40% con un "2" en la escala del 1 al 5. Esto refleja una percepción general positiva de que las opciones disponibles en cada etapa del proceso de votación fueron reconocibles con facilidad.

Un 30% de los participantes respondió con un "3", lo que sugiere que algunos podrían haber experimentado cierta dificultad en la identificación de las opciones disponibles, aunque no lo calificaron como un problema importante de usabilidad.

Pregunta No. 13.

¿Sintió que la plataforma te permitía votar de manera eficiente, adaptándose a sus preferencias y necesidades?

10 respuestas



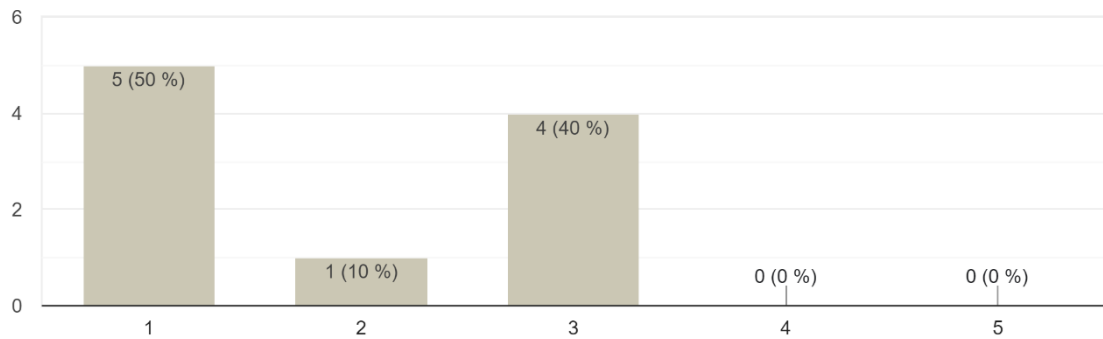
El análisis de los resultados de esta pregunta sugiere que la mayoría de los participantes sintió que la plataforma les permitía votar de manera eficiente, adaptándose a sus preferencias y necesidades. El 90% de los encuestados (nueve de diez) proporcionó respuestas que indican que no perciben problemas significativos en este aspecto, con un 50% respondiendo con un "1" y un 40% con un "2" en la escala del 1 al 5. Esto refleja una percepción general positiva de que la plataforma facilitó un proceso de votación eficiente y adaptable a las preferencias y necesidades de los usuarios.

Solo una persona (10%) respondió con un "3", lo que sugiere que podría haber experimentado cierta eficiencia y adaptabilidad ligeramente menores en comparación con la mayoría de los usuarios. Sin embargo, en general, la mayoría de los participantes considera que la plataforma cumplió eficazmente con este aspecto de usabilidad.

Pregunta No. 14.

¿La plataforma le ofreció opciones para personalizar su experiencia de votación y hacerla más eficiente?

10 respuestas



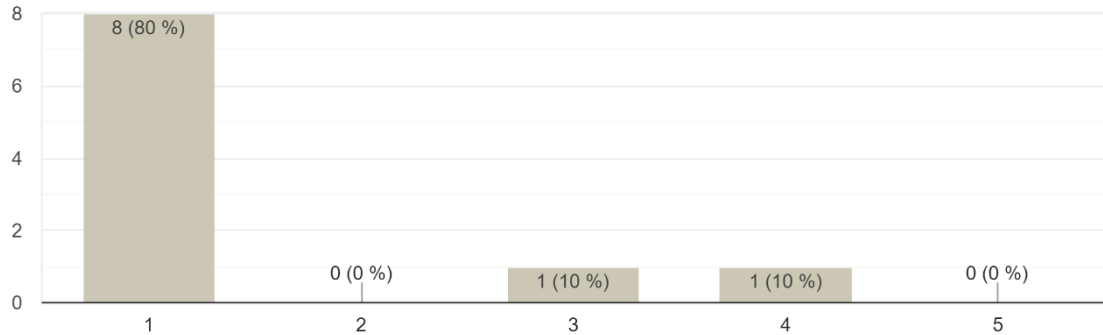
El análisis de los resultados de esta pregunta sugiere que la mayoría de los participantes considera que la plataforma presentó opciones o recordatorios visuales que les ayudaron a reconocer las acciones que debían realizar en lugar de tener que recordarlas. El 90% de los encuestados (nueve de diez) proporcionó respuestas que indican que no perciben problemas significativos en este aspecto, con un 50% respondiendo con un "1" y un 40% con un "3" en la escala del 1 al 5. Esto refleja una percepción general positiva de que la plataforma ofreció opciones visuales o recordatorios efectivos que facilitaron el reconocimiento de las acciones a realizar.

Solo una persona (10%) respondió con un "2", lo que sugiere que podría haber experimentado un nivel moderado de problemas en comparación con la mayoría de los usuarios.

Pregunta No.15.

¿Encontró el diseño de la plataforma atractivo y fácil de entender durante el proceso de votación?

10 respuestas



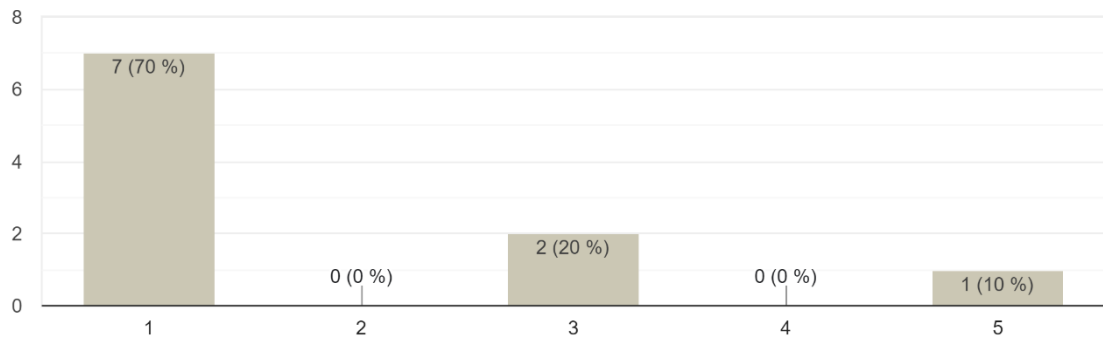
Los participantes encontraron el diseño de la plataforma atractivo y fácil de entender durante el proceso de votación. El 90% de los encuestados (nueve de diez) proporcionó respuestas que indican que no perciben problemas significativos en este aspecto, con un 80% respondiendo con un "1" en la escala del 1 al 5. Esto refleja una percepción general muy positiva de que el diseño de la plataforma fue atractivo y fácil de comprender.

Sin embargo, un 10% de los participantes respondió con un "3", lo que sugiere que un número muy pequeño de usuarios podría haber experimentado cierta dificultad en la comprensión del diseño, aunque no lo calificaron como un problema importante de usabilidad. Además, una persona (10%) respondió con un "4", indicando que, para esa persona, el diseño fue un problema mayor y de alta prioridad para resolver.

Pregunta No. 16.

¿Considera que el diseño minimalista de la plataforma contribuyó a una experiencia de votación más clara y organizada?

10 respuestas



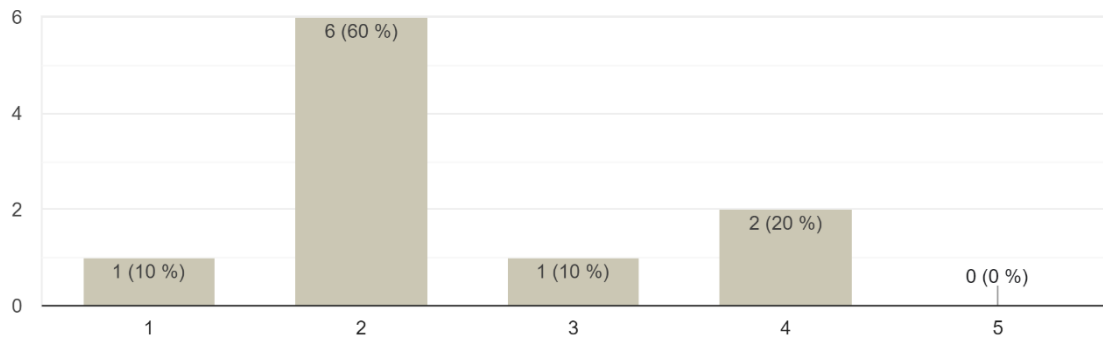
El análisis de los resultados de esta pregunta indica que la mayoría de los participantes considera que el diseño minimalista de la plataforma contribuyó a una experiencia de votación más clara y organizada. El 90% de los encuestados (nueve de diez) proporcionó respuestas que sugieren que no perciben problemas significativos en este aspecto, con un 70% respondiendo con un "1" en la escala del 1 al 5. Esto refleja una percepción general muy positiva de que el diseño minimalista de la plataforma mejoró la claridad y organización de la experiencia de votación.

Solo dos personas (20%) respondieron con un "3", lo que indica que podrían haber tenido opiniones mixtas o haber experimentado ciertas dificultades en relación con el diseño minimalista. Además, una persona (10%) respondió con un "5", lo que indica una percepción de que el diseño minimalista fue un problema de usabilidad grave que requería una solución inmediata.

Pregunta No. 17.

¿La plataforma proporcionó mensajes claros y soluciones para ayudarle a entender y corregir posibles errores durante la votación?

10 respuestas



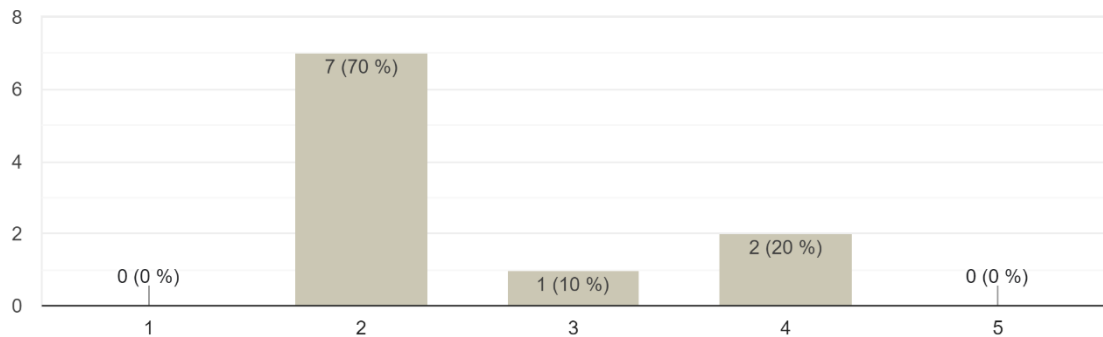
El análisis de los resultados de esta pregunta sugiere que la mayoría de los participantes considera que la plataforma proporcionó mensajes claros y soluciones para ayudar a entender y corregir posibles errores durante la votación. El 70% de los encuestados (siete de diez) proporcionó respuestas que indican que no perciben problemas significativos en este aspecto, con un 10% respondiendo con un "1" y un 60% con un "2" en la escala del 1 al 5. Esto refleja una percepción general positiva de que la plataforma ofreció mensajes claros y soluciones efectivas para la detección y corrección de errores durante la votación.

Sin embargo, el 20% de los participantes respondió con un "4", lo que indica que, para ellos, la plataforma podría haber tenido problemas significativos en este aspecto, lo que se traduce en una alta prioridad para su resolución.

Pregunta No. 18.

¿Se sintió respaldado/a por la plataforma para corregir cualquier error que pudiera haber cometido durante el proceso de votación?

10 respuestas



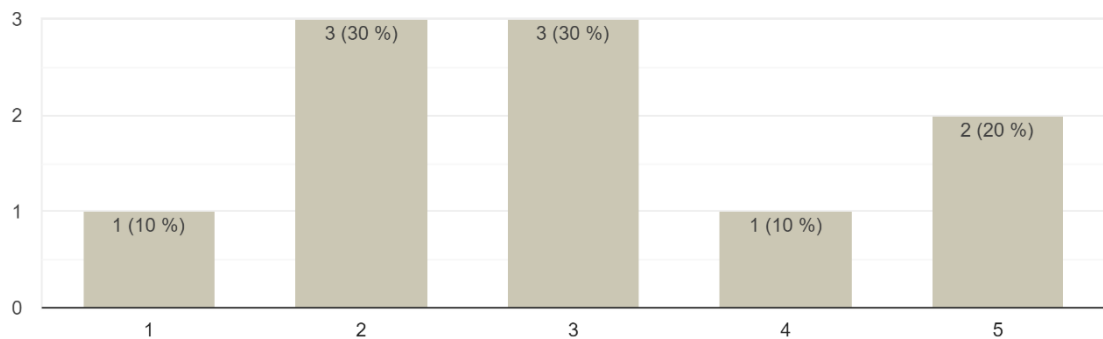
El análisis de los resultados de esta pregunta sugiere que la mayoría de los participantes se sintió respaldada por la plataforma para corregir cualquier error que pudiera haber cometido durante el proceso de votación. El 70% de los encuestados (siete de diez) proporcionó respuestas que indican que no perciben problemas significativos en este aspecto, con un 70% respondiendo con un "2" en la escala del 1 al 5. Esto refleja una percepción general positiva de que la plataforma proporcionó el respaldo necesario para corregir errores durante la votación.

El 20% de los participantes respondió con un "4", lo que sugiere que, para ellos, la plataforma podría haber tenido problemas significativos en este aspecto, lo que se traduce en una alta prioridad para su resolución. Además, un 10% respondió con un "3", indicando que experimentaron cierta dificultad o que el respaldo podría haber sido insuficiente en su opinión.

Pregunta No. 19.

¿Encontró disponible alguna forma de ayuda o documentación que le asistiera en caso de necesitar información adicional durante la votación?

10 respuestas



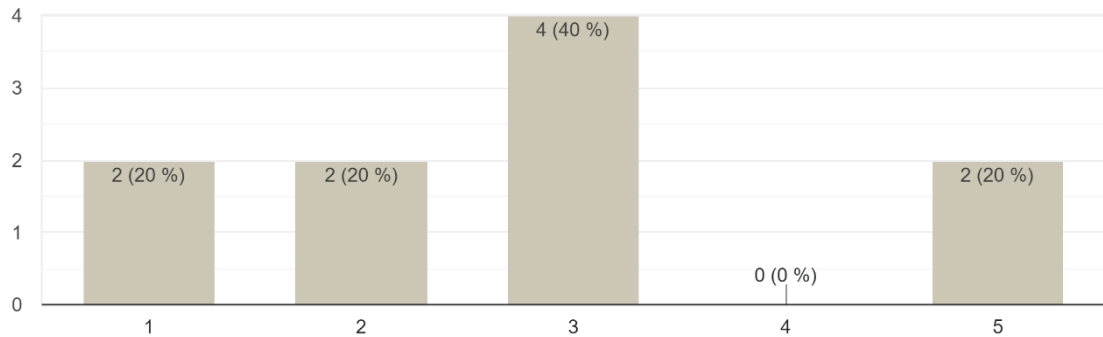
El análisis de los resultados de esta pregunta sugiere que hubo una variabilidad en la percepción de los participantes en cuanto a la disponibilidad de formas de ayuda o documentación durante la votación. Aunque el 40% de los encuestados respondió con "3", lo que indica que consideraron que había formas de ayuda o documentación disponible, el 10% respondió con "2", sugiriendo que para ellos, podría haber habido ciertas dificultades o insuficiencias en este aspecto. Además, un 10% respondió con "1", lo que indica que consideraron que la ayuda estaba disponible y no era un problema importante de usabilidad.

Sin embargo, un 30% de los participantes respondió con "5", lo que indica que percibieron la falta de ayuda o documentación como un problema de usabilidad grave y de alta prioridad para resolver. Además, un 10% respondió con "4", lo que sugiere que también experimentaron problemas significativos en este aspecto, aunque no lo calificaron como una catástrofe de usabilidad.

Pregunta No. 20.

¿Considera que la información de ayuda disponible fue útil y fácil de acceder en caso de requerirla?

10 respuestas



El análisis de los resultados de esta pregunta muestra una variabilidad en la percepción de los participantes con respecto a la utilidad y accesibilidad de la información de ayuda disponible. Aproximadamente el 40% de los encuestados proporcionó respuestas que indican que consideraron que la información de ayuda disponible fue útil y fácil de acceder, ya que el 20% respondió con "1" y el 20% con "2" en la escala del 1 al 5. Esto refleja una percepción general positiva de la utilidad y accesibilidad de la información de ayuda.

Sin embargo, el 40% de los participantes respondió con "3", lo que sugiere que podrían haber tenido una percepción mixta o haber experimentado ciertas dificultades en relación con la utilidad y accesibilidad de la información de ayuda. Además, el 20% respondió con "5", lo que indica que, para ellos, la información de ayuda no fue útil y su accesibilidad fue un problema de usabilidad grave que requería una solución inmediata.

3.2.3.1.1.2 Análisis de entrevistas.

El presente análisis tiene como objetivo examinar y comparar dos entrevistas llevadas a cabo con profesionales de diferentes ámbitos, ambos con perspectivas valiosas sobre la ejecución de la tecnología en procesos electorales. La primera entrevista se realizó con un analista de participación política, con experiencia en procesos electorales, mientras que la segunda entrevista involucra a un desarrollador de software con experiencia en tecnologías como Blockchain. Ambas entrevistas exploran temas cruciales relacionados con la votación electrónica, abordando preocupaciones sobre seguridad, privacidad, confianza y participación ciudadana.

A través de este análisis, buscaremos identificar convergencias y divergencias en las opiniones y perspectivas de estos profesionales. Examinar sus puntos de vista sobre la tecnología blockchain, la votación electrónica, la confianza en la integridad del proceso electoral, y otros aspectos claves que proporcionará una visión integral sobre los desafíos y oportunidades que la tecnología presenta en el contexto electoral. La combinación de la experiencia política y la experiencia técnica en este análisis permitirá destacar las complejidades y consideraciones esenciales para la implementación exitosa de un sistema de votación electrónica.

Tabla 3. Tabla comparativa de resultados de entrevistas

Aspecto	Entrevistado/a 1 (Analista de participación política)	Entrevistado/a 2 (Desarrollador de software)
Familiaridad con la tecnología blockchain	Destaca la importancia de abordar preocupaciones de seguridad y privacidad.	Explica detalladamente la tecnología blockchain y menciona la prevención de fraudes como una ventaja.
Imaginación del proceso de votación electrónica	Menciona la importancia de la participación ciudadana y la revisión constante del sistema.	Visualiza un sistema inclusivo y fácil de usar, enfocándose en la conveniencia y la seguridad.
Preocupaciones sobre la votación electrónica	Destaca la resistencia al cambio y los costos como desafíos políticos.	Se centra en la vulnerabilidad del sistema ante ataques cibernéticos.
Confianza en la tecnología para aumentar la	Destaca la participación ciudadana y la supervisión independiente como fundamentales.	Enfatiza la importancia de abordar cuidadosamente aspectos técnicos y de seguridad.

<p>integridad electoral</p>	
<p>Privacidad y anonimato en la votación electrónica</p>	<p>Menciona que la privacidad es crítica para mantener la integridad y la confianza. Destaca la capacidad de verificar el voto de manera anónima y retirar el consentimiento.</p>
<p>Motivación para participar en elecciones electrónicas</p>	<p>Destaca la necesidad de educación sobre el funcionamiento del sistema. Menciona que la conveniencia y la capacidad de verificar personalmente el voto serían factores motivadores.</p>
<p>Inclusión y participación a través de la tecnología</p>	<p>Destaca la importancia de abordar desafíos de seguridad y privacidad. Resalta la conveniencia y la eliminación de barreras logísticas como beneficios.</p>
<p>Interoperabilidad y colaboración política</p>	<p>Menciona la colaboración entre diferentes entidades políticas para fortalecer la democracia. Subraya la importancia de abordar cuidadosamente aspectos técnicos y de seguridad.</p>

<p>Abordar críticas y desconfianza ciudadana hacia la tecnología</p>	<p>Destaca la combinación de factores, incluida la educación. Enfatiza la importancia de abordar cuidadosamente aspectos técnicos y de seguridad.</p>
<p>Papel de los partidos políticos en la implementación</p>	<p>Destaca la necesidad de la participación activa y constructiva de los partidos políticos. Destaca la colaboración entre diferentes entidades políticas para promover la confianza pública.</p>

3.3 Resultados esperados.

Encuesta

Tabla 4: Heurísticas violadas, problemas de usabilidad y las severidades encontradas en las pantallas del prototipo

Heurística violada	Severidades					Total
	1	2	3	4	5	
1. Visibilidad del estado del sistema	7	8	4	1		20
2. Correspondencia entre la interfaz del sistema y el mundo real	11	4	3	1	1	20
3. Control y libertad del usuario	7	5	8			20
4. Consistencia y estándar	9	6	3	2		20
5. Prevención de errores	5	9	4	2		20
6. Reconocimiento en vez de recordación	5	7	7	1		20
7. Flexibilidad y Eficiencia de Uso	10	5	5			20
8. Estética y diseño minimalista	15		3	1	1	20
9. Ayudar a los Usuarios a Reconocer, Diagnosticar y Recuperarse de Errores	1	13	2	4		20
10. Ayuda y documentación	3	5	7	1	4	20
Total, por heurística	73	62	46	13	6	200
Problemas de usabilidad (Porcentaje)	36,5 %	31%	23%	6,5%	3%	100%

La tabla seleccionada muestra una evaluación detallada de diferentes heurísticas violadas en términos de su severidad y prioridad a ser resueltas. La escala utilizada (1 a 5) clasifica los problemas en diferentes niveles, desde no ser un problema de usabilidad hasta requerir atención inmediata debido a una catástrofe de usabilidad.

La tabla muestra una serie de problemas en diferentes heurísticas, pero es importante tener en cuenta que cada uno tiene una severidad y prioridad diferente. Es esencial priorizar y abordar los problemas con una mayor severidad y prioridad para mejorar la usabilidad del sistema.

Los resultados obtenidos revelaron que las reglas heurísticas más frecuentemente violadas en el sistema fueron " 9. Ayudar a los Usuarios a Reconocer, Diagnosticar y Recuperarse de Errores I" y " Ayuda y documentación ", con un total de 19 problemas de usabilidad identificados en cada una de estas áreas, lo que representa un 9,5% de los problemas en cada categoría.

En cuanto a los principales comentarios proporcionados por los evaluadores en relación a las reglas heurísticas que se encontraban violadas, destacaron la necesidad de mejoras en el diseño, tales como la alteración de colores en el encabezado y pie de página, la presencia de elementos visuales innecesarios en las pantallas, la falta de estándares claros para los enlaces, la ausencia de mensajes de alerta cuando los usuarios hacen clic en un enlace que los lleva a una página web externa, la necesidad de permitir a los usuarios avanzar en el video si no desean verlo por completo y la falta de un botón para desactivar el sonido, lo que permitiría a los usuarios tener un mayor control sobre sus acciones.

Una ventaja significativa de la evaluación heurística es que la evaluación y conclusión que se obtuvo. Además, destacaron tanto los puntos fuertes como las áreas que necesitaban mejoras en el proyecto. Como resultado, todas las sugerencias proporcionadas por la evaluación obtenida se tomaron en consideración en la versión final.

Hasta el momento, los análisis de las respuestas a las preguntas han revelado varias tendencias y patrones:

Diseño Claro y Organizado: La mayoría de los participantes encontró que el diseño de la plataforma era atractivo y fácil de entender, contribuyendo a una experiencia de votación clara y organizada.

Ayuda y Documentación: Hubo una variabilidad en la percepción de la disponibilidad y utilidad de la ayuda y documentación. Algunos participantes consideraron que la ayuda estaba disponible y era útil, mientras que otros experimentaron dificultades o la percibieron como insuficiente.

Mensajes de Error: La mayoría de los participantes consideró que la plataforma proporcionaba mensajes claros y soluciones para entender y corregir posibles errores durante la votación. Sin embargo, un pequeño porcentaje de usuarios podría haber experimentado problemas significativos en este aspecto.

Respaldo para Corrección de Errores: La mayoría de los participantes se sintió respaldada por la plataforma para corregir errores durante el proceso de votación. Sin embargo, un porcentaje minoritario podría haber experimentado problemas significativos en este sentido.

Facilidad en la Identificación de Opciones: La mayoría de los participantes consideró que la plataforma les facilitó reconocer las opciones disponibles en cada paso del proceso de votación.

En general, la plataforma parece haber tenido un buen nivel de usabilidad, con la mayoría de los participantes teniendo una experiencia positiva en términos de diseño claro, ayuda y mensajes de error. Sin embargo, se observa cierta variabilidad en la percepción de la disponibilidad de ayuda y documentación, lo que podría requerir una mayor atención.

Entrevistas

Se brindará un resumen de las entrevistas realizadas empezando por la introducción de la tecnología en los procedimientos electorales, puede brindar eficacia y accesibilidad según lo comentado con los expertos, aunque también presenta desafíos en términos de seguridad y confidencialidad. Para fortalecer la confianza en la integridad y seguridad, es esencial garantizar que los datos y el flujo de estos sean los correctos, así como la participación ciudadana y la realización de auditorías independientes. Medidas como el cifrado y regulaciones son indispensables para

asegurar la transparencia en la votación electrónica, mientras que la privacidad y el anonimato de los votantes deben ajustarse a regulaciones apropiadas. Desafíos como la reticencia al cambio y los costos deben ser abordados colaborativamente entre partidos políticos, expertos y la sociedad civil. La equidad de acceso se logra mediante la colaboración entre gobiernos, partidos políticos y la sociedad civil, y la tecnología puede incrementar la participación, especialmente entre segmentos históricamente menos participativos, siempre y cuando se garantice la seguridad y confidencialidad. La interoperabilidad y cooperación entre entidades políticas son esenciales para reforzar la confianza pública, y responder a las críticas ciudadanas hacia la tecnología requiere transparencia, participación ciudadana, seguridad y educación continua. Los partidos políticos desempeñan un papel crucial en las discusiones y decisiones sobre la implementación de sistemas de votación electrónica, asegurando equidad y aceptación por todas las partes. En resumen, el éxito radica en la colaboración, transparencia y atención continua a la seguridad y confidencialidad para construir confianza en la integridad de los procesos electorales.

PROPUESTA TECNOLÓGICA

CAPITULO IV

CAPITULO IV: PROPUESTA TECNOLÓGICA

En esta propuesta tecnológica se expone la viabilidad de la implementación del sistema de votación fundamentado en la tecnología Blockchain, conforme al planteamiento de (Manero, 2022). Es de conocimiento general que la noción de factibilidad se relaciona con la existencia de los medios y recursos necesarios para alcanzar los objetivos predefinidos. En esta investigación, nos centraremos en tres componentes específicos, a saber:

Factibilidad Técnica: Se describirán en detalle los componentes técnicos relacionados con la ejecución del sistema de sufragio aplicado con la tecnología Blockchain. Se examinarán los recursos y tecnologías que mejor se adapten para el prototipo y que ayude a futuro ser escalable y el procedimiento sea lo más claro para ejecutar este proceso.

Factibilidad Financiera: Se profundizará en la evaluación financiera necesaria para llevar a cabo las actividades y procedimientos requeridos en la implementación del sistema de votación electrónica basado en la tecnología Blockchain. Se examinarán en detalle los recursos financieros, el presupuesto necesario y los aspectos económicos esenciales para garantizar la viabilidad de este proyecto.

Factibilidad Social: Se hace hincapié en la formación del personal que participa en el proceso de votación, lo cual incluye estudiantes, personal docente y profesionales involucrados en política y TI. También se abordará la difusión de la nueva modalidad de votación electrónica, con el objetivo de garantizar que el proceso se lleve a cabo sin obstáculos y que todos los involucrados estén al tanto de la nueva dinámica. Además, se detallará minuciosamente la ejecución del proceso, describiendo las etapas y los actores involucrados, así como los responsables designados para asegurar la óptima implementación de este proyecto.

4.1 Factibilidad Financiera.

La factibilidad de este proyecto nos proporcionará una estimación del gasto necesario para llevar a cabo la introducción del sistema de votación electrónica basado en la tecnología Blockchain. Los detalles de este análisis se presentarán en la siguiente tabla:

Tabla 5. Factibilidad Económica

<i>Cantidad</i>	<i>Detalle</i>	<i>Valor</i>	<i>Total</i>
3	Servidores	2500	7500
3	Desarrolladores	2000	6000
1	Publicidad	850	850
<i>Subtotal</i>			8950
1	Costos de Mantenimiento	500	500
1	Capacitación del Personal	1000	1000
1	Contingencias y Reservas	800	800
1	Costos de Integración	700	700
<i>Total</i>			11,950

Origen: Elaborado por autor

Se estima la necesidad de adquirir dos servidores robustos para manejar la carga de procesamiento y almacenamiento de datos de manera eficiente. El costo unitario de \$2500 se basa en la selección de hardware confiable y capaz de soportar los requisitos del sistema.

Se contempla la contratación de tres ingenieros para supervisar la implementación, realizar pruebas y garantizar la estabilidad del sistema, enfocados a Frontend, Backend y Base de datos. El costo de \$2000 por ingeniero refleja una tarifa competitiva para profesionales con experiencia en proyectos similares.

La partida destinada a la publicidad se justifica como una inversión para informar a la comunidad académica sobre la nueva implementación y fomentar la participación

en el sistema de votación electrónica. El presupuesto de \$850 se ajusta a campañas de promoción en línea y fuera de línea.

4.2 Factibilidad Social.

En esta parte de la propuesta se desarrollará el proceso de concientización del voto electrónico con todo el personal involucrado, esto quiere decir la capacitación al personal que dirigirá las votaciones, a las personas que estarán en las mesas electorales y a los participantes de las votaciones, en cuanto al manejo del nuevo Software y la manera en la que se usará en las diferentes partes del proceso electoral y que de esta manera las elecciones se desarrollen con normalidad.

4.2.1 Objetivos del plan de factibilidad Social.

- Lograr que cada participante en la administración de las elecciones conozca sus roles y responsabilidades de seguridad, privacidad y funcionamiento del software del proceso electoral.
- Concientizar a los participantes de las elecciones del cambio y nueva forma en la que se llevara a cabo las elecciones dentro de la Facultad de Ingeniería Industrial.
- Evaluar si el proceso de concientización ayudo a generar una mayor confianza y seguridad en los procesos electorales.

4.3 Factibilidad Técnica.

Se presentará la propuesta que respalda la viabilidad del sistema de votación destinado a ser un prototipo para verificar la seguridad que brinda una red Blockchain. Se expondrán en detalle los cuatro procesos primordiales del sistema, a saber:

- a) El primer paso hace referencia al de configurar y establecer normas y pautas, es aquí para llevar a cabo en el proceso electoral. En primera instancia se procede que la máquina donde los votantes ejercerán su derecho al voto cuente con los requisitos necesarios, así como la respectiva wallet (cartera digital) para cada uno de ellos, la cual necesitarán para votar.
- b) El segundo paso es definir los horarios en los cuales se llevará cabo las elecciones, un horario específico de inicio y uno de culminación.
- c) Antes de pasar a la fase de votación, se debe cargar el padrón electoral en la base de datos y el votante podrá registrarse en el sistema una vez sus credenciales sea validadas por el servicio web conectado al registro civil, así podrá seleccionar si desea votar por una lista.
- d) En este momento ya se podrán visualizar los en tiempo real y un reporte
- e) En el cierre de la votación en el proceso electoral se podrá examinar cual fue la cantidad votos para cada uno de los candidatos.
- f) Culminado el proceso de votación no se podrá acceder a la elección que se encontraba en curso.

4.3.1 Metodología de desarrollo.

4.3.1.1 Alcance de la aplicación.

Algunos aspectos claves que se incluyen en este desarrollo, es el hecho de permitir el registro de votantes elegibles. Esto podría incluir la verificación de la identidad de los votantes a través de documentos de identificación y la creación de una base de datos de votantes, así como la validación de los documentos de identificación con la entidad del Registro Civil y así manejar datos reales para la simulación de un prototipo de elección.

Para la simulación de este prototipo se tendrá dos roles importantes:

Administrador: se encargará de gestionar y crear un proceso electoral, e incluso actores directos, como candidatos.

Votante: Se encargará de participar en el proceso electoral y ejercer su voto, a su vez tendrá la posibilidad de ver los resultados de la votación.

No se implementará un rol de candidato, esto debido a que el rol de administrador podrá gestionar ese perfil y hacer todo el proceso para que un candidato pueda participar en un proceso electoral. Al evitar la creación de roles específicos para candidatos, la plataforma se mantiene flexible para su uso en una variedad de procesos electorales, ya sea a nivel político, empresarial, estudiantil u otro. Los usuarios pueden adaptar el sistema según sea necesario para diferentes contextos electorales sin restricciones innecesarias.

Se logró garantizar la autenticación segura de los votantes para prevenir el fraude. Esto incluye la verificación de hashes en la red de bloques de la blockchain, el uso de contraseñas seguras o la verificación de códigos temporales vía correo

electrónico. Se implementarán medidas para prevenir la doble votación usando contratos inteligentes vinculados a la red blockchain.

Se proporcionó una interfaz de votación intuitiva y de fácil uso para los votantes. Esto incluye la presentación y gestión de candidatos, votantes, padrones electorales, elecciones y opciones de votación de manera clara y comprensible.

Para el almacenamiento de imágenes que serán cargadas en los diferentes módulos, se hará uso de un servicio de AWS S3 para que ayude a gestionar mejor los recursos multimedia y mantener un mejor rendimiento en la carga de la plataforma.

La plataforma de votación incorpora medidas de seguridad sólidas, como la encriptación de datos sensibles, la resistencia a ataques de denegación de servicio (DDoS) y la protección contra intrusiones, así como la inmutabilidad de los datos, esto gracias a la red Blockchain y su red descentralizada.

Dentro del módulo de votación, se registran de manera segura y anónima los votos emitidos por los usuarios. Esto implica la creación de un registro inmutable de todas las transacciones de votación.

La herramienta debe ser capaz de realizar el recuento automático de votos de manera precisa y eficiente proporcionando resultados en tiempo real a medida que se emiten los votos, lo que permite a los interesados seguir el progreso de la elección.

4.3.1.2 Pruebas de seguridad

En cuanto a las pruebas técnicas que se realizarán para verificar la seguridad de la plataforma:

Se pretende realizar pruebas de penetración para identificar y solucionar vulnerabilidades de seguridad en la plataforma y evaluar la capacidad de la plataforma para manejar un gran número de votantes y ataques DDoS simulados, conocidos como pruebas de estrés.

Verificar la seguridad y el flujo de los datos almacenados y transmitidos, incluida la encriptación y la protección contra amenazas internas y evidenciar la fortaleza de la autenticación de votantes y la prevención de la doble votación. Gracias a la cadena de bloques nos aseguramos de que los votos registrados no puedan ser modificados después de su emisión, por último, validar que la plataforma garantice la privacidad de los votantes y que los votos sean anónimos y así realizar simulacros de elección para probar todo el proceso, desde la autenticación hasta la emisión de votos y la generación de resultados.

En cuanto a la metodología de desarrollo, se utilizó Extreme Programming para la creación del aplicativo web, la cual se enfoca en fortalecer las relaciones interpersonales como un factor clave para alcanzar el éxito en el desarrollo de software. Esta metodología fomenta el trabajo en equipo, se preocupa por el crecimiento y aprendizaje de los desarrolladores, y crea un entorno de trabajo positivo. Además, busca la simplicidad en las soluciones implementadas y la disposición para abordar cambios con valentía. Esta metodología se considera especialmente adecuada para proyectos con requisitos poco definidos y sujetos a cambios frecuentes, así como aquellos que involucran un alto nivel de riesgo técnico. (Sánchez Hernández, Lizano Madriz, & Sandoval Carvajal, 2020).

Existen diversas metodologías para el desarrollo con tecnología blockchain, y la elección de la metodología Extreme Programming (XP) para el desarrollo con blockchain puede depender de varios factores y objetivos específicos del proyecto. Aquí hay algunas razones por las cuales se considera apropiada la metodología XP para el desarrollo de este prototipo:

- XP se centra en la entrega continua de software funcional en iteraciones cortas. En el contexto de blockchain, donde se pueden tener contratos inteligentes complejos y características específicas de la cadena de bloques, un enfoque iterativo permite abordar desafíos paso a paso, mejorando y adaptando constantemente la solución.
- Dado que el proyecto enfrentó cambios en los requisitos debido a la evolución de la tecnología y la comprensión cambiante del diseño, la flexibilidad de XP fue una ventaja.
- XP incluye la participación continua del cliente y usuarios en el proceso de desarrollo. En una plataforma de votación, es esencial comprender y adaptarse a las necesidades cambiantes de los usuarios y autoridades electorales.

El proyecto se desarrolló a través de cinco etapas que se llevaron a cabo de manera secuencial, siguiendo las pautas establecidas por Extreme Programming:

- Planificación del Sistema de Información (PSI)
- Análisis del Sistema de Información (ASI)
- Diseño del Sistema de Información (DSI)
- Construcción del Sistema de Información (CSI)

Estas fases se ejecutaron siguiendo un enfoque secuencial, conforme a las directrices proporcionadas por Extreme Programming.

4.3.1.3 Fase I: Planificación.

Es esencial resaltar que en esta fase se incorporó la evaluación de la viabilidad del sistema, ya que ambas etapas están interrelacionadas. Durante este proceso, se llevó a cabo un análisis de las necesidades del Plan de Sistema de Información, es decir, se definieron los resultados finales esperados por la solución web. Para lograrlo, se establecieron los objetivos que la solución web debía cumplir y se identificaron los responsables y participantes involucrados en el desarrollo del software.

Los actores principales que desempeñaron un papel en el proceso de desarrollo del proyecto fueron:

- Estudiante encargado de desarrollar el proyecto.
- Tutor científico.

Además, en esta etapa se realizó un estudio de la información relevante, cuyo propósito fue recopilar y analizar las fuentes de información y documentación que aportaban al proyecto. Entre los elementos analizados se incluyeron los anexos y documentos correspondientes de la Unidad de Titulación.

En la etapa de la selección de arquitectura del proyecto, se desarrolló el frontend con la arquitectura de componentes, se basa en la creación de componentes reutilizables que representan diferentes partes de la interfaz de usuario de una aplicación web. Estos componentes pueden ser pequeños fragmentos de la interfaz de usuario o componentes más grandes que encapsulan partes completas de la página. En cambio, para la arquitectura del lado del servidor se implementó Modelo-Vista-Controlador (MVC).

Cabe destacar que en esta etapa solo se planificó con que arquitectura trabajar, el diseño/funcionamiento del mismo, se detalla en las siguientes fases, de acuerdo a lo que la metodología indica.

4.3.1.4 Fase II: Análisis.

4.3.1.4.1 Definición del sistema:

En esta fase se realiza el alcance del sistema, el cuál abarcó los siguientes procesos:

Se diseñó y desarrolló una plataforma web que brinda la capacidad al administrador de registrar y modificar información relevante, como votantes, elecciones y candidatos para un proceso electoral. Asimismo, permite a los votantes registrados elegir a un candidato de una lista predefinida en una elección activa y emitir su voto por el candidato seleccionado. Además, la plataforma ofrece la posibilidad de visualizar los resultados de una votación en tiempo parcial o final.

Para asegurar la confianza y transparencia del sistema, se implementó una red blockchain. La plataforma web establece una comunicación eficiente con la red a través de un servicio web, posibilitando el intercambio de información de manera segura y verificable.

Dado que la plataforma está orientada al entorno web, su acceso es a través de un enlace específico, el cual es accesible desde cualquier navegador web ampliamente utilizado.

Se identifican los procesos que se lograron implementar en la plataforma, estos son los siguientes:

- Registro de votantes
- Gestión de candidatos
- Gestión de elecciones
- Gestión de padrones electorales
- Consulta de resultados de votaciones
- Generación de reporte
- Efectuar voto

- Obtención de certificado de votación

De manera continua, se identificó el entorno tecnológico que se requirió para el desarrollo del sistema de información:

- Servidor: Node – Express
- Arquitectura: M.V.C (Modelo-Vista-Controlador)
- Lenguaje: React – Express – Solidity (Blockchain)
- Base de datos: MySQL
- Nube: AWS S3

4.3.1.4.2 Establecimiento de requisitos.

El propósito de esta actividad era obtener un catálogo exhaustivo de los requisitos. Este catálogo sirvió como base para verificar que los productos derivados de las etapas de modelización estuvieran en concordancia con las necesidades de los usuarios. Los requisitos fueron categorizados en dos grupos principales: funcionales y no funcionales.

4.3.1.4.3 Requerimientos funcionales.

Tabla 6: Requerimientos funcionales

Código	Requerimiento	Prioridad
RF1	Para gestionar la plataforma, el administrador debe iniciar sesión con usuario y contraseña.	ALTA
RF2	Se debe permitir al administrador registrar elecciones, en las cuales se agruparán los candidatos; registrar candidatos y crear padrones electorales.	ALTA

RF3	Permitir al administrador modificar la información registrada para las elecciones, candidatos y votantes.	ALTA
RF4	Consultar y validar si un votante puede ejercer el voto	ALTA
RF5	Permitir al administrador eliminar candidatos.	BAJA
RF6	Visualizar los candidatos y poder elegir solo uno de la opciones	ALTA
RF7	Permitir al administrador cambiar el estado de una elección	ALTA
RF8	Visualizar los resultados parciales o finales de la elección.	ALTA

Elaborado por: Autor.

4.3.1.4.4 Requerimientos no funcionales.

Código	Requerimiento	Prioridad
RN1	Visualizar para efectuar el voto desde cualquier computador o dispositivo móvil	ALTA
RN2	La plataforma debe contar con una interfaz amigable para el administrador y para el votante.	MEDIA
RN3	La plataforma debe ser lo suficientemente segura (flujo de datos inmutables).	ALTA

Elaborado por: Autor.

4.3.1.4.5 Análisis de casos de usos.

4.3.1.4.5.1 Gestión de candidatos.

4.3.1.4.5.2 Registrar.

Tabla 7: CU-GC-01 Registrar Candidato

Descripción	El sistema deberá permitir registrar un candidato tal como se describe en este caso de uso
Precondición	El usuario administrador ha iniciado sesión y ha indicado que desea registrar un candidato
Secuencia normal	<ol style="list-style-type: none">1. El administrador diligencia la información requerida del candidato en el formulario2. Selecciona una imagen del rostro del candidato.3. Envía el formulario diligenciado.4. Se valida la información del formulario<ol style="list-style-type: none">a. Si se registra correctamente, el sistema mostrará mensaje de confirmación.
Excepciones	Si la información no se puede validar <ol style="list-style-type: none">a. Se mostrará un mensaje informando del error

Comentarios	
-------------	--

Elaborado por: Autor.

4.3.1.4.5.3 Modificar.

Tabla 8: CU-GC-01 Modificar Candidato

Descripción	El sistema permitirá al administrador modificar información del candidato
Precondición	El usuario administrador ha iniciado sesión y ha indicado que desea registrar un candidato
Secuencia normal	<ol style="list-style-type: none"> 1. El administrador diligencia la información que desea cambiar 2. Si se selecciona una nueva imagen 3. Envía el formulario 4. Se valida la información diligenciada 5. Se procede a identificar si hay una nueva imagen seleccionada <ol style="list-style-type: none"> a. Si la hay, se procede a modificar la existente b. Si no la hay, se ignora 6. En cualquiera de los dos casos el sistema mostrará un

	mensaje confirmando la modificación
Excepciones	Si la información no se puede validar a. Se mostrará un mensaje informando del error
Comentarios	

Elaborado por: Autor.

4.3.1.4.5.4 Eliminar

Tabla 9: CU-GC-03 Eliminar Candidato

Descripción	El sistema permitirá eliminar a un candidato del sistema, siempre y cuando no haya iniciado la contienda en el sistema.
Precondición	El usuario administrador ha iniciado sesión y ha indicado que desea eliminar un candidato previamente seleccionado
Secuencia normal	<ol style="list-style-type: none"> 1. El sistema enviará una alerta de confirmación preguntando si desea continuar con el proceso <ol style="list-style-type: none"> a. Si el usuario confirma continuar, se procederá a eliminar al candidato

	<p>b. Si el usuario cancela el proceso, no se eliminará al candidato</p> <p>2. En cualquier de los dos casos, se cierra la alerta de confirmación y se procede a invocar el caso de uso CU-GC-04</p>
Excepciones	
Comentarios	

Elaborado por: Autor.

4.3.1.4.5.5 Listar.

Tabla 10: CU-GC-04 Listar Candidatos

Descripción	El sistema permitirá visualizar el listado de los candidatos registrados en el sistema.
Precondición	El usuario administrador ha iniciado sesión y ha indicado que desea ver el listado de candidatos registrados
Secuencia normal	1. El sistema visualizará los candidatos que están registrados en el sistema, podrá elegir la opción de modificar o eliminar

	<p>a. Si el usuario administrador selecciona modificar se aplicará el caso de uso CU-GC</p> <p>b. SI el usuario administrador selecciona eliminar continuará en el caso de uso CU-GC-03</p>
Excepciones	Si no hay candidatos registrados se mostrará el mensaje 'No hay candidatos registrados'
Comentarios	

Elaborado por: Autor.

4.3.1.4.6 Gestión de elecciones.

4.3.1.4.6.1 Registrar.

Tabla 11: CU-GE-01 Registrar Elección

Descripción	El sistema permitirá agregar una elección, y configurarla con los parámetros necesarios con los que se llevará a cabo dicho proceso.
Precondición	El usuario administrador iniciará sesión e indica que desea abrir un proceso de elección.
Secuencia normal	<ol style="list-style-type: none">1. El administrador diligencia la información requerida para una nueva elección.2. Envía el formulario diligenciado.3. Se valida la información del formulario<ol style="list-style-type: none">a. Si se registra correctamente, el sistema mostrará mensaje de confirmación.
Excepciones	<ol style="list-style-type: none">1. Si la información no se puede validar<ol style="list-style-type: none">b. Se mostrará un mensaje informando del error
Comentarios	

Elaborado por: Autor.

4.3.1.4.6.2 Iniciar.

Tabla 12: CU-GE-02 Iniciar Elección

Descripción	El sistema permitirá dar inicio a un proceso de elección previamente registrada en el sistema.
Precondición	El usuario administrador ha iniciado sesión y ha indicado que desea iniciar una elección previamente seleccionada, esta elección debe tener candidatos asignados y que haya votantes registrados.
Secuencia normal	<ol style="list-style-type: none">1. El sistema enviará una alerta de confirmación indicando si está seguro continuar con el proceso.<ol style="list-style-type: none">a. Si el administrador responde afirmativamente, se llevará a cabo el inicio de la elección en cuestión.b. Si el administrador cancela el proceso no se dará inicio a la elección seleccionada.2. En cualquiera de los dos casos, se cierra la alerta de confirmación y se invoca el caso de uso CU-GE-06

Excepciones	
Comentarios	

Elaborado por: Autor.

4.3.1.4.6.3 Finalizar.

Tabla 13: CU-GE-03 Finalizar Elección

Descripción	El sistema podría finalizar automáticamente una elección para clausurar el proceso de elección. El sistema permitirá al administrador finalizar una elección
Precondición	Cumplir con el parámetro de finalización, se tiene en cuenta la fecha y hora agregada al momento de registrar la elección o El administrador ha iniciado sesión y ha indicado que desea finalizar una elección previamente seleccionada.
Secuencia normal	<p>Cuando el administrador ha indicado finalizar el proceso.</p> <ol style="list-style-type: none"> 1. El sistema mostrará una alerta de confirmación preguntando si desea continuar con el proceso. <ol style="list-style-type: none"> a. Si desea continuar el proceso se finalizará la elección.

	<p>b. Si se cancela, no se finalizará la elección.</p> <p>2. En cualquier de los dos casos, se cerrar la alerta de confirmación y se invocará el caso de uso CU-GE-06 Automáticamente</p> <p>a. El sistema llevará a cabo finalizar la elección</p>
Excepciones	
Comentarios	

Elaborado por: Autor.

4.3.1.4.6.4 Modificar elección.

Tabla 14: CU-GE-04 Modificar Elección

Descripción	El sistema permitirá modificar los parámetros de una elección.
Precondición	El usuario administrador ha iniciado sesión y ha indicado que desea modificar una elección previamente seleccionada.
Secuencia normal	<ol style="list-style-type: none">1. El administrador diligencia la información requerida.2. Envía el formulario diligenciado.3. Se valida la información del formulario<ol style="list-style-type: none">b. Si se modifica correctamente, el sistema mostrará mensaje de confirmación.
Excepciones	Si la información no se puede validar, se mostrará un mensaje informando del error
Comentarios	

Elaborado por: Autor.

4.3.1.4.6.5 Eliminar elección.

Tabla 15: CU-GE-05 Eliminar Elección

Descripción	El sistema permitirá eliminar una elección
Precondición	El usuario administrador ha iniciado sesión y ha indicado que desea eliminar una elección que no ha sido iniciada.
Secuencia normal	<ol style="list-style-type: none">1. El sistema mostrará una alerta de confirmación preguntando si desea continuar con el proceso.<ol style="list-style-type: none">a. Si desea continuar el proceso se eliminará la elección.b. Si se cancela, no se elimina la elección.2. En cualquier de los dos casos, se cerrará la alerta de confirmación y se invocará el caso de uso CU-GE-06
Excepciones	
Comentarios	

Elaborado por: Autor.

4.3.1.4.6.6 Listar elecciones.

Tabla 16: CU-GE-05 Listar elecciones

Descripción	El sistema permitirá listar las elecciones que se hayan registrado.
Precondición	El usuario administrador ha iniciado sesión y ha indicado que listar las elecciones.
Secuencia normal	<ol style="list-style-type: none">1. El sistema visualizará las elecciones que están registradas en el sistema, podrá elegir la opción de iniciar o finalizar elección, modificar y eliminar<ol style="list-style-type: none">a. Si el usuario administrador selecciona iniciar se aplicará el caso de uso CU-GE-02b. Si el usuario administrador selecciona finalizar se llevará a cabo el caso de uso CU-GE-03c. Si el usuario administrador selecciona modificar se aplicará el caso de uso CU-GE-04d. Si el usuario administrador selecciona eliminar continuará en el caso de uso CU-GE-05

Excepciones	Si no hay elecciones registradas se mostrará el mensaje 'No hay elecciones registradas'
Comentarios	

Elaborado por: Autor.

4.3.1.4.7 Operaciones de votantes.

4.3.1.4.7.1 Registrar.

Tabla 17: CU-GV-01 Registrar Votante

Descripción	El sistema permitirá registrar un votante
Precondición	El usuario votante se registrará en la página inicial, validando su registro con su cedula de identificación y correo electrónico.
Secuencia normal	<ol style="list-style-type: none"> 1. El usuario votante llena la información requerida en el formulario. 2. Envía el formulario diligenciado 3. Se valida la información del formulario <ol style="list-style-type: none"> a. Si se registra correctamente, el sistema mostrará

	mensaje de confirmación.
Excepciones	Si la información no se puede validar, se mostrará un mensaje informando del error

Comentarios

4.3.1.4.7.2 Listar Votantes.

Tabla 18: Listado de votantes

Descripción	El sistema permitirá mostrar el listado de los votantes registrados en el sistema.
Precondición	El usuario administrador ha iniciado sesión y ha indicado que desea ver el listado de los votantes registrados
Secuencia normal	El sistema visualizará los votantes que están registrados en el sistema
Excepciones	Si no hay elecciones registradas se mostrará el mensaje 'No hay elecciones registradas'
Comentarios	

Elaborado por: Autor.

4.3.1.4.8 Consultar reportes.

4.3.1.4.8.1 Mostrar resultados.

Tabla 19: CU-CR-01 Mostrar Resultados

Descripción	El sistema permitirá mostrar los resultados de una elección.
Precondición	Se ha indicado al sistema que se desea ver los resultados de una elección.
Secuencia normal	<ol style="list-style-type: none">1. Seleccionar la elección.2. Confirmar que se desea mostrar los resultados.
Excepciones	Si no se puede mostrar los resultados de la elección seleccionada se mostrará un mensaje indicando el error.
Comentarios	

Elaborado por: Autor.

4.3.1.4.9 Efectuar voto.

4.3.1.4.9.1 Validar votante.

Tabla 20: CU-EV-01 Validar Votante

Descripción	El sistema permitirá validar un votante que desea efectuar su voto.
Precondición	Se ha seleccionado una elección y se ha indicado al sistema hacer efectivo un voto, el votante no debe haber votado en la elección seleccionada.
Secuencia normal	<ol style="list-style-type: none">1. Digitar el número de identificación registrado en el sistema.2. Enviar información diligenciada.3. Validar información<ol style="list-style-type: none">b. Si se validó correctamente la información, se invocará el caso de uso CU-EV-02.
Excepciones	Si no se puede validar la información. a. El sistema mostrar un mensaje indicando el error.
Comentarios	

Elaborado por: Autor.

4.3.1.4.9.2 Seleccionar candidato.

Tabla 21: CU-EV-02 Seleccionar Candidato

Descripción	Se ha validado la identidad del votante en el sistema.
Precondición	<ol style="list-style-type: none">1. Mostrar el listado de los candidatos.2. Seleccionar el candidato por el cual se efectuará el voto.3. Confirmar la selección.<ol style="list-style-type: none">a. Si se confirma se invocará el caso de uso CU-EV-03b. Si se cancela, se invocará este caso de uso.
Secuencia normal	<ol style="list-style-type: none">4. Digitar el número de identificación registrado en el sistema.5. Enviar información diligenciada.6. Validar información<ol style="list-style-type: none">c. Si se validó correctamente la información, se invocará el caso de uso CU-EV-02.
Excepciones	Si no se puede validar la información. <ol style="list-style-type: none">a. El sistema mostrará un mensaje indicando el error.
Comentarios	

Elaborado por: Autor.

4.3.1.4.9.3 Confirmar voto.

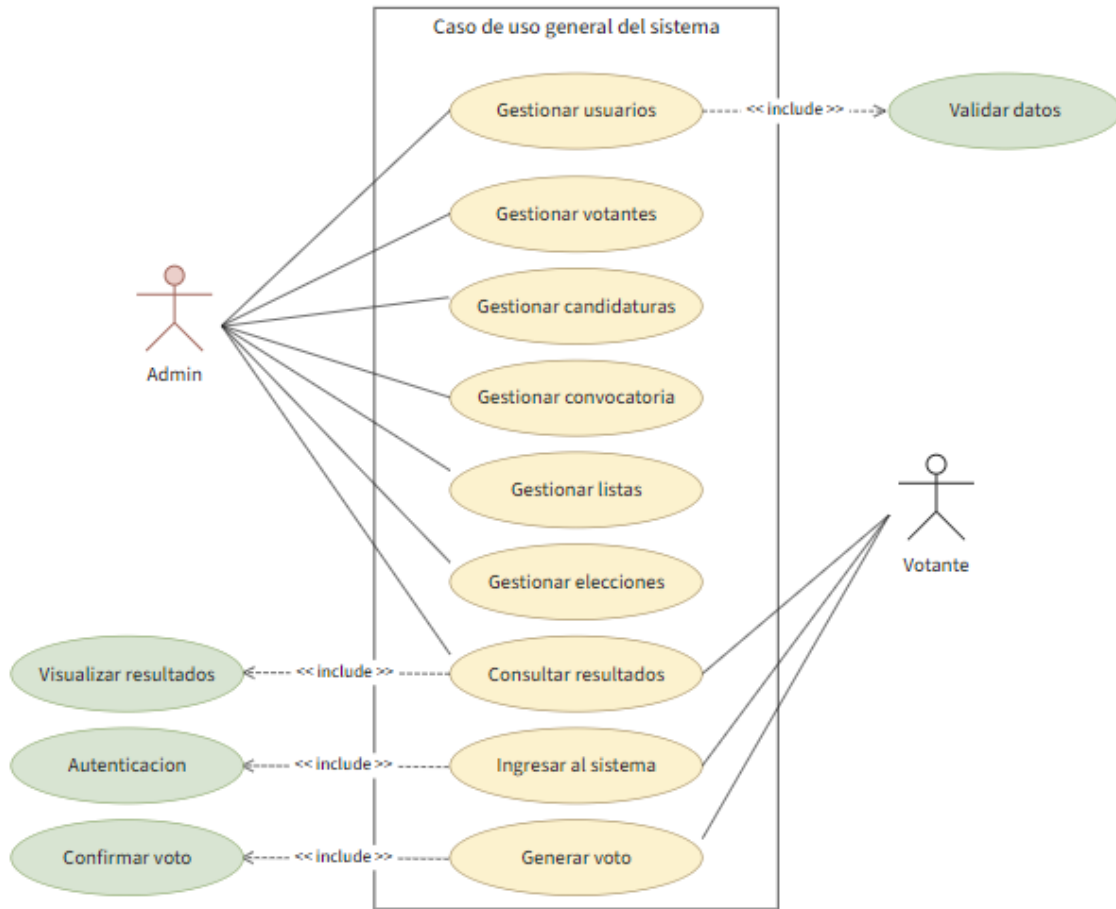
Tabla 22: CU-EV-03 Confirmar Voto

Descripción	El sistema permitirá confirmar el voto por el candidato elegido.
Precondición	Se ha seleccionado al candidato y se ha confirmado la selección.
Secuencia normal	<ol style="list-style-type: none">1) Se solicitará confirmar el voto.<ol style="list-style-type: none">a. Si se confirma, se efectuará el voto.b. Si se cancela, no se efectuará el voto.2) En cualquiera de los casos, se mostrará un mensaje indicando el resultado de la operación y se invocará el caso de uso CU-EV-01
Excepciones	
Comentarios	

Elaborado por: Autor.

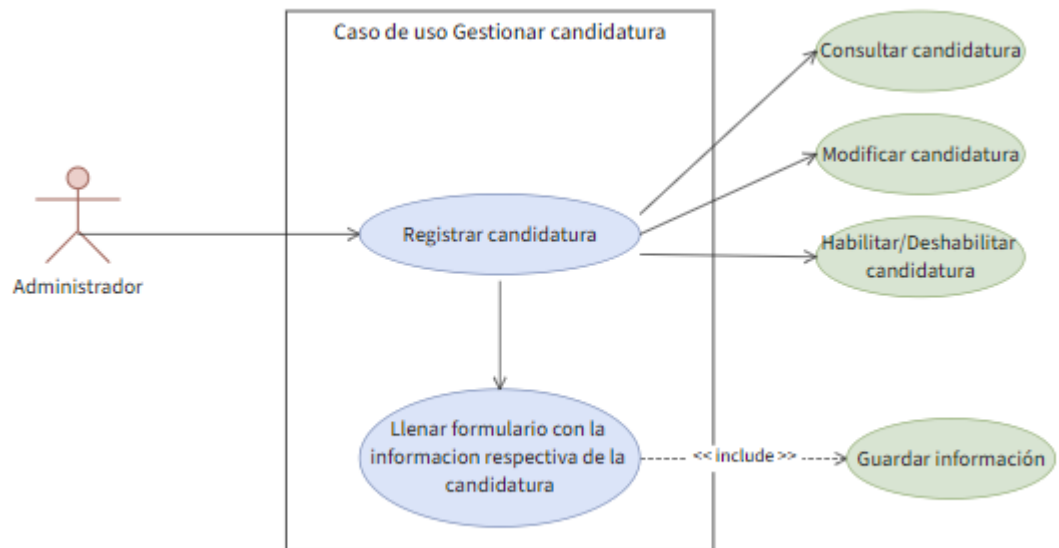
4.3.1.4.10 Casos de uso.

4.3.1.4.10.1 Diagrama general.

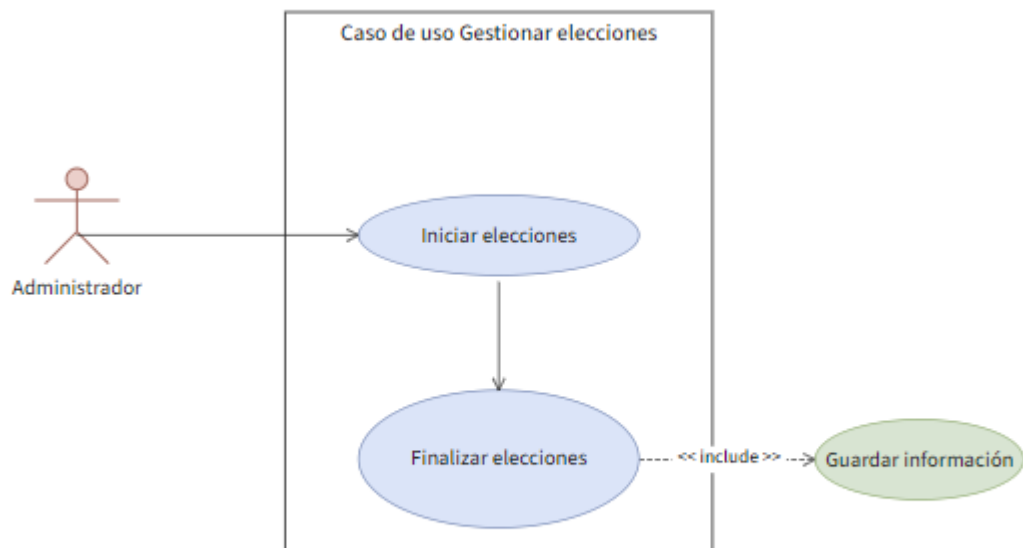


Caso de uso general del sistema, se describen los casos de uso específicos y los actores que interactúan con el sistema.

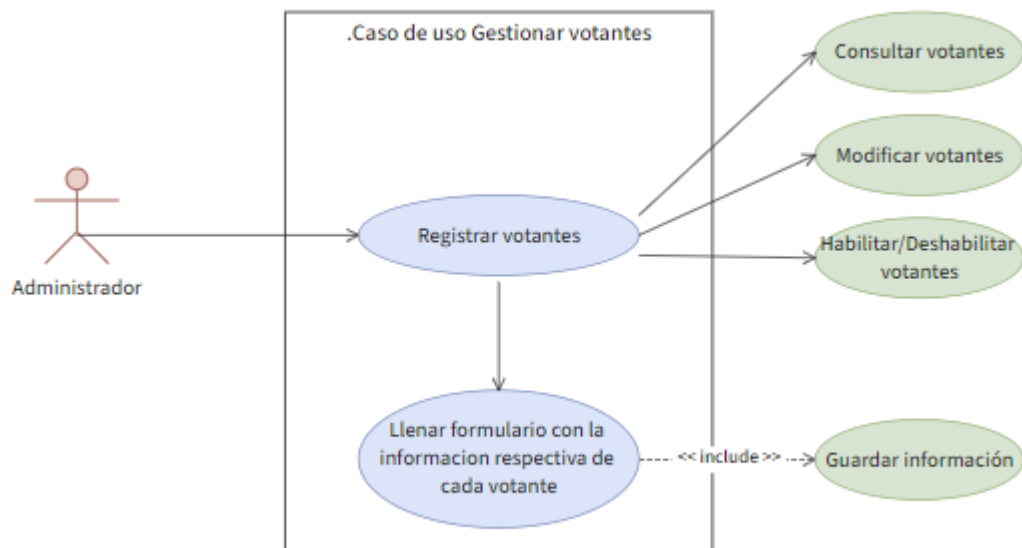
4.3.1.4.10.2 Gestión de candidatos.



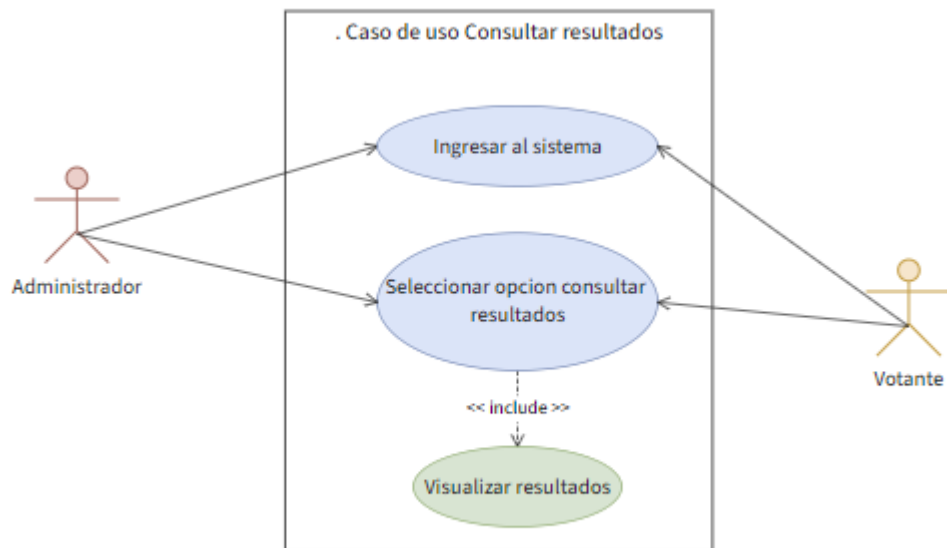
4.3.1.4.10.3 Gestión de elecciones.



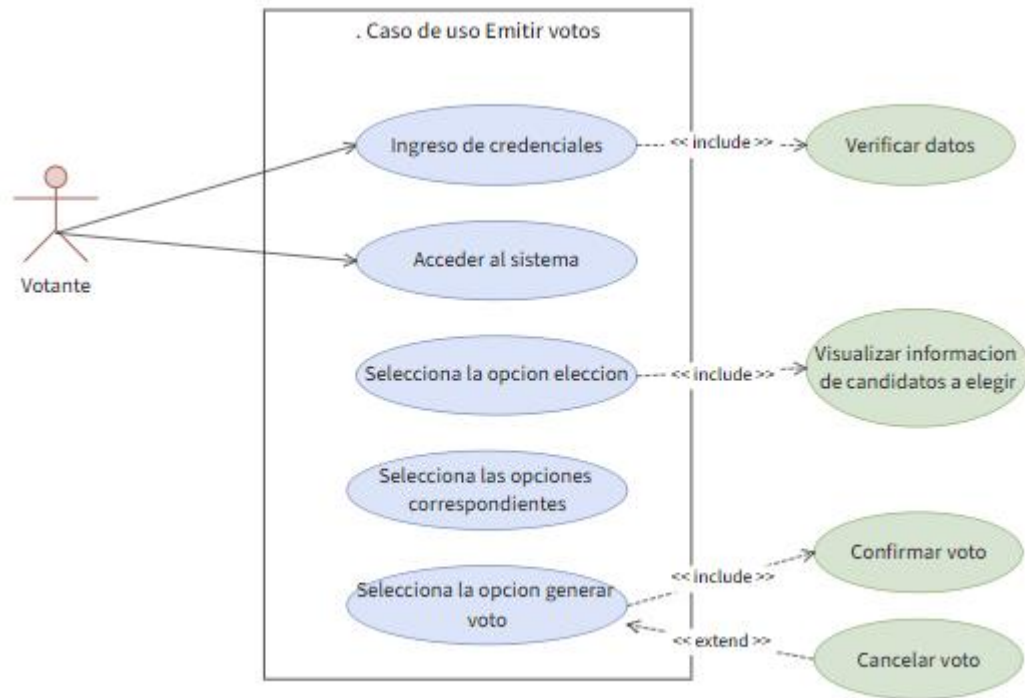
4.3.1.4.10.4 Gestión de votantes.



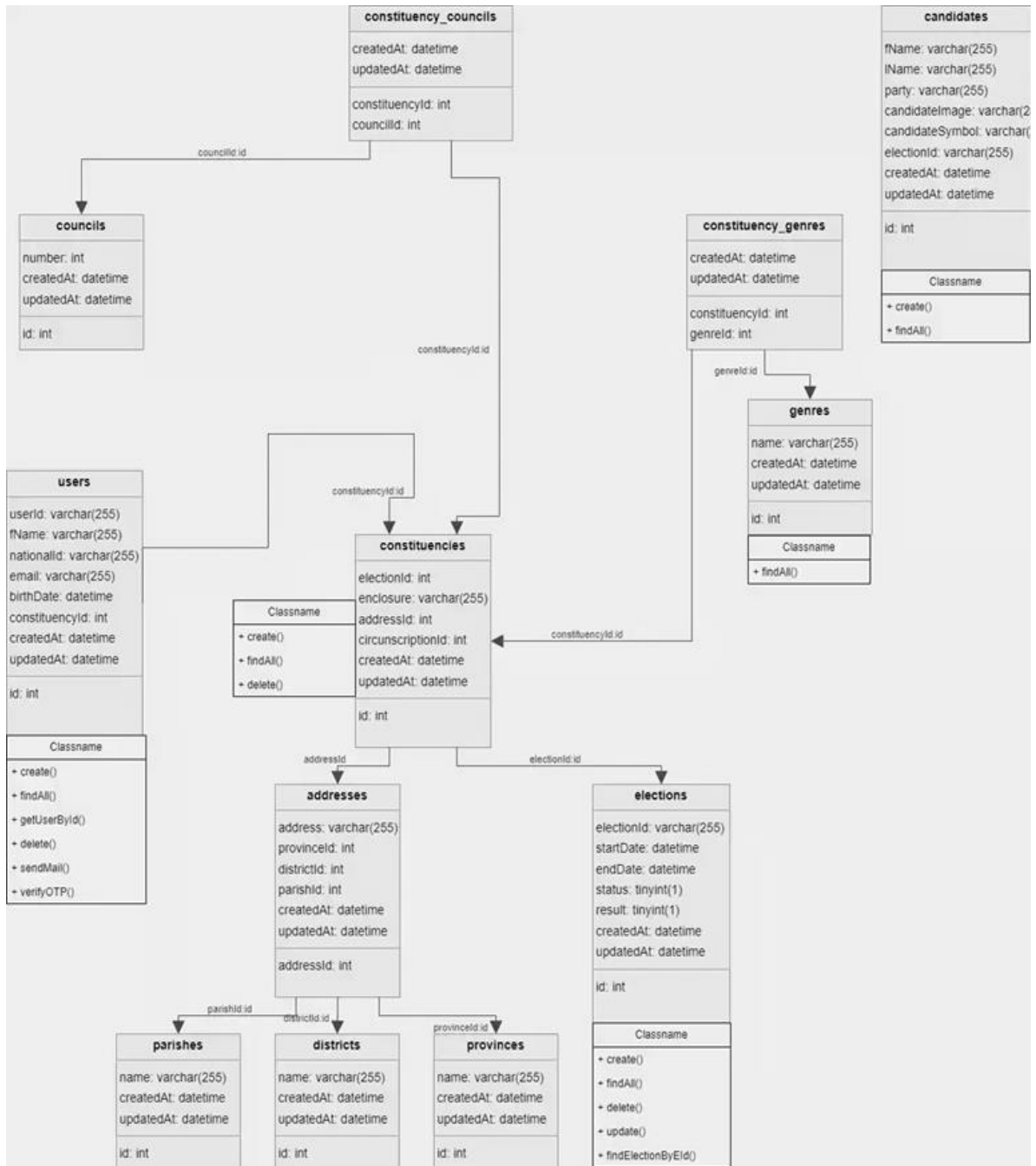
4.3.1.4.10.5 Consulta de resultados y reportes



4.3.1.4.10.6 Emisión de voto.



4.3.1.4.11 Diagrama de clases.



4.3.1.5 El voto electrónico y Blockchain: Diseño.

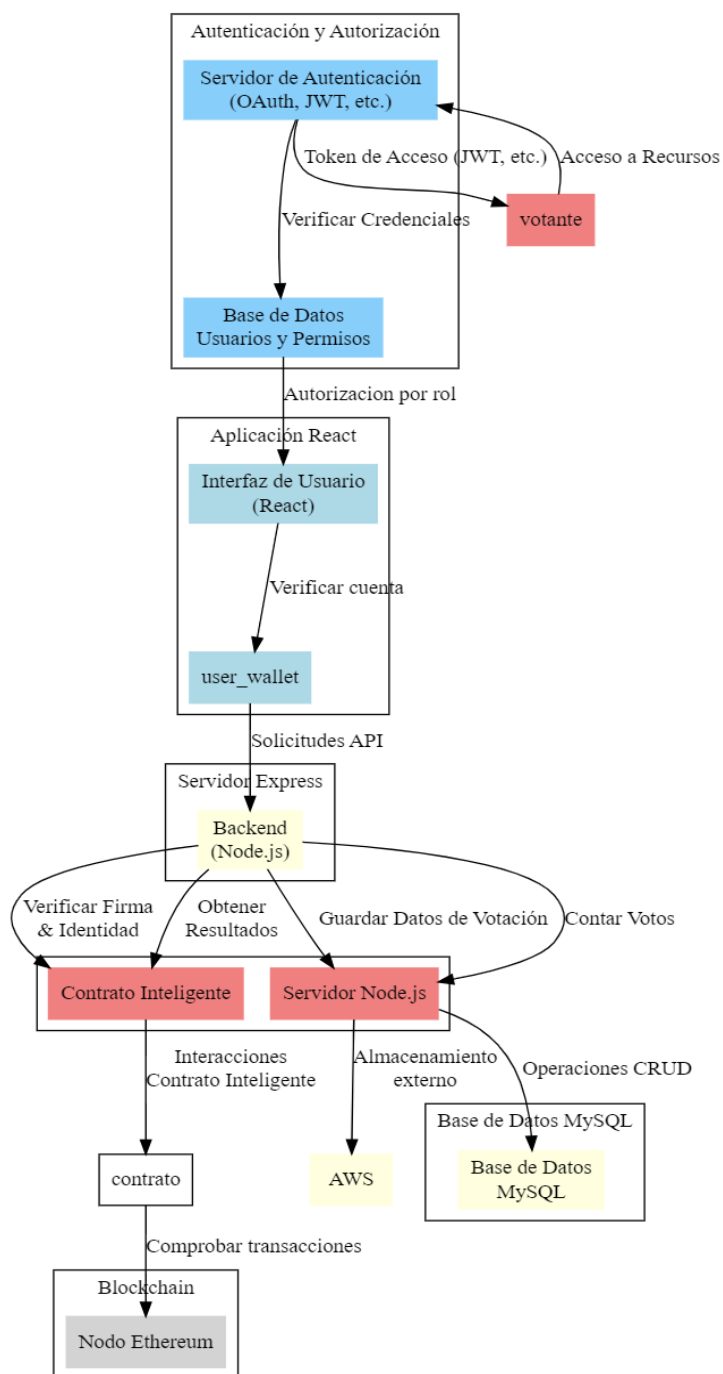
4.3.1.5.1 Definición de la arquitectura del sistema.

La arquitectura de este sistema se fundamentó en el modelo cliente-servidor, dada la clara separación entre la interacción con el usuario y la parte lógica-funcional de la plataforma. Este enfoque posibilita el desarrollo de aplicaciones cliente en diversas plataformas, tales como web, móviles y de escritorio.

Durante la creación del sistema, se optó por aplicar la metodología de programación por capas, utilizando el conocido patrón arquitectónico M.V.C (Modelo, Vista, Controlador). Esta arquitectura se destaca por su habilidad para dividir de manera clara la lógica y las interacciones en la aplicación. Emplear este patrón ofrece beneficios significativos al permitir una clara separación entre los datos y la lógica de negocio de la aplicación, por un lado, y la interfaz de usuario y el módulo encargado de gestionar los eventos y las comunicaciones, por otro. (Castillo Yagual & Coronel Suárez, 2023)

Esta estructura arquitectónica facilita la idea de reutilización de código y la distinción de conceptos, aspectos fundamentales que simplifican tanto el proceso de desarrollo de aplicaciones como su posterior mantenimiento. Estas ventajas resultan vitales para respaldar los requerimientos no funcionales del sistema. (Castillo Yagual & Coronel Suárez, 2023)

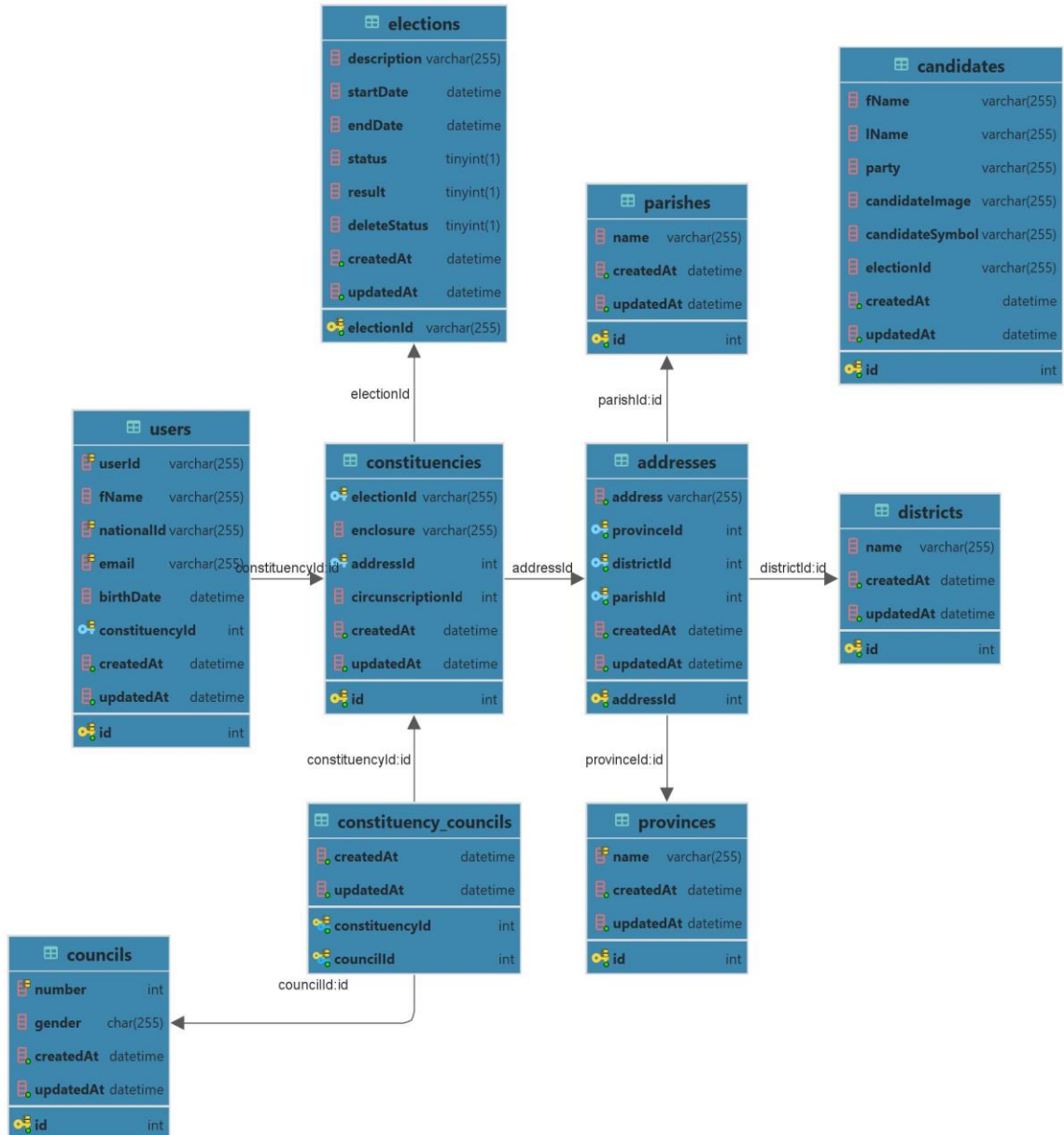
Figura 7. Arquitectura del sistema. Elaborado por autor.



Nota. Arquitectura implementada en el desarrollo de la plataforma.

4.3.1.5.2 Diagrama Entidad-Relación.

Figura 8. Diagrama Entidad-Relación.



4.3.1.5.3 Modelo.

En esta etapa, se establecen las directrices de operación del negocio y se delimitan tanto los datos como la funcionalidad integrados en la aplicación mediante mecanismos de persistencia. Si se producen modificaciones en los datos, se informa a la vista y, en ciertas instancias, al controlador. La responsabilidad recae en responder a las peticiones de la vista para que el usuario pueda visualizarlas a través de las instrucciones (eventos) que el controlador envía. (Castillo Yagual & Coronel Suárez, 2023)

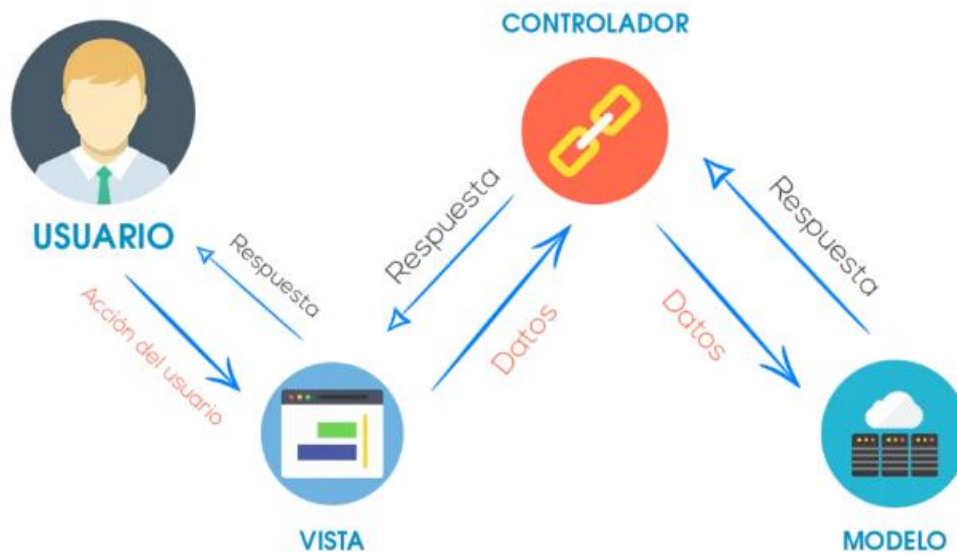
4.3.1.5.4 Vista.

La interfaz de usuario, también denominada como la forma en que el usuario interactúa con la aplicación, posibilita la visualización de los datos (en formato HTML) de la aplicación para el usuario final, los cuales han sido previamente solicitados al modelo. Es a través de esta interfaz que el usuario interactúa con la aplicación, ya sea para enviar o recibir datos del modelo. Es importante destacar que los eventos generados son gestionados por el controlador. (Castillo Yagual & Coronel Suárez, 2023)

4.3.1.5.5 Controlador.

La capa del controlador es la que más participación tiene en esta arquitectura, debido a que es la encargada de interactuar con las capas del modelo y vista. Actúa como un puente entre el modelo y las vistas, encargándose de responder a los eventos y/o acciones que el usuario inicia en la aplicación. Este componente gestiona los datos enviados por el usuario y, en consecuencia, actualiza el modelo según la solicitud realizada (Castillo Yagual & Coronel Suárez, 2023).

Figura 9. Diagrama que representa el funcionamiento del patrón M.V.C.



Nota. Patrón de diseño implementado para el desarrollo Backend de la plataforma

4.3.1.5.6 Arquitectura en el cliente.

En el ámbito del frontend, se implementó la arquitectura basada en componentes, una metodología reconocida por su eficacia en la organización y desarrollo de la interfaz de usuario. Este enfoque se centra en la construcción de la aplicación dividiéndola en piezas independientes y reutilizables, llamadas componentes. Cada módulo simboliza una parte determinada de la interfaz y encapsula tanto su presentación visual como su lógica.

Esta arquitectura facilita la modularidad y reutilización del código, permitiendo a los desarrolladores trabajar en componentes individuales de manera independiente. Además, posibilita una gestión eficaz del estado de la aplicación, asegurando un flujo de datos uniforme y una respuesta ágil ante las interacciones del usuario.

La separación clara entre componentes optimiza el mantenimiento y la escalabilidad de la aplicación, permitiendo actualizaciones y modificaciones sin afectar otras partes del sistema. Además, se garantiza una experiencia de usuario coherente y atractiva al reutilizar componentes en diferentes secciones de la aplicación.

4.3.1.6 Fase IV: Construcción del Sistema de Información.

4.3.1.6.1 Preparación del Entorno de Generación y Construcción,

El propósito de esta tarea fue garantizar que se contara con todos los recursos y herramientas necesarias para llevar a cabo la codificación del sistema de información. Estos recursos incluyen la preparación de los gestores de bases de datos, las librerías de programas, las utilidades para generar código, así como documentación de las tecnologías a usar y archivos de prueba, entre otros.

4.3.1.6.2 Ambiente de desarrollo.

- Servidor: Node – Express
- Arquitectura: M.V.C (Modelo-Vista-Controlador)
- Frontend: React
- Backend: NodeJs – Express
- Entorno Blockchain: Turffle - Ganache
- Solidity (Blockchain)
- Base de datos: MySQL
- Nube: AWS S3

4.3.1.6.3 Descripción de pantallas

4.3.1.6.3.1 Inicio de sesión.

Figura 10. Pantalla Inicio sesión votante

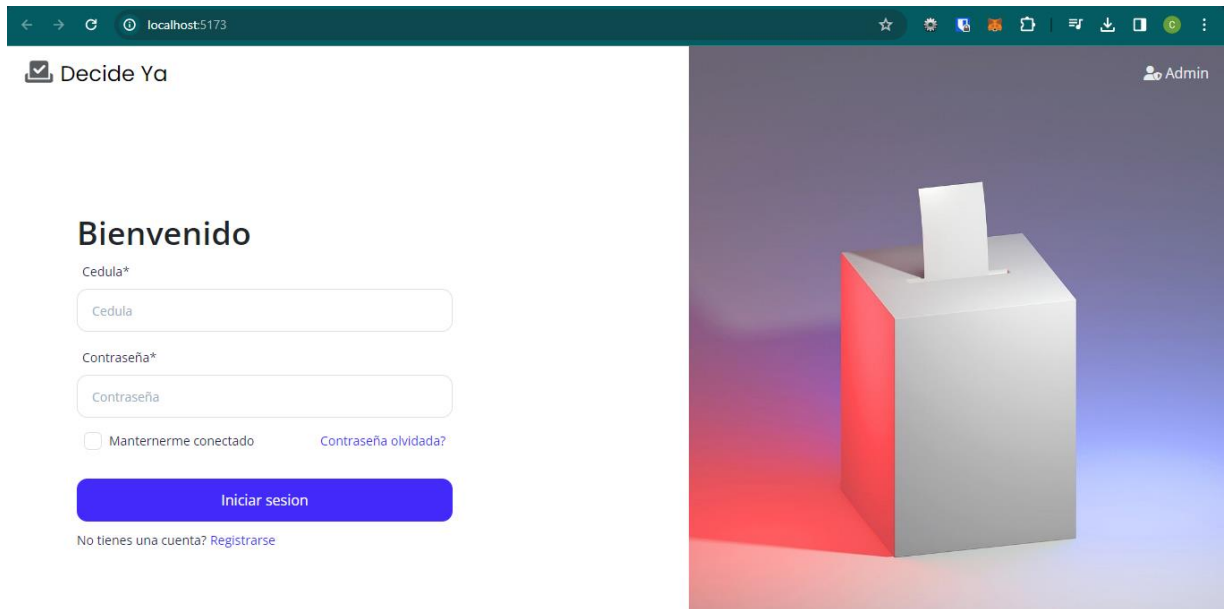


Figura 11. Pantalla Inicio Sesión administrador

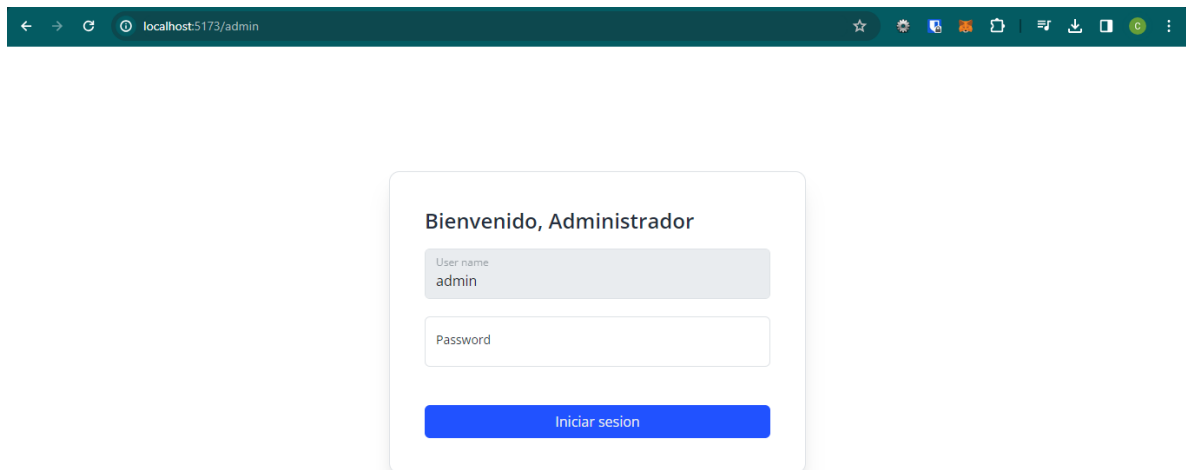


Figura 12. Dashboard principal del administrador.

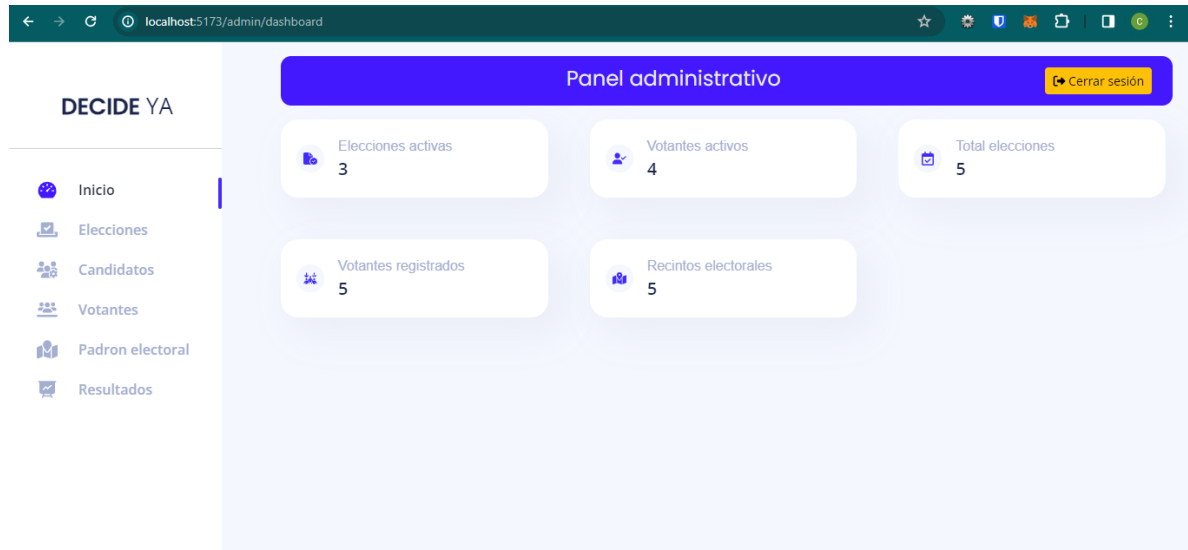


Figura 13. Panel de gestión de elecciones



Figura 14. Panel para agregar candidato

DECIDE YA

- Inicio
- Elecciones
- Candidatos
- Votantes
- Padron electoral
- Resultados

Gestion de candidatos

Cerrar sesión

Selecciona imagen de candidato
Seleccionar archivo Ningu... selec.

Selecciona imagen de partido politico
Seleccionar archivo Ningu... selec.

Primer nombre

Apellido

Partido

Eleccion

Agregar candidato

Figura 15. Listado de votantes

DECIDE YA

- Inicio
- Elecciones
- Candidatos
- Votantes
- Padron electoral
- Resultados

Gestión de votantes

Cerrar sesión

#	Usuario	Cedula	Accion
1	LOPEZ AGUIRRE CHRISTIAN ADRIAN	0932320658	Verified
2	MELENDREZ MUÑOZ ADRIANA CAMILLE	0912236114	Verified
3	MENDOZA CONTRERAS ARIEL ANDRES	1203646664	Verify
4	LOPEZ AGUIRRE STEPHANO SANTIAGO	0943798330	Verified
5	MUJICA ZAMBRANO DANIEL ANTONIO	1715784292	Verified

Figura 16. Gestión de padrones electorales.

The screenshot shows the 'Gestión de padrones' interface. On the left is a sidebar with 'DECIDE YA' and navigation links: Inicio, Elecciones, Candidatos, Votantes, Padron electoral (selected), and Resultados. The main content area has a search bar 'Buscar padron electoral' and a table with the following data:

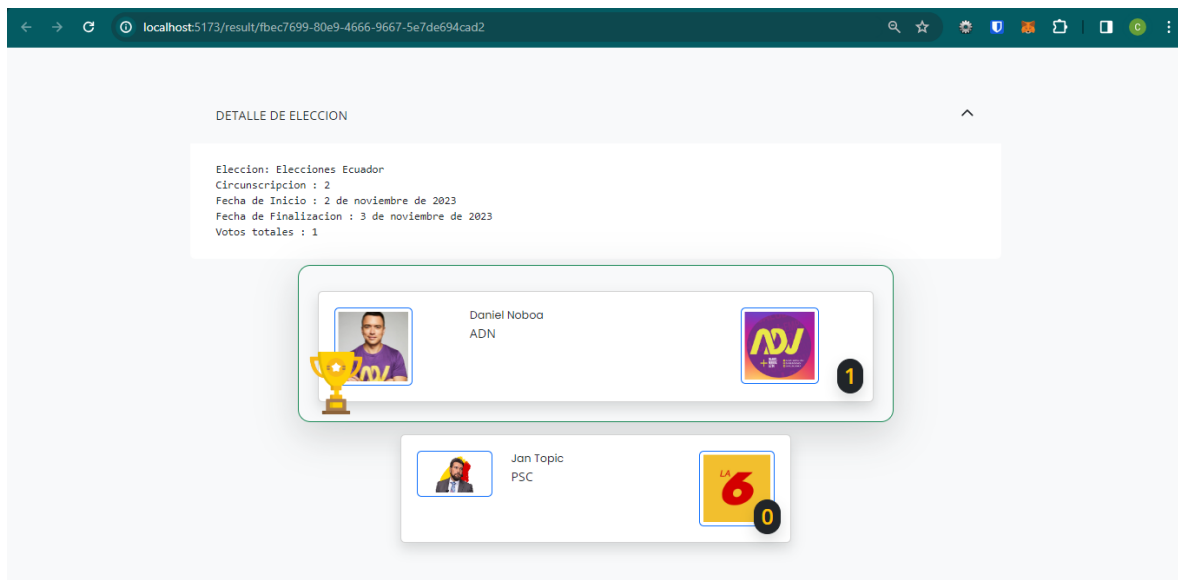
RECINTO	DIRECCION	PROVINCIA	CANTÓN	PARROQUIA	JUNTA	ACCIONES
UNIDAD EDUCATIVA MATILDE AMADOR SANTISTEVAN	Luis Urdaneta 209 entre Baquerizo Moreno y General Córdova	Guayas	Guayaquil	Tarqui	248 - M	Editar Eliminar
UNIDAD EDUCATIVA BRISAS DEL RIO	Cdla. Brisas del Rio MZ. D3 Solares 21-26 y Av. José María Egas	Guayas	Guayaquil	Tarqui	1 - F	Editar Eliminar
ACADEMIA NAVAL GUAYAQUIL	Av. Antonio Parra Velasco Mz.B / Solar 1 y 2	Guayas	Guayaquil	Tarqui	180 - M	Editar Eliminar
LICEO CRISTIANO DE GUAYAQUIL	Juan Tanca Marengo km 2.5 y Rosa Campuzano	Guayas	Guayaquil	Tarqui	34 - F	Editar Eliminar
UNIDAD EDUCATIVA LICEO ALBONOR	Ciudadela La Alborada XIII Etapa	Guayas	Guayaquil	Tarqui	122 - M	Editar Eliminar

Figura 17. Pantalla - listado de resultados

The screenshot shows the 'Resultados de las elecciones' interface. On the left is a sidebar with 'DECIDE YA' and navigation links: Inicio, Elecciones, Candidatos, Votantes, Padron electoral, and Resultados (selected). The main content area has a table with the following data:

#	Eleccion	Descripción	Ver resultado
1	fbec7699-80e9-4666-9667-5e7de694cad2	Elecciones Ecuador	Ver

Figura 18. Interfaz de resultados de votaciones



CONCLUSIONES

Basado en los objetivos generales se llega a lo siguiente:

En primer lugar se logró fundamentar la incorporación de la tecnología en el ámbito de los procesos electorales identificando los beneficios de la tecnología en cuanto a vulnerabilidades y amenazas a la seguridad de estos sistemas informáticos.

Luego de revisar la metodología propuesta para definir el prototipo y simulación en se pudieron extraer varias conclusiones:

Destacar la importancia de identificar y definir los requisitos del prototipo desde el inicio. Este enfoque contribuye a una comprensión clara de las funcionalidades esenciales que se deben demostrar, incluyendo aspectos como seguridad, usabilidad y transparencia.

La elección adecuada de tecnologías es un paso crucial en el desarrollo de la plataforma. Así destacando la importancia de seleccionar herramientas y frameworks apropiados, asegurando el desarrollo efectivo del prototipo.

Es esencial para visualizar la estructura tecnológica y los patrones de diseño. Esto proporciona una guía clara para el desarrollo y la integración de funcionalidades.

Tal como se ha demostrado, se implementó el sistema siguiendo la metodología Extreme Programming (XP), lo que habilitó la consecución de mejoras continuas durante las iteraciones del proyecto. Como resultado de esta aproximación, se logró con éxito la satisfacción de los requisitos estipulados dentro del marco temporal establecido. En esta perspectiva, el proceso se inició con la definición de roles, la elaboración de historias de usuario y seguidamente se efectuó la planificación de las iteraciones junto con sus respectivas tareas, culminando con la fase de desarrollo del sistema.

Se logró el desarrollo de un prototipo el cual habilita la instauración de un proceso electoral y, gracias a la inclusión de un contrato inteligente en una red blockchain,

adquiere las funcionalidades necesarias para llevar a cabo el proceso de sufragio, escrutinio y generación de resultados de forma descentralizada e inalterable.

La evaluación del sistema mediante la aplicación de los principios heurísticos de Nielsen permitió identificar y abordar eficazmente las deficiencias en cuanto a usabilidad y experiencia del usuario. Esta metodología de evaluación demostró ser una herramienta efectiva para medir y mejorar el rendimiento del sistema, lo que a su vez contribuye al logro de un sistema más eficaz y exitoso en términos de satisfacción y usabilidad por parte de los usuarios.

RECOMENDACIONES

Se sugiere una implementación gradual de la tecnología Blockchain en procesos electorales. Comenzar con elecciones piloto permitirá evaluar su rendimiento y abordar posibles problemas antes de una adopción a mayor escala.

Con el objetivo de lograr una mayor calidad en el producto de software, es esencial emplear una metodología que facilite el proceso de desarrollo. En este caso, se optó por Extreme programming y es recomendable que se la pueda unir a una metodología ágil como Scrum, la cual, mediante la realización de iteraciones, permite una mejora continua del producto. No obstante, para hacer uso efectivo de una metodología, es fundamental investigar y familiarizarse con la documentación asociada, lo que proporciona un conjunto de buenas prácticas.

En el contexto de la creación de aplicaciones basadas en tecnología blockchain (DApps), es altamente recomendable adquirir un profundo entendimiento de su funcionamiento y características. Esto resulta fundamental para aprovechar al máximo los beneficios que esta tecnología ofrece. Además, es importante adquirir competencias en algún lenguaje de programación, como Solidity, que permita la creación de contratos inteligentes. Asimismo, es crucial investigar las diversas plataformas presentes en el ecosistema blockchain.

En el desarrollo de aplicaciones descentralizadas (DApps), se aconseja enviar únicamente los datos más sensibles y esenciales a la blockchain, con el propósito de evitar costos innecesarios a largo plazo.

Debido a que es una herramienta nueva, es importante que los usuarios sean capacitados, a través de los manuales o de forma presencial, para que puedan realizar un buen uso de los módulos del aplicativo.

Bibliografía

- Alvarez, S. (10 de Agosto de 2022). *Precognis*. Obtenido de Qué es Modelo Vista Controlador en el mundo de la programación. Ventajas y desventajas.: <https://www.precognis.com/blog/modelo-vista-controlador/>
- Bravo Cuero, A. (2023). *Vulnerabilidades en los Smart Contracts: (DoS) Denegación de Servicio*. Obtenido de LinkedIn: <https://www.linkedin.com/pulse/vulnerabilidades-en-los-smart-contracts-dos-de-alfredo-bravo-cuero/>
- Castillo Yagual, C., & Coronel Suárez, M. (28 de 06 de 2023). Frameworks PHP basados en la arquitectura Modelo-Vista-Controlador para desarrollo de aplicaciones web. *Revista Científica y Tecnológica UPSE*, 10(1), 70-78. doi:<https://doi.org/10.26423/rctu.v10i1.703>
- Consultores, B. (2 de Marzo de 2020). *Técnicas de recolección de datos para realizar un trabajo de investigación*. Obtenido de Online-Tesis: <https://online-tesis.com/tecnicas-de-recoleccion-de-datos-para-realizar-un-trabajo-de-investigacion/>
- Cuvi Santacruz, M., & Franco Cortázar, C. (2023). Principios rectores de los smart contracts en el ordenamiento jurídico ecuatoriano. *YACHANA*, 12(1). Obtenido de <http://revistas.ulvr.edu.ec/index.php/yachana/article/view/851>
- de Carvalho, L., Martinez Évora, Y., & Zem-Mascarenhas, S. (2016). Evaluación de usabilidad de un prototipo de tecnología digital. *Revista Latino-Am. Enfermagem*, 24. doi:<https://doi.org/10.1590/1518-8345.1054.2777>
- Defelipe Díaz, S. (21 de Junio de 2018). Blockchain en Colombia sí, criptomonedas no. *Impactotic*.
- Demestichas, K., Nikolaos, P., Alexakis, T., & Evgenia, A. (15 de Junio de 2020). Blockchain in Agriculture Traceability Systems. *Applied Sciences*, 10(12), 1-22. doi:<https://doi.org/10.3390/app10124113>
- Dhulavvagol, P., Bhajantri, V., & Totad, S. (2020). Blockchain Ethereum Clients Performance Analysis Considering E-Voting Application. *Procedia Computer Science*, 167, 2506-2515. doi:<https://doi.org/10.1016/j.procs.2020.03.303>

Domínguez Padilla, C. (2022). LA REVOLUCIÓN BLOCKCHAIN Y LOS SMART. *Actualidad Jurídica Iberoamericana N, 16*, 1088-1109.

Euskadi.eus. (2022). *Voto electrónico en el mundo*. Obtenido de euskadi.eus:
<https://www.euskadi.eus/informacion/voto-electronico-voto-electronico-en-el-mundo/web01-a2haukon/es/>

García, C. (9 de Febrero de 2018). *Ecuador ya tiene su primer cajero automático de múltiples criptomonedas*. Obtenido de Criptonoticias:
<https://www.criptonoticias.com/mercados/ecuador-tiene-primer-cajero-automatico-multiples-criptomonedas/>

Garzón Sherdek, K., & Cahuasquí Cevallos, S. (2021). Sistema electoral ecuatoriano, ¿concentrador o proporcional?: una aproximación crítica a las reformas del 2019-2020. *Estado & comunes, revista de políticas y problemas públicos, 1(12)*, 17-36.

Hegedús, P. (2019). Towards Analyzing the Complexity Landscape of Solidity Based Ethereum Smart Contracts. *Technologies, 7(1)*, 6. doi:<https://doi.org/10.3390/technologies7010006>

Horni, M. (1 de Octubre de 2021). *Contribución de la Organización de Estados Americanos a la cooperación*. Obtenido de Universidad Siglo 21:
<https://repositorio.uesiglo21.edu.ar/handle/ues21/23983>

IBM. (2022). *¿Qué es la tecnología blockchain?* Obtenido de IBM:
<https://www.ibm.com/eses/topics/what-is-blockchain>

ihodl. (2017). *Cómo van los contratos inteligentes a cambiar nuestras vidas*. Obtenido de ihodl:
<https://es.ihodl.com/tutorials/2017-07-13/como-van-los-contratos-inteligentes-cambiar-nuestras-vidas/>

Lajpop Ajpacajá, K. (s.f.). Voto Electrónico con “Blockchain”: La Unión entre la Tecnología y Sociedad. *Revista Científica del Sistema de Estudios de Postgrado de la Universidad de San Carlos de Guatemala, 4(1)*, 85-93. doi:<https://doi.org/10.36958/sep.v4i1.79>

Lifeder. (2020). *Enfoque de la investigación: tipos y características*. Obtenido de
<https://www.lifeder.com/enfoque-investigacion/>

Limanorum. (Octubre de 2018). *Impacto del uso de Blockchain en materia electoral*. Obtenido de repository.usta.edu.co:

<https://www.te.gob.mx/transparencia/media/files/b7156d608ecac4d.pdf>

Llamas Covarrubias, J. Z., Llamas Covarrubias, I. N., & Llamas Covarrubias, B. A. (2021).

Características de validez en el voto electrónico mediante Blockchain. *Revista de Ciencia de la Legislación*(10), 10-14.

Manero, P. (31 de mayo de 2022). *Estudiocontar*. Obtenido de Estudios de factibilidad de un proyecto 2022: qué son y cuál es su objetivo:

<https://blog.estudiocontar.com/2022/05/31/estudios-de-factibilidad-que-son/>

Muñoz, D. (17 de Julio de 2023). *Blockchain: Una exploración de sus tipos y usos*. Obtenido de

Linkedin: <https://www.linkedin.com/pulse/blockchain-una-exploraci%C3%B3n-de-sus-tipos-y-usos-dar%C3%ADo-echeverr%C3%ADa-mu%C3%B1oz/?originalSubdomain=es>

Muruganandam, S., & Natarajan, V. (2022). Blockchain Based Adaptive Resource Allocation in Cloud Computing. *Brazilian Archives of Biology and Technology*, 65.

doi:<https://doi.org/10.1590/1678-4324-2022220025>

Nielsen, J. (2006). *Prioritizing Web Usability*. (H. Loranger, & J. Nielsen, Trads.)

Pailiacho Mena, V., Garcés Freireia, E., & Balseca Manzano, J. (2022). Usabilidad del software: Una revisión sobre su evolución conceptual y. *Publicaciones en Ciencias y Tecnología*, 16(2),

121-134. doi:<https://doi.org/10.5281/zenodo.7131510>

Porxas, N., & Cornejo, M. (15 de Enero de 2018). *www.uria.com*. Obtenido de

<https://www.uria.com/documentos/publicaciones/5799/documento/art02.pdf?id=7875>

Rivero, J. (6 de Mayo de 2018). *Transparencia electoral: 5 plataformas blockchain para votaciones*.

Obtenido de Criptonoticias: <https://www.criptonoticias.com/comunidad/transparencia-electoral-5-plataformas-blockchain-para-votaciones/>

Rodriguez, N. (2018). *La Mejor Guia Sobre La Tecnología Blockchain: Una Revolución Para Cambiar*

El Mundo. Obtenido de 101blockchains: <https://101blockchains.com/es/tecnologia-blockchain/>

Sánchez Hernández, D., Lizano Madriz, F., & Sandoval Carvajal, M. (2020). Integración de pruebas remotas de usabilidad en Programación Extrema: revisión de literatura. *UNICIENCIA*, 34(1), 20-31. doi:<http://dx.doi.org/10.15359/ru.34-1.2>

Sánchez Herrera, S. (2021). Sistema de voto electrónico basado en blockchain. *Serie Científica de la Universidad de las Ciencias Informáticas*(14), 9-32.

Tinoco Plasencia, C., Juarez Trinidad, A., Gonzales Rosas, F., & Tamayo Franco, J. (Mayo de 2023). Tecnología Bloc-kchain en Educación: una revisión sistemática. *Revista Conrado*, 19(92), págs. 326-334.

Waldman , J. (Marzo de 2018). Cadena de bloques: aspectos básicos de la cadena de bloques. *MSDN Magazine*, 33(3).

ANEXO

4.4 Anexo 1

Modelo de test de Usuario para Medir la Usabilidad de la Plataforma de Votación Electrónica

Prueba de Usabilidad con los 10 principios heurísticos de Nielsen

PRESENTACIÓN

Agradecemos su participación en este test de usuario que tiene como objetivo evaluar la usabilidad de una plataforma de votación electrónica apoyada por blockchain. Durante esta sesión, te pediremos que realices una serie de tareas y respondas preguntas sobre tu experiencia así nos ayudará a evaluar el sitio web que desarrollamos y detectar posibles fallas que éste tenga.

DATOS ENCUESTADO

Nombre:

Edad:

Experiencia previa en votación electrónica:

Considere lo siguiente:

Antes de comenzar con las preguntas sobre el sitio mismo, queremos comentarle que, en la prueba que hagamos, puede que haya ciertas acciones que no podrá completar. Si eso sucede, representará que el sitio debe ser mejorado y la prueba será exitosa. Si todo sale bien, significará que el sitio fue diseñado pensando en el usuario y también que esta experiencia obtuvo el éxito. La prueba tiene una duración máxima de 30 minutos aproximadamente.

Le vamos a solicitar que durante las operaciones que desarrolle, vaya declarando en voz alta lo que vaya repasando con el fin de que logremos opinar lo que sugiere de lo que va mostrando cada pantalla.

Lea cada pregunta y evalúa tu experiencia en la plataforma de votación electrónica en base a los 10 principios heurísticos de Nielsen.

Proporciona tus respuestas y comentarios de manera honesta y detallada.

Las interrogaciones que le surjan en la navegación sólo las alcanzaremos a manifestar al culminar la prueba.

PREGUNTAS

Estas preguntas se deben hacer cuando el usuario está mirando la pantalla inicial y antes de comenzar a navegar o hacer “click” sobre algún contenido.

1. Visibilidad del Estado del Sistema:

Pregunta 1:

¿Pudiste identificar fácilmente el estado actual del proceso de votación en la plataforma?

Pregunta 2:

¿Te resultó claro saber en qué etapa del proceso de votación te encontrabas en todo momento?

2. Correspondencia entre el Sistema y el Mundo Real:

Pregunta 1:

¿La terminología y los botones utilizados en la plataforma eran comprensibles y correspondían con el proceso de votación real?

Pregunta 2:

¿Le resultó fácil entender cómo transferir sus decisiones y preferencias reales a la plataforma?

3. Control y Libertad para el Usuario:

Pregunta 1:

¿Sintió que tenía el control sobre el proceso de votación y podía realizar cambios antes de confirmar tu voto?

Pregunta 2:

¿Pudo volver atrás o modificar su elección de voto de manera sencilla si así lo deseaba?

4. Consistencia y Estándares:

Pregunta 1:

¿Notó que existía consistencia en el diseño y la forma en que se presentaban las opciones a lo largo de la plataforma?

Pregunta 2:

¿La plataforma seguía un patrón estándar que facilitó su navegación y comprensión del proceso de votación?

5. Prevención de Errores:

Pregunta 1:

¿La plataforma incluyó medidas para evitar que cometa errores durante el proceso de votación?

Pregunta 2:

¿Hubo alguna característica que le impidiera o advirtiera sobre posibles errores en su elección antes de confirmar el voto?

6. Reconocimiento en lugar de Recordar:

Pregunta 1:

¿La plataforma presentó opciones o recordatorios visuales que le ayudaron a reconocer las acciones que debía realizar en lugar de tener que recordarlas?

Pregunta 2:

¿Fue fácil para usted reconocer las opciones disponibles en cada paso del proceso de votación?

7. Flexibilidad y Eficiencia de Uso:

Pregunta 1:

¿Sintió que la plataforma te permitía votar de manera eficiente, adaptándose a sus preferencias y necesidades?

Pregunta 2:

¿La plataforma le ofreció opciones para personalizar su experiencia de votación y hacerla más eficiente?

8. Estética y Diseño Minimalista:

Pregunta 1:

¿Encontró el diseño de la plataforma atractivo y fácil de entender durante el proceso de votación?

Pregunta 2:

¿Considera que el diseño minimalista de la plataforma contribuyó a una experiencia de votación más clara y organizada?

9. Ayudar a los Usuarios a Reconocer, Diagnosticar y Recuperarse de Errores.

Pregunta 1:

¿La plataforma proporcionó mensajes claros y soluciones para ayudarlo a entender y corregir posibles errores durante la votación?

Pregunta 2:

¿Se sintió respaldado/a por la plataforma para corregir cualquier error que pudiera haber cometido durante el proceso de votación?

10. Ayuda y Documentación:

Pregunta 1:

¿Encontró disponible alguna forma de ayuda o documentación que le asistiera en caso de necesitar información adicional durante la votación?

Pregunta 2:

¿Considera que la información de ayuda disponible fue útil y fácil de acceder en caso de requerirla?

Tareas específicas

A continuación, le pediremos que nos ayude a revisar algunos aspectos particulares del sitio, realizando tareas específicas. Le recordamos mostrar en voz alta sus opiniones durante este proceso.

Tareas y Evaluación de Usabilidad:

Tarea 1: Registro e Inicio de Sesión

Regístrate como nuevo usuario en la plataforma.
Inicia sesión con tu cuenta.

Tarea 2: Explorar la Interfaz y Navegación

Explora las diferentes secciones de la plataforma y familiarízate con la navegación.
Encuentra información sobre cómo funciona la votación y las opciones disponibles.

Tarea 3: Emisión de un Voto

Selecciona una opción de voto en una simulación de elección.
Confirma tu elección y completa el proceso de votación.

Tarea 4: Verificación del Estado de Votación

Verifica que tu voto ha sido registrado correctamente y que puedes acceder a información sobre tu participación en la votación.

4.5 Anexo 2

Extractos de la entrevista realizada

NOMBRE DE LA ORGANIZACIÓN	FORMATO DE ENTREVISTA	FECHA DE EMISIÓN:
		14 OCTUBRE 2023
		VERSIÓN: 01
		DOCUMENTO CONTROLADO

FECHA: _____

NOMBRE DEL ENTREVISTADOR:

I. DATOS PERSONALES

NOMBRE DEL ENTREVISTADO:

CARGO DEL ENTREVISTADO:

EDUCACIÓN: _____

III. PREGUNTAS	
¿Qué opinión tiene sobre la implementación de la tecnología en un proceso electoral? ¿Qué ventajas y desventajas cree que puede tener desde una perspectiva política?	La implementación de la tecnología en un proceso electoral es un tema complejo. Si se gestiona adecuadamente, puede ofrecer ventajas en términos de eficiencia y accesibilidad. Sin embargo, es esencial abordar las preocupaciones que se tiene en cuanto con seguridad y privacidad.
En su opinión, ¿cómo cree que la tecnología podría aumentar la confianza en la integridad y seguridad de los procesos electorales?	Se debe garantizar implementando tecnología que ayude a proteger los datos y prevenir cualquier abuso de poder. La confianza en la tecnología electoral también se construye a través de la participación ciudadana, la supervisión independiente y la revisión constante de los sistemas para garantizar su integridad.
¿Qué medidas o regulaciones cree que serían necesarias para garantizar la transparencia y confianza en un sistema de votación electrónica?	Las auditorías independientes y Cifrado en seguridad de red. Estas medidas y regulaciones son esenciales para garantizar que el sistema de votación electrónica sea transparente y confiable. Tecnologías como el Blockchain pueden ayudar en este caso

<p>¿Cuál es su percepción sobre la privacidad y anonimato de los votantes en un sistema de votación electrónica?</p>	<p>Es que la privacidad y el anonimato de los votantes en un sistema de votación son aspectos críticos que deben mantener la integridad y la confianza en el proceso electoral. Los sistemas de votación electrónica deben implementar medidas sólidas de seguridad y cumplir con regulaciones de privacidad adecuadas para garantizar que los votantes puedan ejercer su derecho al voto</p>
<p>¿Qué desafíos cree que podrían surgir al implementar un sistema de votación electrónica y cómo podrían abordarse desde una perspectiva política?</p>	<p>La resistencia al cambio, costos y financiamiento, pero abordar estos aspectos desde una perspectiva política conlleva la colaboración entre partidos políticos, expertos en tecnología y la sociedad civil para garantizar elecciones justas, seguras y confiables.</p>
<p>Desde el punto de vista político, ¿cómo se podrían asegurar que todos los ciudadanos tengan igualdad de acceso y oportunidad para participar en un sistema de votación electrónica?</p>	<p>Se requiere un enfoque integral que involucre a los gobiernos, partidos políticos, organizaciones de la sociedad civil y otros actores relevantes. La participación ciudadana y la colaboración entre estas partes son clave para lograr un proceso electoral inclusivo y equitativo.</p>
<p>En términos de inclusión y participación, ¿cómo podría la tecnología ayudar a involucrar a segmentos de la población que históricamente han tenido bajos niveles de participación electoral?</p>	<p>Facilita el acceso a la información sobre candidatos y propuestas, y ofrece opciones de votación en línea, lo que atrae a votantes jóvenes y con dificultades de movilidad. Sin embargo, es crucial abordar desafíos de seguridad y privacidad para certificar la rectitud del proceso electoral y la igualdad de acceso.</p>
<p>¿Cuál sería su opinión sobre la interoperabilidad y la colaboración entre diferentes entidades políticas con respecto a la implementación de un sistema de votación electrónica?</p>	<p>la interoperabilidad y la colaboración son pilares clave para garantizar elecciones juntos con la cooperación entre diferentes entidades políticas, así promoviendo la confianza del público y fortaleciendo la democracia.</p>
<p>¿Cómo podrían abordarse las posibles críticas y desconfianza de los ciudadanos hacia la tecnología en el contexto de procesos electorales?</p>	<p>En última instancia, la combinación de transparencia, participación ciudadana, seguridad, educación y mejora continua es fundamental para abordar las críticas y la desconfianza de los ciudadanos hacia la tecnología en los procesos electorales y para construir una mayor confianza en la integridad de las elecciones.</p>
<p>¿Qué papel cree que deben desempeñar los partidos políticos en la discusión y toma de decisiones sobre la implementación de un sistema de votación electrónica</p>	<p>Los partidos políticos desempeñan un papel importante en la discusión y toma de decisiones sobre la implementación de un sistema de votación electrónica. Su participación activa y constructiva es esencial para garantizar que el proceso sea equitativo, transparente y aceptado por todas las partes.</p>

4.6 Anexo 3

Figura 19. Prueba de creación de bloque y función hash

The screenshot shows the Ganeche interface with the following components:

- Navigation Bar:** ACCOUNTS, BLOCKS, TRANSACTIONS, CONTRACTS, EVENTS, LOGS. Search bar: SEARCH FOR BLOCK NUMBERS OR TX HASHES.
- System Info:** CURRENT BLOCK: 186, GAS PRICE: 2000000000, GAS LIMIT: 6721975, HARDFORK: MERGE, NETWORK ID: 5777, RPC SERVER: HTTP://127.0.0.1:7545, MINING STATUS: AUTOMINING, WORKSPACE: EVOTINGEC, SWITCH, Settings icon.
- STORAGE:** A JSON object representing storage data:

```
{ 10 items
  adminRole: {...} struct 1 item
  userRole: {...} struct 1 item
  ElectionsMap: {} mapping 0 items
  UsersMap: {} mapping 0 items
  CandidatesMap: {} mapping 0 items
  candidates: [] 0 items
  elections: [] 0 items
  users: [ 1 item
    0: string "0x24dd77c6a5ddcc805ad6cc6e1669a2ad907c4572"
  ]
  adminId: address "0x9851421444c920817f..."
  adminPwd: string "admin"
}
```
- TRANSACTIONS:** TX HASH: 0x04aed58cdc9b2444f66aac5bab7f226e1a9a99a9177d3d271e3030e01017d2ac. FROM ADDRESS: 0x24dd77c6a5ddcc805ad6cc6e1669a2ad907c4572. TO CONTRACT ADDRESS: Voting. GAS USED: 163502. VALUE: 0. CONTRACT CALL button.

Figura 20. Prueba de un bloque de transacción

The screenshot shows the Ganeche interface with the following components:

- Navigation Bar:** ACCOUNTS, BLOCKS, TRANSACTIONS, CONTRACTS, EVENTS, LOGS. Search bar: SEARCH FOR BLOCK NUMBERS OR TX HASHES.
- System Info:** CURRENT BLOCK: 186, GAS PRICE: 2000000000, GAS LIMIT: 6721975, HARDFORK: MERGE, NETWORK ID: 5777, RPC SERVER: HTTP://127.0.0.1:7545, MINING STATUS: AUTOMINING, WORKSPACE: EVOTINGEC, SWITCH, Settings icon.
- Transaction Details:** TX: 0xf4d4b03cb2401e4d7e224ba9271ce78d8248aa6643bd03b52d997e3c69a10be8. SENDER ADDRESS: 0x24dd77c6a5ddcc805ad6cc6e1669a2ad907c4572. TO CONTRACT ADDRESS: 0xf300951B230b32cBcBF8601997F23D3e23B3Cf54. VALUE: 0.00 ETH. GAS USED: 44244. GAS PRICE: 2500000008. GAS LIMIT: 66366. MINED IN BLOCK: 186. TX DATA: 0x4d8131200000000000000000000000000024dd77c6a5ddcc805ad6cc6e1669a2ad907c4572. CONTRACT CALL button.
- CONTRACT:** Contract: Voting, ADDRESS: 0xf300951B230b32cBcBF8601997F23D3e23B3Cf54. FUNCTION: verifyUser(_voter: address). INPUTS: 0x24dd77c6a5ddcc805ad6cc6e1669a2ad907c4572.

Figura 21. Prueba de carga y estrés.

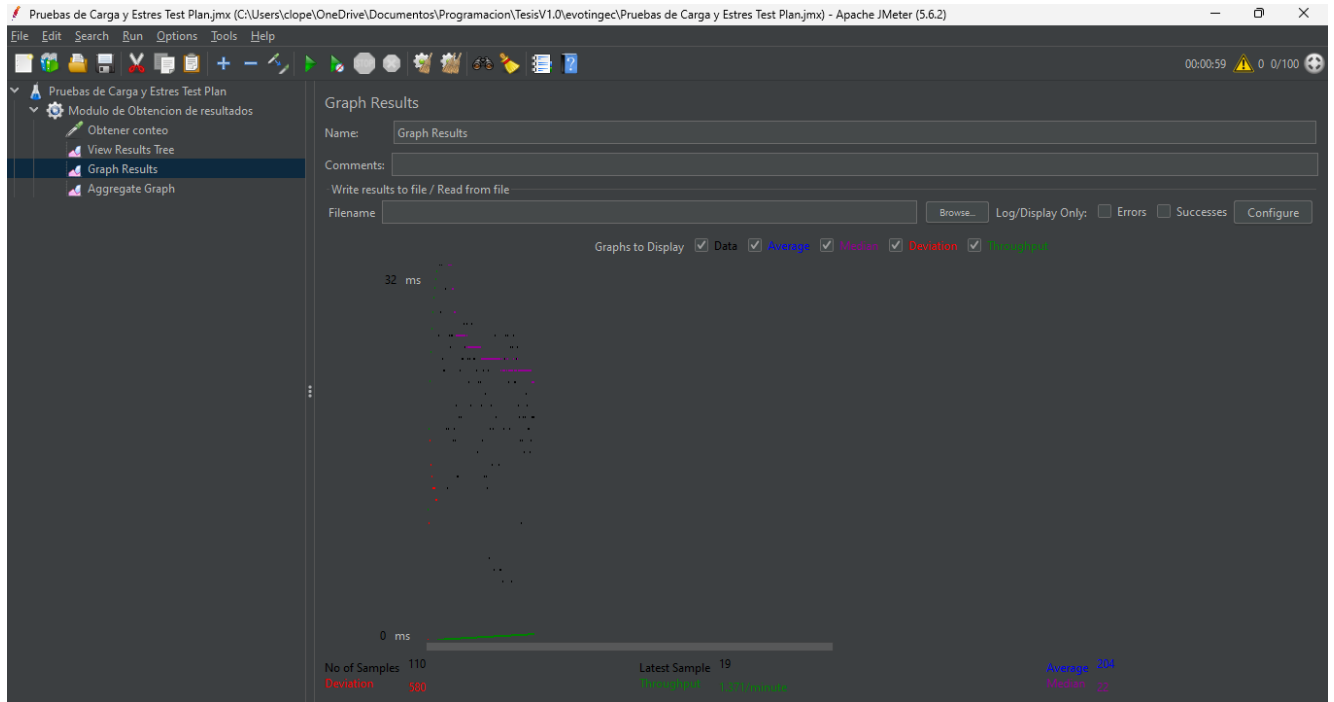
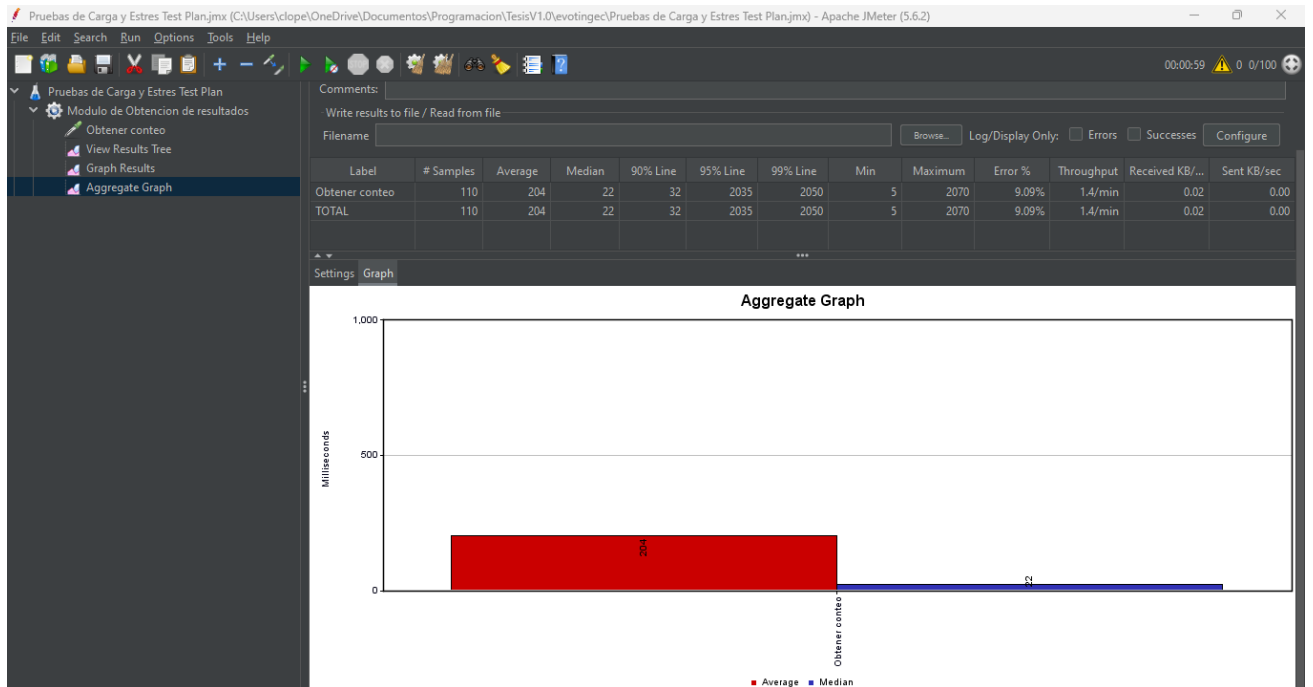


Figura 22. Resultado de promedio y media de peticiones en modo de carga



4.7 Anexo 4

Figura 23. Diccionario de datos.

evoting_relational Data Dictionary

2023-12-09

Alphabetic Index

- [addresses](#)
- [candidates](#)
- [constituencies](#)
- [constituency_councils](#)
- [councils](#)
- [districts](#)
- [elections](#)
- [parishes](#)
- [provinces](#)
- [users](#)

addresses

Column name	Data Type	PK	NN	UQ	BIN	UN	ZF	AI	Default	Comment
addressId	INT	✓	✓					✓		
address	VARCHAR(255)		✓							
provinceId	INT		✓							
districtId	INT		✓							
parishId	INT		✓							
createdAt	DATETIME		✓							
updatedAt	DATETIME		✓							

candidates

Column name	Data Type	PK	NN	UQ	BIN	UN	ZF	AI	Default	Comment
id	INT	✓	✓					✓		
fName	VARCHAR(255)								NULL	
lName	VARCHAR(255)								NULL	
party	VARCHAR(255)								NULL	
candidateImage	VARCHAR(255)								NULL	
candidateSymbol	VARCHAR(255)								NULL	
electionId	VARCHAR(255)								NULL	
createdAt	DATETIME		✓							
updatedAt	DATETIME		✓							

constituencies

Column name	Data Type	PK	NN	UQ	BIN	UN	ZF	AI	Default	Comment
id	INT	✓	✓					✓		
electionId	VARCHAR(255)								NULL	
enclosure	VARCHAR(255)								NULL	
addressId	INT								NULL	
circumscriptionId	INT								NULL	
createdAt	DATETIME		✓							
updatedAt	DATETIME		✓							

constituency councils

Column name	Data Type	PK	NN	UQ	BIN	UN	ZF	AI	Default	Comment
constituencyId	INT	✓	✓							
councilId	INT	✓	✓							
createdAt	DATETIME		✓							
updatedAt	DATETIME		✓							

councils

Column name	Data Type	PK	NN	UQ	BIN	UN	ZF	AI	Default	Comment
id	INT	✓	✓					✓		
number	INT								NULL	
gender	CHAR(255)								NULL	
createdAt	DATETIME		✓							
updatedAt	DATETIME		✓							

districts

Column name	Data Type	PK	NN	UQ	BIN	UN	ZF	AI	Default	Comment
id	INT	✓	✓					✓		
name	VARCHAR(255)								NULL	
createdAt	DATETIME		✓							
updatedAt	DATETIME		✓							

elections

Column name	Data Type	PK	NN	UQ	BIN	UN	ZF	AI	Default	Comment
electionId	VARCHAR(255)	✓	✓							
description	VARCHAR(255)								NULL	
startDate	DATETIME								NULL	
endDate	DATETIME								NULL	
status	TINYINT(1)								NULL	
result	TINYINT(1)								NULL	
deleteStatus	TINYINT(1)								NULL	
createdAt	DATETIME		✓							
updatedAt	DATETIME		✓							

parishes

Column name	Data Type	PK	NN	UQ	BIN	UN	ZF	AI	Default	Comment
id	INT	✓	✓					✓		
name	VARCHAR(255)								NULL	
createdAt	DATETIME		✓							
updatedAt	DATETIME		✓							

provinces

Column name	Data Type	PK	NN	UQ	BIN	UN	ZF	AI	Default	Comment
id	INT	✓	✓					✓		
name	VARCHAR(255)								NULL	
createdAt	DATETIME		✓							
updatedAt	DATETIME		✓							

users

Column name	Data Type	PK	NN	UQ	BIN	UN	ZF	AI	Default	Comment
id	INT	✓	✓					✓		
userId	VARCHAR(255)								NULL	
fName	VARCHAR(255)								NULL	
nationalId	VARCHAR(255)								NULL	
email	VARCHAR(255)								NULL	
birthDate	DATETIME								NULL	
constituencyId	INT								NULL	
createdAt	DATETIME		✓							
updatedAt	DATETIME		✓							