UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

DESARROLLO DE UN SISTEMA DE VOTACIÓN ELECTRÓNICA UTILIZANDO UNA TECNOLOGÍA DE CONTABILIDAD DISTRIBUIDA PARA EL ALMACENAMIENTO SEGURO DE LA INFORMACIÓN

ASTUDILLO CRUZ GABRIELA LISSETH
INGENIERA DE SISTEMAS

MACHALA
2021

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

DESARROLLO DE UN SISTEMA DE VOTACIÓN ELECTRÓNICA UTILIZANDO UNA TECNOLOGÍA DE CONTABILIDAD DISTRIBUIDA PARA EL ALMACENAMIENTO SEGURO DE LA INFORMACIÓN

ASTUDILLO CRUZ GABRIELA LISSETH
INGENIERA DE SISTEMAS

MACHALA
2021

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

TRABAJO TITULACIÓN
PROPUESTAS TECNOLÓGICAS

DESARROLLO DE UN SISTEMA DE VOTACIÓN ELECTRÓNICA UTILIZANDO UNA TECNOLOGÍA DE CONTABILIDAD DISTRIBUIDA PARA EL ALMACENAMIENTO SEGURO DE LA INFORMACIÓN

ASTUDILLO CRUZ GABRIELA LISSETH
INGENIERA DE SISTEMAS

HERNANDEZ ROJAS DIXYS LEONARDO

MACHALA, 26 DE ABRIL DE 2021

MACHALA
2021

tesis G

INFORME DE ORIGINALIDAD

2%	2%	1%	0%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

ENCONTRAR COINCIDENCIAS CON TODAS LAS FUENTES (SOLO SE IMPRIMIRÁ LA FUENTE SELECCIONADA)

< 1%

★ uchlsistemas.net

Fuente de Internet

Excluir citas	Activo	Excluir coincidencias	< 30 words
Excluir bibliografía	Activo		

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

La que suscribe, ASTUDILLO CRUZ GABRIELA LISSETH, en calidad de autora del siguiente trabajo escrito titulado DESARROLLO DE UN SISTEMA DE VOTACIÓN ELECTRÓNICA UTILIZANDO UNA TECNOLOGÍA DE CONTABILIDAD DISTRIBUIDA PARA EL ALMACENAMIENTO SEGURO DE LA INFORMACIÓN, otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

La autora declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

La autora como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 26 de abril de 2021

ASTUDILLO CRUZ GABRIELA LISSETH
0706618386

DEDICATORIA

A mi familia, por ser el principal soporte e inspiración que tengo para alcanzar cada una de las metas que me he propuesto. De manera especial a mi madre y hermana que siempre confiaron en mí.

A todos los docentes que he tenido desde que inicié mi formación escolar, quienes han sabido guiarme, aconsejarme y han aportado sus conocimientos para fortalecer mis capacidades.

A mis amigos y compañeros de la carrera de Ingeniería de Sistemas, con quienes he compartido muchos momentos de aprendizaje mediante el desarrollo de diferentes proyectos de asignaturas y tareas colaborativas.

A mis vecinos y conocidos, que están pendientes de mi preparación académica y siempre me saludan amablemente deseándome un futuro exitoso.

AGRADECIMIENTO

A Dios, por brindarme la vida y la salud, así como también la inteligencia y la fortaleza para culminar con mi carrera universitaria superando las dificultades.

A mi madre, por el apoyo constante e incondicional, por el cariño recibido a diario y por ser mi motivación para realizar mi mejor esfuerzo en cada actividad de mi vida.

A las autoridades de la Universidad Técnica de Machala, por gestionar adecuadamente los recursos que han hecho posible contar con excelentes instalaciones y equipos tecnológicos utilizados a lo largo de los años de estudio.

A los docentes de la carrera de Ingeniería de Sistemas, por compartir los conocimientos y experiencias profesionales que han aportado considerablemente en mi formación académica.

Al ingeniero Dixys Hernández, por haberme guiado en el desarrollo de la propuesta tecnológica con sus ideas y conocimientos, además por el tiempo dedicado a la revisión del presente informe para su correcta presentación.

RESUMEN

Las votaciones son importantes para la democracia de cualquier país, empresa o institución educativa. En la Universidad Técnica de Machala, la Escuela de Informática, conformada por las carreras de Ingeniería de Sistemas y Tecnologías de la Información, anualmente realiza la elección de sus representantes estudiantiles de forma presencial mediante votación en papel, pero actualmente debido al inconveniente que generan las aglomeraciones de personas, requiere de una alternativa segura y confiable de votación electrónica que permita ejercer el derecho al voto de manera online. El principal problema con los sistemas de votación electrónica que guardan la información en bases de datos centralizadas, es que son mucho más vulnerables al fraude que la votación en papel, puesto que, si el ente administrador o un atacante informático manipulara indebidamente los datos, difícilmente sería detectado. Por tal motivo, el objetivo de la presente propuesta es desarrollar un sistema de votación electrónica utilizando una tecnología de contabilidad distribuida (DLT) para el almacenamiento seguro de la información. La ventaja que ofrece este tipo de tecnología es la descentralización, ya que una DLT consta de una red de nodos distribuidos que según su configuración de acceso puede ser pública, privada o federada. Los puntos de la red verifican mediante mecanismos de consenso cada transacción realizada y almacenan la información estructurando los datos en una cadena de bloques o un grafo acíclico dirigido (DAG), haciendo uso de métodos criptográficos que garantizan su seguridad e inmutabilidad. Tomando en consideración los requerimientos del sistema y los recursos necesarios para la implementación de los diferentes tipos de tecnologías de contabilidad distribuida, se eligió IOTA porque es una solución robusta de código abierto que permite registrar transacciones sin costo y tiene un gran potencial de escalabilidad. Para el desarrollo del sistema de votación propuesto se siguió la metodología Agile Block Chain Dapp Engineering, también conocida como ABCDE; se utilizó el lenguaje de programación JavaScript con sus Frameworks Express y Vue; de una base de datos Postgres se obtuvieron las identificaciones necesarias para establecer el padrón electoral con estudiantes acreditados. Estas herramientas permitieron desarrollar un frontend adaptable a diversos dispositivos electrónicos y un backend funcional que utiliza una API con bibliotecas de IOTA para guardar los votos de forma segura en una especie de urna digital. En la ejecución del prototipo, se configuró una convocatoria, se registraron listas y candidaturas que se pudieron visualizar en el sitio web informativo; se probó el funcionamiento de la aplicación web de votación, la cual

proporciona un hash para que el estudiante pueda verificar su voto registrado correctamente en IOTA; finalmente, se presentó en un dashboard los resultados obtenidos. La evaluación de calidad en uso de acuerdo con la norma ISO/IEC 25022:2016, demuestra la viabilidad para la implementación de la propuesta tecnológica en elecciones reales de representantes estudiantiles de la Escuela de Informática de la UTMACH, dado que los usuarios perciben un nivel de eficacia, eficiencia y satisfacción considerablemente mayor con esta nueva solución informática que con la antigua forma de votación presencial y otras formas de votación electrónica.

Palabras clave: Votación electrónica, aplicación web, IOTA, Blockchain, DLT, DAG.

ABSTRACT

Voting is important for the democracy of any country, company or educational institution. At the Universidad Técnica de Machala, the School of Computer Science, made up of the careers of Systems Engineering and Information Technology, annually elects its student representatives in person by voting on paper, but currently due to the inconvenience generated by the agglomerations of people, requires a safe and reliable alternative to electronic voting that allows them to exercise the right to vote online. The main problem with electronic voting systems that store information in centralized databases is that they are much more vulnerable to fraud than voting on paper, since, if the administering entity or a computer attacker were to tamper with the data, it would hardly be detected. For this reason, the objective of this proposal is to develop an electronic voting system using distributed ledger technology (DLT) for the secure storage of information. The advantage offered by this type of technology is decentralization, since a DLT consists of a network of distributed nodes that, depending on their access configuration, can be public, private or federated. The points of the network verify through consensus mechanisms each transaction carried out and store the information by structuring the data in a chain of blocks or a directed acyclic graph (DAG), making use of cryptographic methods that guarantee its security and immutability. Taking into consideration the system requirements and resources necessary for the implementation of the different types of distributed ledger technologies, IOTA was chosen because it is a robust open-source solution that allows to record transactions at no cost and has great potential for scalability. For the development of the proposed voting system, the Agile Block Chain Dapp Engineering methodology, also known as ABCDE, was followed; the JavaScript programming language was used with its Frameworks Express and Vue; From a Postgres database, the necessary identifications were obtained to establish the electoral roll with accredited students. These tools made it possible to develop a frontend adaptable to various electronic devices and a functional backend that uses an API with IOTA libraries to save votes safely in a kind of digital ballot box. In the execution of the prototype, a call was set up, lists and candidatures were registered that could be viewed on the informative website; the operation of the voting web application was tested, which provides a hash so that the student can verify their vote correctly registered in IOTA; finally, the results obtained were presented on a dashboard. The evaluation of quality in use in accordance with the ISO/IEC 25022:2016 standard, demonstrates the viability for the implementation of the technological proposal in real elections of student representatives of the School of

Computer Science of the UTMACH, given that users they perceive a level of effectiveness, efficiency and satisfaction considerably higher with this new IT solution than with the old form of presential voting and other forms of electronic voting.

Keywords: Electronic voting, web application, IOTA, Blockchain, DLT, DAG.

ÍNDICE DE CONTENIDO

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

GLOSARIO

ABCDE: Agile Block Chain Dapp Engineering. Es una metodología ágil para el desarrollo de aplicaciones basadas en blockchain [1].

API: Application Programming Interfaces**.** Se traduce como "Interfaz de Programación de Aplicaciones". Las API permiten mantener la seguridad y control en la comunicación entre productos de software, habilitando el acceso a sus recursos [2].

Árbol de Merkle: Árbol binario donde cada valor de nodo interior es una función hash de los valores de nodo de sus hijos. Los árboles Merkle han sido diseñados concretamente para que se pueda verificar un valor de hoja con respecto a un valor raíz [3].

BTC: Criptomoneda Bitcoin. El bitcoin se utiliza como moneda en el mundo de Internet. La forma de generar nuevos bitcoins es a través de la minería que consiste en contribuir con poder computacional en la validación de la cadena de bloques de Bitcoin [4].

Criptografía: Es una disciplina/tecnología enfocada en solucionar problemas de autenticidad y confidencialidad, haciendo posible la transmisión segura de información por un medio no necesariamente seguro; de tal forma que no pueda ser comprendida sin que alguien autorizado la descifre [5].

DLT: Distributed Ledger Technology. En el presente informe se hace referencia como Tecnología de Contabilidad Distribuida, pero también se traduce como Tecnología de Libro Mayor Distribuido.

DAPPS: Decentralized applications. Se traduce como aplicaciones descentralizadas. Una DApp utiliza en el frontend las mismas tecnologías que las aplicaciones tradicionales, pero usa contratos inteligentes para acceder a la blockchain como backend [6].

DAG: Directed Acyclic Graph**.** Se traduce como Grafo Acíclico Dirigido. El Gráfo Acíclico Dirigido (DAG) como árbol es la arquitectura DLT más joven: se utiliza como base para un gráfico hash, es decir, una estructura de datos que documenta, quién y en qué orden se conecta con quién [7].

ECDSA: Algoritmo de firma digital de curva elíptica (ECDSA) es un derivado estandarizado del anterior Algoritmo de firma digital (DSA), pero tiene la ventaja de ser más eficiente y requerir longitudes de clave mucho más cortas para el mismo nivel de seguridad. Además de los casos de uso como mensajería autenticada e

inicio de sesión remoto, ECDSA se ha adoptado con entusiasmo donde la alta eficiencia es importante. Por ejemplo, lo utilizan TLS, DNSSec y muchas criptomonedas [8].

Hash: Hash es una función criptográfica (algoritmo matemático) que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija, independientemente de la longitud de los datos de entrada [9].

HTTP: Hypertext Transfer Protocol o Protocolo de Transferencia de Hipertexto en español, se utiliza para la comunicación entre los navegadores y servidores web siguiendo el clásico modelo cliente-servidor, en el que un cliente realiza una petición a un servidor y espera una respuesta [10].

IOTA: Internet of Things Automatization. IOTA es el primer libro mayor distribuido creado para el "Internet de todo", una red para intercambiar valor y datos entre humanos y máquinas. La red IOTA está diseñada para Internet de las cosas, con datos a prueba de manipulaciones, micro transacciones gratuitas y bajos requisitos de recursos [11].

JWT: J**S**ON Web Token (JWT) es un estándar abierto que define una forma compacta y autónoma de transmitir información de forma segura mediante un objeto JSON. Esta información es confiable y puede ser verificada porque está firmada digitalmente ya sea con un secreto o un par de claves pública / privada usando RSA o ECDSA [12].

SMS: Short Message Service. Se traduce como servicio de mensajes cortos o servicio de mensajes simples. Es un servicio de mensajería en el entorno de las comunicaciones de telefonía móvil [13].

Tangle: Es el nombre que le da la Fundación IOTA al grafo acíclico dirigido que utiliza como estructura de datos; el cual registra de manera inmutable el intercambio de datos y valores, garantizando que la información sea confiable y no pueda ser manipulada ni destruida [11].

Trytes: Son caracteres del sistema de numeración ternario que representan uno de los 27 (3^3) posibles estados mediante las letras mayúsculas A-Z y el número 9. En IOTA, los datos se representan en ternario equilibrado, que consta de 1, 0 o -1. Estos valores se llaman trits, y tres de ellos son iguales a un tryte [14].

UML: Unified Modeling Language o Lenguaje unificado de modelado. Es un estándar que se utiliza como un medio para comunicar los requisitos y la intención del diseño en el proceso de desarrollo de software [15].

INTRODUCCIÓN

A nivel global las votaciones desempeñan un rol fundamental para la democracia de los países, de igual forma en las universidades éste es un proceso esencial con el que la comunidad universitaria elige a sus representantes. Lamentablemente, el voto que se emite de manera tradicional mediante papel presenta inconvenientes como la demora en la obtención de resultados y problemas de credibilidad. Además, la logística del sufragio ocasiona aglomeraciones, dado que los votantes comúnmente deben esperar su turno haciendo largas filas, lo cual no es recomendable en el contexto de la actual crisis sanitaria de COVID-19 [16].

Ante los problemas que posee la votación en papel, la implementación de tecnología permite hacer más eficiente el proceso electoral, por lo que algunos países y organizaciones han incursionado en el voto electrónico [17]. Naturalmente también existen diversos trabajos académicos que proponen soluciones informáticas de votación electrónica [18], en los cuales se identifican dos enfoques principales. El primero consiste en utilizar una máquina o dispositivo diseñado específicamente para la recepción del voto, por tanto, los electores deben presentarse a votar en un lugar específico [19]. El segundo enfoque de estos sistemas es posibilitar el sufragio a distancia, de forma online utilizando una aplicación web [20]; ésta es la orientación de la presente propuesta tecnológica.

Los sistemas de votación electrónica que permiten el voto online resultan convenientes en varios escenarios de aplicación, porque eliminan la problemática de la aglomeración de personas y favorecen la participación [21]. No obstante, al residir la información en una base de datos centralizada, la entidad o individuo que tiene el control sobre ésta pudiera alterar los resultados, lo que ocasiona desconfianza en la transparencia del proceso [22]. En este sentido, es necesaria la implementación de una de tecnología de contabilidad distribuida (DLT). Éste es un concepto que incluye a la blockchain, considerada como una tecnología disruptiva capaz de afectar una amplia variedad de dominios, que van desde las finanzas hasta la gobernanza, al ofrecer seguridad, confiabilidad y transparencia de manera descentralizada [23].

Diseñar un sistema de voto electrónico más seguro y práctico se ha convertido en un tema popular en el área de la industria y la seguridad de la información [24], por lo que se está experimentando ampliamente la implementación de la tecnología Blockchain en los sistemas de votación [25], [26], [27]. Sin embargo, estas soluciones tienen como

desventajas, el tiempo que demoran las transacciones en ser aprobadas, el alto consumo de energía empleada en establecer el consenso y el cobro de comisiones.

En la presente propuesta tecnológica se utiliza IOTA para almacenar la información de las votaciones de forma encriptada y distribuida. Esta DLT supera las limitaciones de una blockchain clásica [28], debido a que surgió como un protocolo liviano para la automatización de la comunicación entre aplicaciones de Internet de las cosas (IoT); en donde se requiere optimización en el uso de recursos y un bajo consumo de energía para la gestión de grandes flujos de datos y eventos en tiempo real [29], [30], [31]. Por estas características se la considera idónea para el almacenamiento seguro en un sistema de votación electrónica que presenta alta transaccionalidad.

Se realizó una investigación previa con 100 estudiantes de la carrera Tecnologías de la Información, para determinar el nivel de aceptación que tendría un sistema de votación electrónica con almacenamiento seguro mediante una tecnología de contabilidad distribuida. Los resultados indican que un 95% de los encuestados participaría en las votaciones utilizando una Laptop, Smartphone, computadora de escritorio o una Tablet. Un 74% está de acuerdo con la implementación de una tecnología como blockchain, y un 58% considera que ésta brindaría mayor seguridad y confianza a los procesos electorales (Ver Anexo 2). Consecuentemente, se plantea el objetivo de automatizar el proceso de elecciones estudiantiles de la Escuela de Informática de la UTMACH.

En el desarrollo del prototipo se utiliza la metodología ágil ABCDE, la API de IOTA, el lenguaje de programación JavaScript, el framework backend Express y el framework frontend Vue. Este documento constituye el informe del trabajo de titulación para una propuesta tecnológica y se encuentra estructurado en tres capítulos que se detallan a continuación:

Capítulo 1. Titulado como Diagnóstico de necesidades y requerimientos; incluye el ámbito de aplicación, el establecimiento de requerimientos y su justificación.

Capítulo 2. Es el apartado más extenso del informe, en este se presenta el desarrollo del prototipo tecnológico; además de la definición, también contiene la fundamentación teórica, los objetivos, el diseño y la ejecución o ensamblaje.

Capítulo 3. En esta sección se evalúa el prototipo; contiene tanto el plan de evaluación como sus resultados. Finalmente se declaran las conclusiones y recomendaciones.

1. CAPÍTULO I: DIAGNÓSTICO DE NECESIDADES Y REQUERIMIENTOS

1.1. Ámbito de Aplicación: descripción del contexto y hechos de interés

En la UTMACH, las carreras de Ingeniería de Sistemas y Tecnologías de la Información conforman la Escuela de Informática, en donde se eligen dirigentes estudiantiles para gestionar actividades académicas internas que promueven la unidad y compañerismo. Las votaciones normalmente se realizan cada año de manera presencial, siguiendo las directrices establecidas en el Reglamento de Elecciones y Referendo de la Universidad Técnica de Machala, en el que se pueden identificar las siguientes etapas [32]:

- Convocatoria
- Inscripción de candidaturas
- Aprobación de candidaturas
- Campaña electoral
- Elecciones
- Escrutinio
- Publicación de resultados

La primera etapa es la convocatoria, realizada por el Tribunal Electoral, en la cual se presentan las fechas de inicio y fin de campaña, los plazos y términos, así como también los requisitos que deben cumplir los candidatos. Las listas postulantes deben estar conformadas por estudiantes que cumplan con los requisitos para poder ser candidatos, de acuerdo con lo establecido en el Estatuto de la UTMACH; además deberán presentar la documentación pertinente descrita en el Art. 38 del Reglamento de Elecciones y Referendo de la Universidad Técnica de Machala [32].

La campaña debe desarrollarse en el marco del respeto, honestidad, verdad y convivencia universitaria. El día de las elecciones, cada junta receptora del voto levanta un Acta de Instalación, que sirve para registrar el cumplimiento del padrón, papeletas electorales y urna. Luego de finalizado el plazo de votación, se realiza el escrutinio, donde pueden participar los delegados políticos en calidad de veedores. Terminando este proceso, se deja la constancia en el Acta de Finalización que será suscrita por todos los presentes, anexando la documentación recibida al inicio de la jornada y los votos escrutados entregados de manera inmediata al Tribunal Electoral para la correspondiente publicación de los resultados [32].

La Figura 1 presenta el flujo de cómo se realiza el proceso electoral, en donde constan las diferentes actividades que cumplen cada uno de los actores. Este es el proceso que normalmente se sigue en las elecciones de representantes estudiantiles de la Escuela de Informática de la UTMACH, cuando las votaciones son presenciales. Pero actualmente las clases universitarias se dictan de forma online, debido a la crisis sanitaria provocada por la pandemia de COVID-19, mientras que el proceso de elección de representantes estudiantiles que tradicionalmente se celebraba por las carreras de Ingeniería de Sistemas y Tecnologías de la Información como un acto democrático para elegir a sus líderes políticos, ha quedado relegado; ya que es preferible no crear eventos en los que pueden existir aglomeración de personas en un espacio cerrado o reducido.

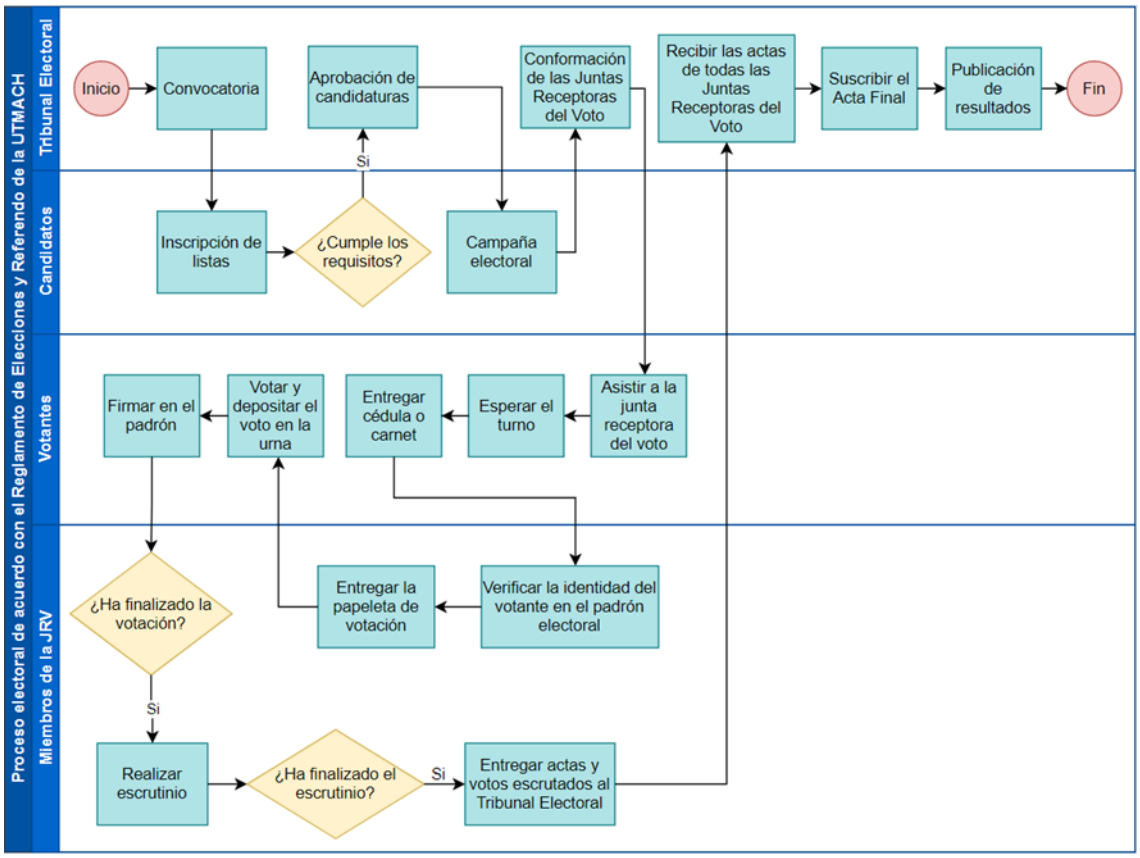


Figura 1. Diagrama de flujo del proceso electoral de acuerdo con el Reglamento de Elecciones y Referendo de la UTMACH

1.2. Establecimiento de Requerimientos

El sistema de votación electrónica propuesto tiene como requerimientos principales la descentralización, autenticación, confidencialidad, integridad, verificabilidad y adaptabilidad. A continuación, se detallan cada uno de estos.

Descentralización: La descentralización de la información permite que la confianza en la veracidad de los resultados no dependa exclusivamente de una entidad reguladora, por lo cual el sistema a desarrollar se conectará a la red de nodos distribuidos de IOTA para el almacenamiento seguro de los votos emitidos por estudiantes empadronados.

Autenticación: Los usuarios requieren autenticarse para ejercer su derecho al voto, por lo cual el sistema asignará un código de acceso a cada estudiante para garantizar la autenticidad del votante.

Confidencialidad: La confidencialidad total de los votantes se garantizará haciendo uso criptografía. El sistema respetará el secreto electoral almacenando el voto de forma encriptada y sin vincularlo a la identidad del votante.

Integridad: Cada votante puede emitir solo un voto, que será un registro inmutable, es decir que no podrá ser alterado ni eliminado, por lo que se requiere su almacenamiento en una base de datos segura para protegerlo contra ataques informáticos. Cuando un usuario ha registrado correctamente su voto ya no se le permitirá volver a ingresar al módulo de votación.

Verificabilidad: Una vez registrada la votación del estudiante, el sistema le presentará un código hash al votante con el que podrá verificar en cualquier momento que su voto se encuentra correctamente almacenado. El escrutinio se realizará automáticamente y los resultados se publicarán en el sitio web.

Adaptabilidad: El sistema podrá ser usado desde diferentes tipos de dispositivos, tales como tablets, smartphones, computadores de escritorio y laptops; por lo tanto, las interfaces gráficas de usuario tendrán un diseño responsivo.

La recopilación de los requerimientos funcionales del sistema se realizó utilizando como herramienta las historias de usuario presentadas en el Anexo 3.

1.3. Justificación del requerimiento a satisfacer

La pandemia global de COVID-19 ha creado desafíos políticos y económicos únicos, la democracia se ha visto afectada y se ha tenido que decidir entre celebrar elecciones en circunstancias inciertas o posponerlas [16]. En el caso de la Asociación de Estudiantes de la Escuela de Informática en la UTMACH, sus dirigentes optaron por posponer las votaciones que se realizan internamente y de esa forma evitar exponer a contagios a su comunidad estudiantil, ya que no se disponía de un sistema confiable y seguro que permita la votación online.

Un sistema de votación electrónica presenta muchas ventajas al facilitar ejercer el derecho al voto desde cualquier lugar utilizando un dispositivo conectado a internet, como por ejemplo un smartphone, Tablet o laptop. Actualmente, esto representa una solución para evitar las aglomeraciones de personas, quienes normalmente tienen que hacer largas filas en los recintos electorales.

La implementación de un sistema de votación electrónica para la elección de representantes estudiantiles en la Escuela de Informática de la UTMACH se considera pertinente debido a que los electores se encuentran familiarizados con el manejo de sistemas de información y utilizan frecuentemente dispositivos electrónicos para el desarrollo de sus actividades académicas; además la Unidad de Bienestar Estudiantil ha implementado ayudas tecnológicas que consisten en la entrega de Tablets y paquetes de datos a estudiantes de bajos recursos para que puedan conectarse a las clases online; esto ha hecho posible que prácticamente todos tengan un dispositivo con el cual ejercer su derecho al voto de manera remota, por lo que la participación electoral sería del 95%, según la encuesta aplicada (Ver Anexo 2).

Los sistemas convencionales centralizan el control de la información a través de su almacenamiento en bases de datos administradas por una entidad reguladora. En el caso específico de la votación electrónica, esta centralización provoca desconfianza en la veracidad de los resultados del proceso electoral [33]. Por tanto, es necesario el desarrollo de soluciones descentralizadas orientadas a brindar resultados confiables que garanticen la seguridad de la información y que no dependan estrictamente de una sola fuente de verdad o punto de falla [34].

2. CAPÍTULO II: DESARROLLO DEL PROTOTIPO

2.1. Definición del Prototipo Tecnológico

El sistema de votación electrónica propuesto utiliza una tecnología de contabilidad distribuida para el almacenamiento seguro de la información. Los votos serán almacenados en una base de datos descentralizada que ofrece un registro inmutable. El prototipo tecnológico incluye un panel de configuraciones, un módulo para el sufragio y un sitio web informativo, ha sido diseñado para la elección de representantes estudiantiles en la Escuela de Informática de la Universidad Técnica de Machala, con la finalidad de lograr automatización de procesos y confiabilidad en los resultados.

Los usuarios accederán al sistema mediante autenticación previa. El rol de administrador será para un delegado del Tribunal Electoral, quien realizará las configuraciones respectivas para registrar el plazo de inscripciones, periodo de campaña, y la fecha de sufragio; también podrá inscribir las candidaturas que se hayan aprobado de acuerdo al cumplimiento con los requisitos establecidos en el Reglamento de Elecciones y Referendo de la Universidad Técnica de Machala [32]. Los votantes tendrán acceso al módulo de votación el día y horario establecido, pudiendo votar solo una vez en una determinada convocatoria.

El sitio web público informará sobre el plazo de inscripción, periodo de campaña y la fecha de las votaciones; además permitirá visualizar las candidaturas registradas, se mostrará la propuesta de cada lista participante, la foto, nombres y apellidos de los candidatos. El padrón electoral se publicará junto a la convocatoria y será conformado automáticamente por los estudiantes que están matriculados en las carreras de Ingeniería de Sistemas y Tecnologías de la Información, las cuales pertenecen a la Escuela de Informática, por lo que se utilizará postgres para representar la base de datos institucional. Finalmente, el sistema hará el recuento de los votos registrados en la red DLT y presentará los resultados electorales mediante un dashboard.

En la Figura 2 se muestra el diagrama de casos de uso del sistema, en donde se identifican los roles que tienen los usuarios y sus funciones dentro de los módulos que componen la presente propuesta tecnológica.

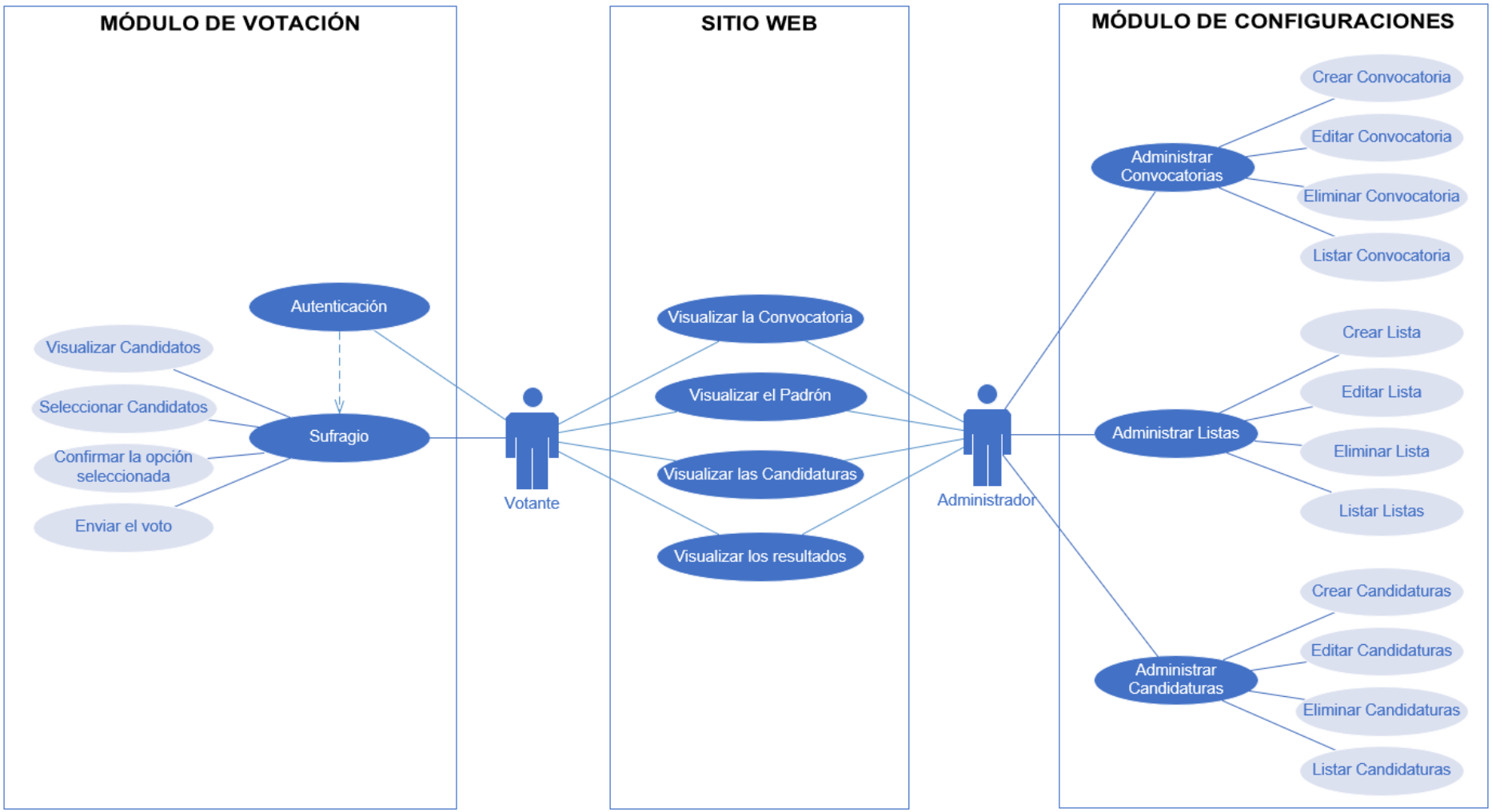


Figura 2. Diagrama de casos de uso del Sistema de Votación Electrónica

2.2. Fundamentación Teórica del Prototipo

En este apartado se presentan los conceptos analizados en la propuesta tecnológica, fundamentándose en artículos de revistas indexadas en bases de datos científicas.

2.2.1. Votación Electrónica

La votación electrónica es la forma en que un elector puede ejercer su derecho al voto utilizando medios de automatización para procesos electorales que un estado o institución posean, e incorporando básicamente tecnología para las diferentes etapas que contiene una jornada electoral; configurar, administrar, emitir, procesar y presentar resultados oficiales [35]. Concisamente, esta forma de sufragio es la versión electrónica de la votación en papel, mediante la aplicación de tecnología para automatizar los diferentes procesos electorales.

Voto electrónico, voto por internet, voto telemático, voto informático, tele democracia, tecno democracia, ciber democracia, democracia tecnológica, democracia electrónica, democracia digital, democracia online, política virtual, tecno política, son expresiones que describen de cierto modo la nueva correlación entre la informática y el derecho político del voto [35].

2.2.1.1. Beneficios

- Las soluciones de voto electrónico tienden a aumentar el número de votantes, simplificar el proceso de votación y reducir costos al eliminar el papel y requerir menos recursos humanos [25].
- El voto electrónico puede ahorrar tiempo y esfuerzo con una alta eficiencia y flexibilidad, por lo cual está recibiendo cada vez más atención en lugar del voto tradicional [36].

2.2.1.2. Adopción

Estonia, Brasil, Holanda y Noruega son algunos de los países que han adoptado el voto electrónico para las elecciones nacionales [17], por lo cual este tipo de soluciones informáticas están adquiriendo cada vez mayor legitimidad. Sin embargo, la votación electrónica se enfrenta a desafíos, como seguridad, transparencia y privacidad [25].

2.2.1.3. Clasificación

La votación electrónica se puede clasificar en las siguientes categorías [26], [37]:

- La primera es la votación presencial o fuera de línea, supervisada físicamente por autoridades electorales; utiliza máquinas de votación ubicadas en colegios electorales para facilitar el conteo de los votos.
- La segunda es la votación híbrida en la que los votantes son supervisados físicamente por los funcionarios electorales, pero las máquinas de votación están conectadas a Internet.
- La última es la votación *online*, donde los votantes están sin la supervisión de funcionarios electorales. Por lo general, los votantes emiten sus votos a través de Internet utilizando una computadora personal o un teléfono móvil.

2.2.1.4. Requisitos

Un sistema de elección electrónica confiable requiere que toda la información involucrada se haga pública, es decir, se enfoca no solo en la transparencia sino también en cuestiones de privacidad. En otras palabras, cada boleta debe contarse de manera anónima, correcta y eficiente [38]. Los requisitos generales de seguridad de los sistemas de votación electrónica se describen en la Figura 3 [18]:

- **Elegibilidad:** Solo pueden votar quienes cumplan con ciertos criterios.
- **Democracia:** Cada votante puede votar una sola vez.
- **Privacidad:** Nadie debería poder relacionar un voto con su elector.
- **Verificabilidad:** Cualquier votante puede verificar que su voto se registró correctamente y que el recuento final contiene su voto.
- **Precisión:** El resultado final de la elección debe contener todos los votos válidos, que deben estar correctamente registrados y contados.
- **Equidad:** Para evitar cualquier interferencia en el comportamiento de los votantes, el conteo no puede comenzar hasta que finalice la elección.
- **Robustez:** Debe ser robusto contra ataques pasivos y activos de autoridades o votantes corruptos, así como contra fallas.
- **Libre de recibo:** El recibo no debe demostrar la intención del voto.
- **Resistente a la coacción:** El sistema no debe permitir posibles coacciones.

2.2.2. Tecnología de Contabilidad Distribuida (DLT)

La Tecnología de Contabilidad Distribuida o Tecnología de Libro Mayor Distribuido proviene del término inglés DLT (*Distributed Ledger Technology*), frecuentemente mencionada como "blockchain" [39], ofrece un enfoque innovador para almacenar información, ejecutar transacciones, realizar funciones y establecer confianza en un entorno abierto, por lo que ha disfrutado de un espectacular ascenso a la prominencia en los últimos años [40].

La distribución de transacciones hace que sea más transparente verificar todos los registros almacenados. DLT posee mayor eficiencia que la arquitectura centralizada clásica de los sistemas informáticos [34]. Por tanto, las futuras interacciones entre pares y la automatización de procesos pueden ser más confiables y transparentes en comparación con las aplicaciones tradicionales [41].

El tipo más destacado de DLT es blockchain, que tiene su origen en la criptomoneda Bitcoin, propuesta en 2008 por Satoshi Nakamoto [42], la cual resolvió por primera vez el problema del doble gasto a través de su algoritmo de consenso conocido como prueba de trabajo [43], desde entonces, han surgido muchas otras tecnologías y aplicaciones de contabilidad distribuida [39].

Las DLT se utilizan en diversas industrias, como la banca, el gobierno y el derecho, la atención médica, los seguros y el transporte [44]; muchos las consideran un avance tecnológico de la criptografía y la ciberseguridad, con casos de uso que van desde sistemas de criptomonedas implementados a nivel mundial como Bitcoin, hasta contratos inteligentes, redes inteligentes a través del Internet de las cosas, etc [45].

En síntesis, DLT mejora la arquitectura centralizada clásica al distribuir registros de bases de datos entre varios usuarios involucrados en una red descentralizada; y brinda confianza gracias a las características de integridad y seguridad del mecanismo de consenso, con el cual se validan las transacciones.

2.2.2.1. Características de las DLT

Las DLT ofrecen numerosas características de seguridad [34], [46], [47], entre las que se pueden mencionar las siguientes:

- Descentralización
- Inmutabilidad
- Auditabilidad
- Integridad
- Tolerancia a fallas
- Confiabilidad
- Transparencia
- Disponibilidad
- Coherencia
- Privacidad

2.2.2.2. Elementos de las DLT

Una DLT está compuesta principalmente por tres elementos que son el *ledger* o libro mayor; la red P2P que puede ser pública, privada o federada de acuerdo a la facilidad de participación de nuevos integrantes; y la Gobernanza que consiste principalmente en el mecanismo de consenso con el cual los nodos de la red validan las transacciones para ser anexadas al *ledger* (Fig. 3).

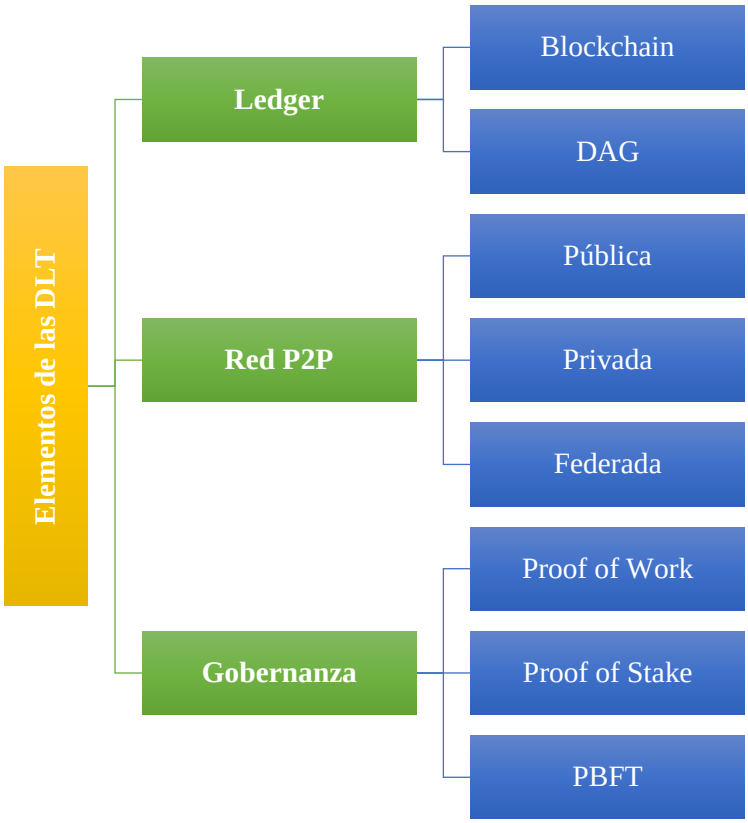


Figura 3. Elementos de las DLT

A. Libro mayor (Ledger)

En una tecnología de contabilidad distribuida, el libro mayor o *ledger* representa la estructura de datos que define la forma con la que se almacenan las transacciones [41].

i. Blockchain (Cadena de Bloques)

Como libro mayor seguro, blockchain organiza la creciente lista de registros de transacciones en una cadena de bloques, que es una estructura de datos ordenada, donde cada bloque contiene un conjunto de transacciones y está protegido por técnicas de criptografía para reforzar la integridad de sus registros [48]. El hash del bloque anterior, sirve como enlace criptográfico para formar la cadena de bloques. El valor hash de todo el bloque en sí, puede verse como su imagen criptográfica y sirve para verificar que ninguna de las transacciones ha sido alterada; dado que se calcula en función de todas las transacciones que almacena el bloque, considerando también el hash del bloque anterior [45]. Las transacciones que forman parte del bloque se estructuran en un árbol de Merkle y el valor de la raíz de este árbol también se almacena en el encabezado del bloque como se muestra en la Fig. 4 [49].

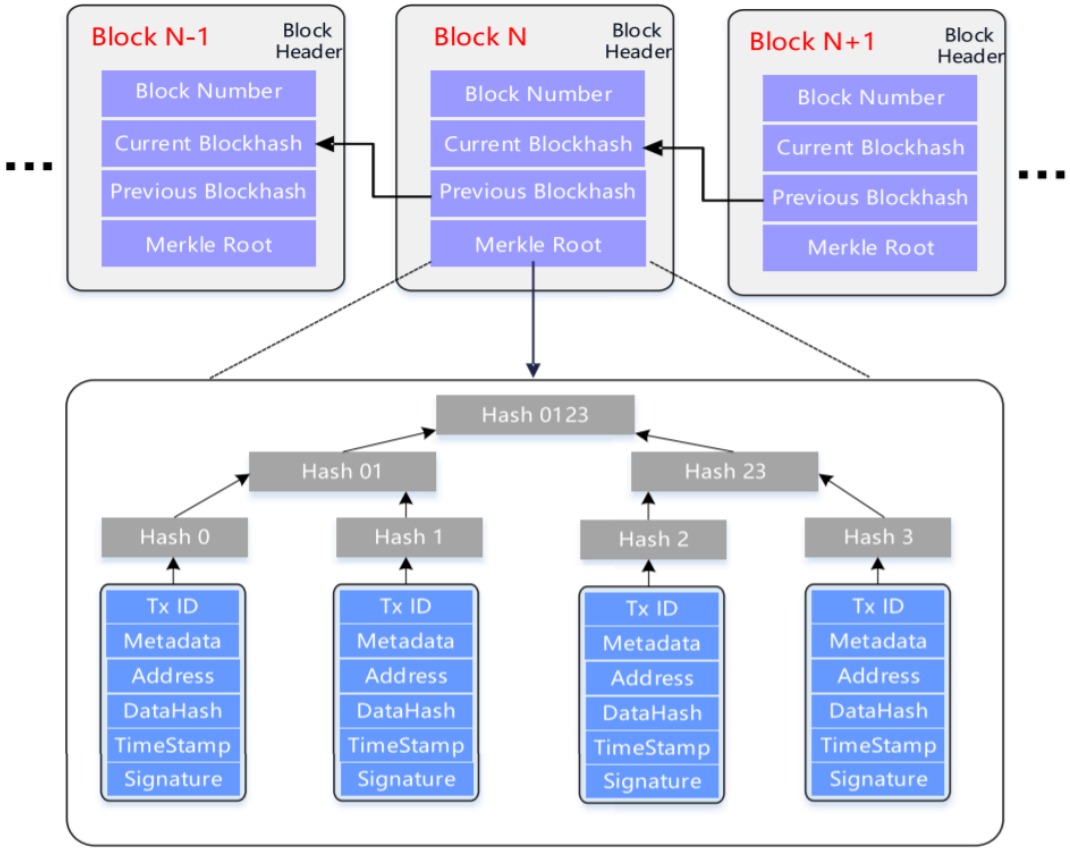


Figura 4. Estructura de blockchain

ii. DAG (Grafo Acíclico Dirigido)

El grafo acíclico dirigido o DAG por sus siglas en inglés (Directed Acyclic Graph), es un libro mayor con un flujo de transacciones individuales entrelazadas que se pueden confirmar en paralelo (por ejemplo, IOTA [41]. Desde una perspectiva de Ciencias de la Computación, un DAG sirve como un grafo donde las transacciones actúan como los nodos y los bordes tienen direcciones. En los DAG no hay minería y las transacciones no se agrupan para formar bloques. Las nuevas transacciones deben autenticar al menos una transacción previa al unirse al DAG. Cada nueva transacción debe referirse a la transacción principal. La nueva transacción firma los hashes de la transacción principal y luego incorpora esos hashes en la nueva transacción [47]. En la Figura 5 se puede observar cómo se incorpora una nueva transacción al DAG [50].

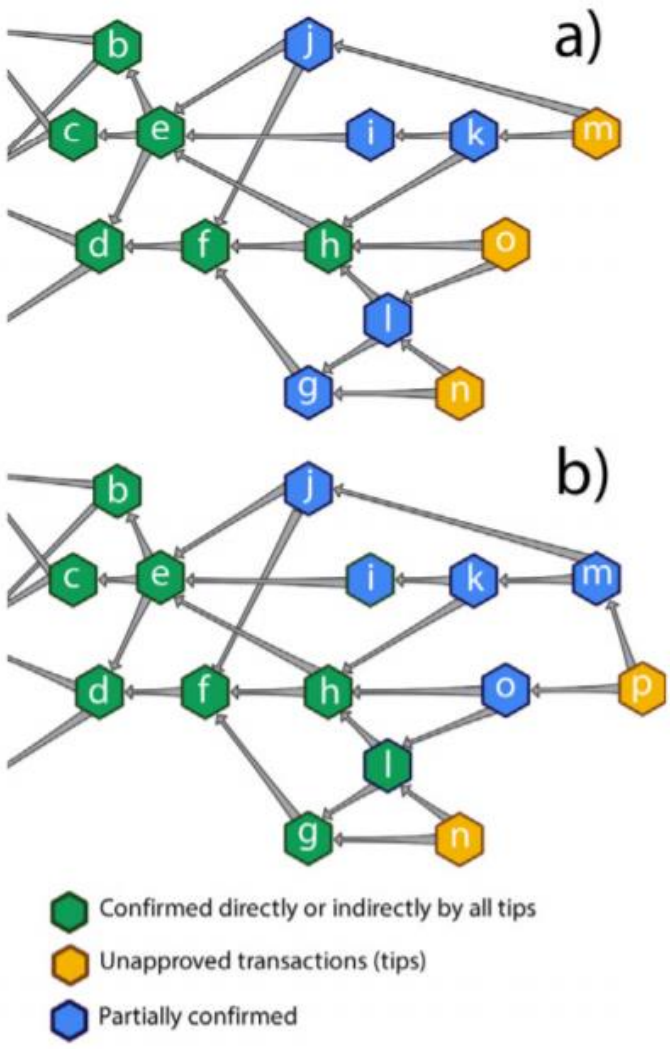


Figura 5. Parte de un Grafo Acíclico Dirigido (a) Estado en un momento t (b) Estado t+1, con una nueva transacción p

B. Red P2P

Los *ledgers* se replican en los nodos de una red distribuida peer-to-peer. La configuración de estos nodos puede ser sin permiso en las redes públicas o con permiso en las redes privadas y federadas [41].

i. Pública

En una red pública, el principio básico es garantizar la equidad a través de la transparencia al compartir toda la información. Cualquiera puede participar en las actividades de esta red. Es natural utilizar sistemas públicos de cadena de bloques, como Bitcoin y Ethereum, como tecnología subyacente para respaldar la ejecución de este tipo de red que funciona a gran escala, por lo que estos sistemas deben resistir el fraude y la piratería de nodos de blockchain maliciosos [51].

ii. Federada o de Consorcio

Este tipo de red es administrada por un grupo particular de usuarios y no permite que los participantes fuera del grupo verifiquen las transacciones. Es posible que el público pueda leer transacciones, pero solo los miembros de un grupo seleccionado pueden escribir transacciones. Hyperledger Fabric es la cadena de bloques federada más común y mejor establecida [47].

iii. Privada

Las redes privadas suelen ser fundamentales para una sola organización que tiene la capacidad de autenticar transacciones. Se puede permitir que el público o las partes aprobadas lean las transacciones [47]. Esta es una red centralizada que tiene una autoridad central que determina el permiso sobre quién puede leer, escribir o participar en la cadena de bloques. Por lo tanto, el mecanismo de consenso en las cadenas de bloques privadas está definido por una sola autoridad central [52].

C. Gobernanza

El gobierno del DLT define el conjunto de reglas para los usuarios que interactúan con el sistema. El componente más importante es el mecanismo de consenso, que es responsable de definir cómo escribir, validar y mantener la consistencia de los registros de transacciones incluidos en la copia del *ledger* en cada nodo de la red [45].

i. Proof of Work

PoW es el mecanismo de consenso más clásico [53]. Su idea central es que los miembros de la red trabajan para verificar transacciones, sugerir bloques candidatos y recolectar recompensas [54]. La prueba de trabajo también es conocida como minería, se basa en una función que requiere una gran potencia computacional, producir un dato es costoso, ocupa mucho tiempo y energía [4]. Las funciones de prueba de trabajo más comunes incluyen raíz cuadrada entera, módulo de un primo grande y secuencias de hash. Puede defenderse de los ataques de denegación de servicio (DoS) porque se necesita una potencia informática masiva para montar un ataque DoS exitoso [47].

ii. Proof of Stake

Después de la Prueba de trabajo, el siguiente algoritmo de consenso común en las DLT es la Prueba de participación o PoS. El nodo seleccionado para realizar el nuevo bloque se elegirá mediante un proceso en el que la selección depende de los activos almacenados en la billetera (o grupo de acciones) relacionados con ese nodo. Este método no necesita una alta potencia informática para validar ninguna prueba y, por lo tanto, los mineros no recibirán ninguna recompensa, excepto las tarifas de transacción [47], [52].

iii. Practical Byzantine Fault Tolerance (PBFT)

Tolerancia práctica a fallas bizantinas o PBFT es un nuevo algoritmo de replicación de máquina de estado que funciona en un sistema asincrónico y es capaz de tolerar fallas bizantinas [49]. Cuando un nodo transmite un mensaje, los nodos restantes intercambian información para verificar el mensaje en caso de que se vea comprometido durante la transmisión. Los buenos nodos llegan a un acuerdo mayoritario con respecto al estado de la cadena de bloques. Este algoritmo requiere una latencia baja y un tiempo de sobrecarga reducido. [47].

2.2.2.3. Plataformas DLT

A. Bitcoin

Bitcoin es un sistema de moneda digital basado en la criptología informática y la arquitectura de red descentralizada (peer-to-peer), para servir como medio de pago y almacenamiento de valor mediante un sistema de autenticación descentralizado que permite contrarrestar las falsificaciones y los problemas de doble gasto sin requerir que instituciones centrales autentiquen las transacciones y sirvan como repositorios [55]. Las transacciones de Bitcoin se lanzan a la red y los nodos las validan a medida que se propagan por toda la red. Los nodos de validación, conocidos como mineros, compiten para extraer grupos de transacciones en bloques y ganar BTC como recompensa [4].

B. Etherium

La segunda criptomoneda más grande es Ethereum Blockchain, cuenta con una plataforma informática distribuida de código abierto que destaca la utilidad de los contratos inteligentes (secuencias de comandos), los cuales son interpretados por una máquina virtual restringida llamada Ethereum Virtual Machine (EVM) y se programan en lenguaje Solidity [56].

"Ether" es el combustible criptográfico interno de Ethereum, ya que se utiliza como tarifa de transacción. Todos los que quieran enviar cualquier transacción, requieren de una cuenta; en esta blockchain existen dos tipos de cuentas: las de propiedad externa, que se controlan mediante claves privadas; y cuentas de contrato, en donde el control se realiza a través de su código de contrato o Smart Contract [57].

C. Hyperledger

Hyperledger es uno de los proyectos más grandes en la industria blockchain, que se compone de un conjunto de subproyectos y herramientas de código abierto de la Fundación Linux, e incluye líderes en diferentes sectores que tienen como objetivo construir un marco de cadena de bloques sólido. Es un proyecto general, que tiene la finalidad de proporcionar soluciones empresariales y pautas universales para la implementación de blockchain [58]. Los proyectos clave dentro del marco de Hyperledger son Hyperledger Fabric, Hyperledger Iroha, Hyperledger Indy, Hyperledger Sawtooth, Hyperledger Cello, Hyperledger Explorer, Hyperledger Composer [59].

D. Hedera Hashgraph

Hashgraph es una *blockchain* basada en DAG, utiliza el protocolo *gossip* y el mecanismo de voto virtual para garantizar que el algoritmo pueda ejecutarse de manera eficiente y tener una alta seguridad en un entorno asincrónico [54], tiene tolerancia a fallas bizantinas y puede escalar más allá de las 250.000 transacciones por segundo [39].

Hedera está diseñada para aplicaciones rápidas, justas y seguras; aprovecha la eficiencia de hashgraph en una red pública descentralizada en la que puede confiar, su plataforma es *open review* pero no *open source* [60]. Hedera Consensus y Token Service aprovechan las características de alto rendimiento y baja latencia de la red, ejecutándose con el rendimiento nativo del protocolo hashgraph subyacente de la red. El Hedera Token Service (HTS) permite la configuración, acuñación y gestión de tokens fungibles y no fungibles, sin necesidad de configurar e implementar un contrato inteligente [60].

E. IOTA

IOTA es una DLT que utiliza el *Tangle*, un grafo acíclico dirigido o DAG [61], este grafo es el responsable de la persistencia de las transacciones en la red [62]. IOTA no tiene bloques, ni cadenas, ni mineros; por lo tanto, funciona de manera bastante diferente en comparación con blockchain y otros DLT. El algoritmo de firma digital de curva elíptica (ECDSA) se utiliza para crear los enlaces entre los bloques. Además, IOTA se basa en firmas de criptografía basadas en hash de Winternitz. Sin embargo, todavía existen algunas similitudes subyacentes entre IOTA y blockchain; ya que ambas tecnologías emplean bases de datos distribuidas, redes peer-to-peer, y mecanismos de consenso [63].

El objetivo de IOTA es facilitar la comunicación de igual a igual entre máquinas y humanos [62], garantiza un alto rendimiento de las transacciones generadas en los sistemas de IoT, por sus características clave, como el soporte de micropagos y la ausencia de tarifas de transacción [64], [65], además su arquitectura DAG le otorga escalabilidad, descentralización, transacciones rápidas, inmunidad cuántica, integridad de datos e interoperabilidad con blockchain [28], [66]. Las transacciones se agregan continuamente al Tangle y cada nueva transacción aprueba dos transacciones existentes a las que selecciona como padres para incorporarse a la red [64]. En otras palabras, el Tangle es un nuevo tipo de base de datos [67], en donde cada participante de la red que está realizando una transacción, participa activamente en el consenso [66].

2.2.3. Análisis comparativo de las plataformas DLT

Al momento de elegir una plataforma DLT como almacenamiento seguro, se deben considerar los requisitos y arquitectura del proyecto. Con la finalidad de establecer una comparativa, se han establecido cuatro características: capacidad de transacciones gratuitas, consumo de energía, tipo de red P2P y si su código es Open Source (Tabla 1).

La capacidad de transacciones gratuitas es una característica importante en el presente proyecto, en donde no sería lógico que los votantes tengan que pagar una comisión por emitir su voto. El consumo de energía de las DLT que utilizan minería es alto. Por el contrario, las DLT basadas en DAG como IOTA y Hedera Hashgraph presentan un consumo de energía más eficiente [68], [69]. Las DLT con red P2P pública ofrecen una mayor descentralización, aun así, las redes privadas y federadas pueden tener interesantes usos empresariales, pero requieren de recursos suficientes para configurar y desplegar los nodos propios. Finalmente, el código Open Source es esencial para asegurar la transparencia de la plataforma.

DLT	Transacciones gratuitas	Consumo de energía	Red P2P	Open Source
BITCOIN	No	Alto	Pública	Si
ETHERIUM	No	Medio	Pública	Si
HYPERLEDGER FABRIC	Si	Medio	Federada	Si
HEDERA HASGRAPH	No	Bajo	Pública	No
IOTA	Si	Bajo	Pública	Si

Tabla 1. Comparación de plataformas DLT

Luego de un análisis de varias alternativas, se eligió utilizar IOTA para desarrollar el prototipo de la presente propuesta tecnológica, tomando en consideración que permite realizar transacciones gratuitas, su consumo de energía es bajo, es de acceso público y es *Open Source*. Inicialmente está DLT fue diseñada por sus creadores para almacenar las grandes cantidades de datos generados por el Internet de las Cosas; sin embargo, su eficiencia y escalabilidad pueden ser aprovechadas en la votación electrónica para ofrecer confiabilidad mediante el almacenamiento encriptado e inmutable en una red segura que funciona como una base de datos distribuida.

2.2.4. Metodología Ágil centrada en el desarrollo de Software Blockchain

Agile Block Chain Dapp Engineering, también conocida como metodología ABCDE, sigue los principios del Manifiesto Ágil, por lo que utiliza varias prácticas como las historias de usuario y el desarrollo iterativo e incremental. Sin embargo, también hace uso de notaciones más formales, como algunos diagramas UML que describen el diseño del sistema. ABCDE aprovecha un enfoque ágil, para adaptarse al desarrollo de sistemas cuyos requisitos no se comprenden completamente desde el principio, o tienden a cambiar, como es el caso de las DAPPS. ABCDE cubre todas las fases estándar del ciclo de vida del software: obtención de requisitos, diseño, implementación, evaluación, prueba de seguridad y mantenimiento continuo. En la Figura 6, tomada de [70], se presenta gráficamente el flujo de actividades establecidos por la metodología ABCDE.

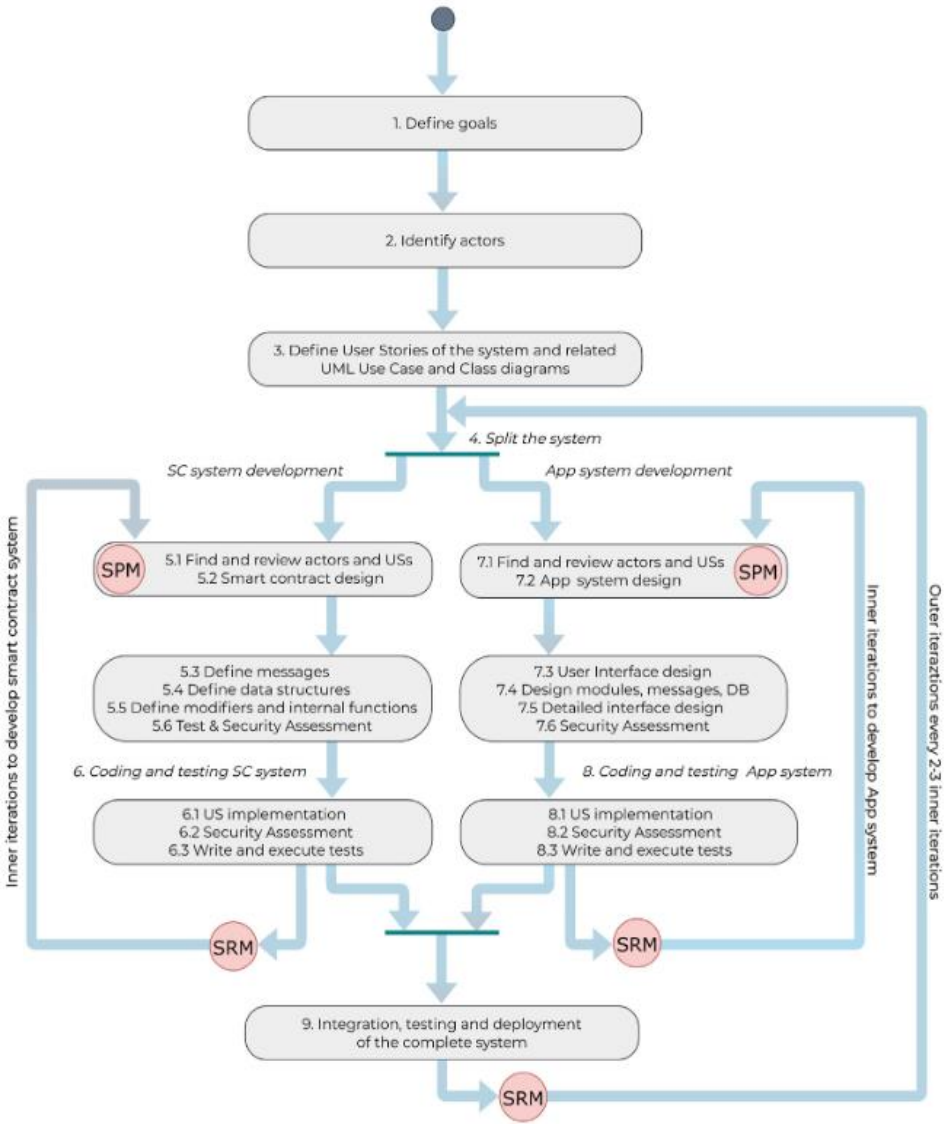


Figura 6. Procesos de la metodología ABCDE

2.2.5. Tecnologías de desarrollo web

Internet es uno de los grandes éxitos técnicos de nuestra época, comenzando con solo cuatro nodos en 1969, utilizado únicamente por investigadores para un conjunto muy limitado de aplicaciones orientadas a texto, ha crecido hasta convertirse en una infraestructura mundial que brinda servicios sofisticados que tienen un papel fundamental en la vida diaria de millones de personas. Es imposible no sorprenderse de su asombroso crecimiento y el grado en que ha cumplido su ambicioso objetivo de proporcionar acceso a la información, a cualquier persona, en cualquier lugar y tiempo [71]. Actualmente, hay una variedad de tecnologías para el desarrollo web, entre las que destacan: el Lenguaje de Marcado de Hipertexto (HTML), las Hojas de Estilo en Cascada (CSS), JavaScript y otros lenguajes de programación, para los que han ido surgiendo frameworks o librerías que permiten múltiples funcionalidades, así como también la conexión a bases de datos.

2.2.5.1. Lenguaje de Programación

A. JavaScript

JavaScript se ha convertido en un lenguaje de programación popular en aplicaciones web, tanto en el lado del cliente como para el lado del servidor [72]. Se usa para asignar controladores de eventos a botones, enlaces y cuadros de entrada, definiendo efectivamente la funcionalidad de la aplicación web cuando el usuario interactúa con sus componentes. Además, JavaScript se puede utilizar para enviar solicitudes HTTP asincrónicas al servidor y actualizar el contenido de la página web con la respuesta resultante [73].

JavaScript contiene varias características que lo distinguen de los lenguajes tradicionales. En primer lugar, el código JavaScript se ejecuta mediante un modelo asincrónico. Esto permite que los controladores de eventos se ejecuten bajo demanda, ya que el usuario interactúa con los componentes de la aplicación web. En segundo lugar, gran parte de JavaScript está diseñado para interactuar con una entidad conocida como Document Object Model (DOM). Esta estructura dinámica en forma de árbol que incluye los componentes de la aplicación web y cómo están organizados. JavaScript se puede usar para acceder o manipular los componentes del DOM permitiendo así que la página web cambie sin necesidad de recargarse [73].

B. NodeJS

Node.js escrito en lenguaje C ++, es un entorno de ejecución de JavaScript, que utiliza el motor Google Chrome V8 para un buen rendimiento. Node.js utiliza programación asíncrona impulsada por eventos y está diseñado para facilitar el desarrollo y ejecución de un servidor web, incluyendo HTTP, DNS, NET, UDP, HTTPS, TLS, etc [74].

NodeJS se usa a menudo como parte de una pila completa de tecnologías para el desarrollo de aplicaciones web, porque permite a los desarrolladores utilizar el mismo lenguaje (Javascript / Typecript) para el backend y para el frontend [75].

2.2.5.2. Frameworks

A. Framework Backend: Express

Express es un framework de desarrollo del lado del servidor muy simple y flexible basado en NodeJS. Este marco de trabajo contiene un conjunto de módulos que ayudan a los desarrolladores a crear aplicaciones y servicios web [76].

B. Framework Frontend: Vuejs

Vuejs es un framework de programación frontend basado en JavaScript que se caracteriza por su simplicidad y se centra principalmente en separar los componentes para su reutilización. La división de la lógica empresarial en componentes dedicados se conoce como separación de preocupaciones y se considera una práctica recomendada [77].

2.2.5.3. Base de datos

A. Postgresql

PostgreSQL es un marco de administración de bases de datos (DBMS) de código abierto creado por un grupo general de voluntarios. Tiene más de 15 años de avance dinámico y un diseño demostrado que le ha valido una sólida notoriedad por su confiabilidad, veracidad y corrección de la información; no está controlado por ninguna empresa u otra sustancia privada y el código fuente es accesible sin costo alguno [78].

2.3. Objetivos del Prototipo

2.3.1. Objetivo General

- Desarrollar un sistema de votación electrónica utilizando una tecnología de contabilidad distribuida para el almacenamiento seguro de la información en las elecciones de representantes estudiantiles en la Escuela de Informática de la UTMACH.

2.3.2. Objetivos Específicos

- Seleccionar una tecnología de contabilidad distribuida para el almacenamiento encriptado y descentralizado de la información del sistema de votación propuesto.
- Determinar la forma de incorporar en el padrón electoral únicamente a los estudiantes legalmente matriculados en las carreras de la Escuela de Informática de la UTMACH para el periodo académico en el que se realizan las votaciones.
- Utilizar un mecanismo de autenticación que permita certificar la identidad de los votantes para evitar el fraude electoral.
- Desarrollar una aplicación web adaptable a dispositivos móviles para que los estudiantes voten desde cualquier lugar, sin necesidad de acudir a un recinto electoral.
- Gestionar de forma transparente la información del proceso electoral para generar confianza en los votantes; utilizando un sitio web que permita la visualización de la convocatoria, el padrón, las candidaturas y los resultados obtenidos.

2.4. Diseño del Prototipo

2.4.1. Diseño de la Arquitectura de alto nivel

El prototipo tecnológico consiste en una aplicación web que utiliza una tecnología de contabilidad distribuida para el almacenamiento seguro de la información. La DLT seleccionada es IOTA, la cual posee una infraestructura de nodos distribuidos que garantizan la inmutabilidad de las transacciones registradas. La conexión del servidor institucional con la red de IOTA se establecerá mediante una API, que permitirá almacenar los votos con criptografía resistente a la computación cuántica.

La arquitectura del sistema un modelo cliente servidor en donde la comunicación se realiza a través de solicitudes y respuestas HTTP. El servidor web se conecta a Postgres y extrae el listado de estudiantes matriculados en el periodo académico correspondiente a las elecciones, para establecer el padrón electoral. En la fase de pruebas de la propuesta tecnológica se utiliza un conjunto de información ficticia, pero se espera que en un ambiente de producción el Sistema de Votación Electrónica establezca conexión con la base de datos institucional. La aplicación web es adaptable a diferentes tamaños de pantalla, por lo que puede ser accedida desde un navegador mediante dispositivos como tablets, smartphones, laptops y PCs (ver Figura 7).

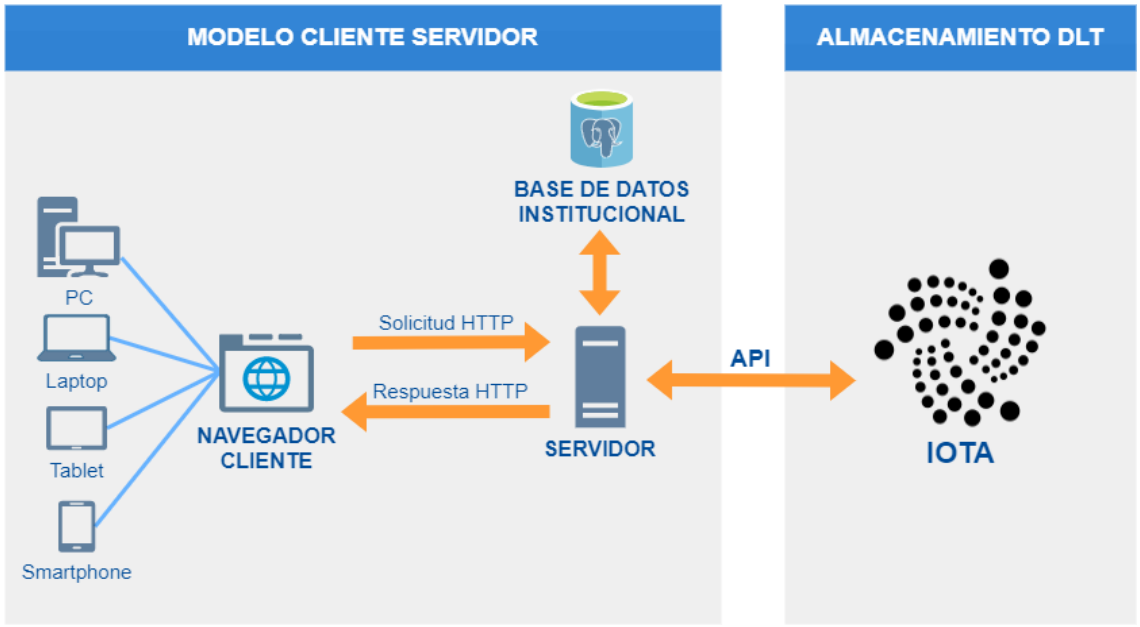


Figura 7. Arquitectura de red del prototipo tecnológico

2.4.2. Diagramas de secuencia

La metodología ABCDE establece los diagramas UML para representar el funcionamiento del sistema, por lo cual se han elaborado diagramas de secuencias para el proceso de creación y publicación de una convocatoria, registro de candidaturas, proceso de sufragio, escrutinio y publicación de resultados (Figs. 8-11).

El proceso de creación y publicación de una convocatoria se presenta en la Figura 8, iniciando con la autenticación del administrador mediante usuario y contraseña, luego el sistema autentica sus credenciales y emite un token de seguridad (JWT) con los permisos de acceso al módulo de configuración. El usuario administrador puede crear una convocatoria a través de un formulario en donde se registran los datos correspondientes como el periodo académico correspondiente, los plazos de fechas para la inscripción de candidaturas, campaña y votación, así como también los requisitos necesarios para la participación de listas o movimientos políticos estudiantiles. Habiendo registrado toda la información pertinente se procede a guardar el registro, con lo cual el módulo de configuraciones crea automáticamente el padrón electoral únicamente con los estudiantes que poseen una matrícula en las carreras de Ingeniería de Sistemas y Tecnologías de la Información para el periodo académico seleccionado en la convocatoria, la misma que puede ser editada o eliminada antes de su publicación en el sitio web informativo, en donde los estudiantes tendrán acceso a la información del proceso electoral.

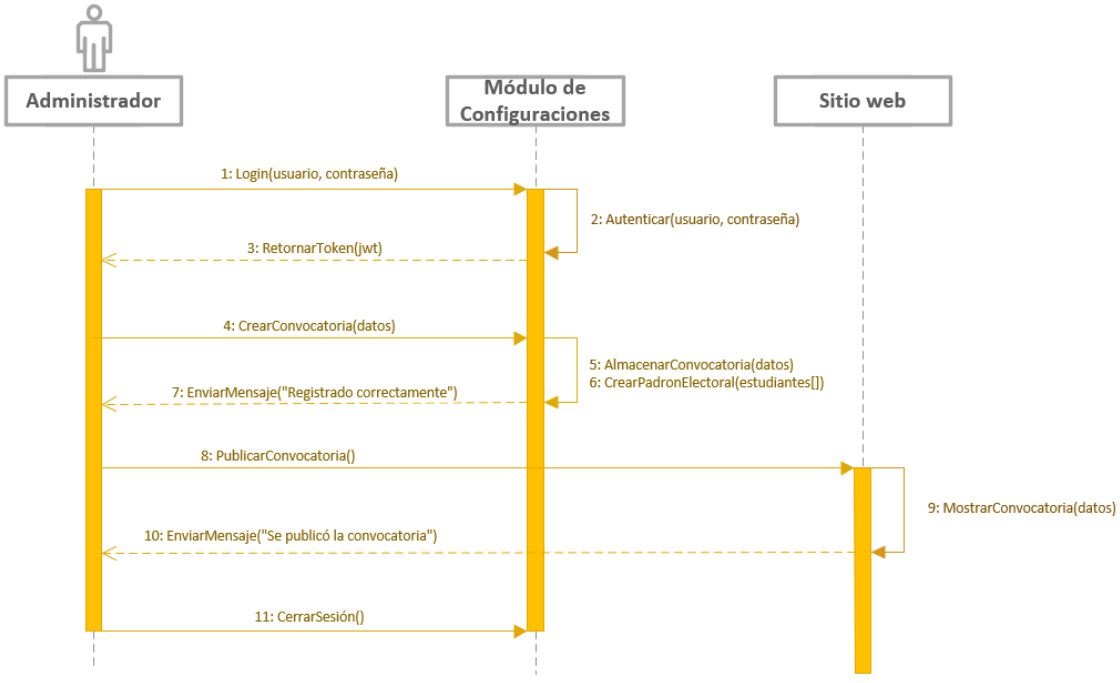


Figura 8. Creación y publicación de una convocatoria

El proceso de registro de candidaturas (Fig. 9) igualmente requiere de la correcta autenticación del usuario administrador. Cada una de las candidaturas aprobadas será registrada en el sistema a través del módulo de configuraciones. Los datos que se registran en una candidatura son la lista, candidatos participantes y la propuesta de trabajo. La información de las candidaturas puede ser modificada antes de su publicación en el sitio web en donde se presenta públicamente toda la información relevante del proceso de votación.

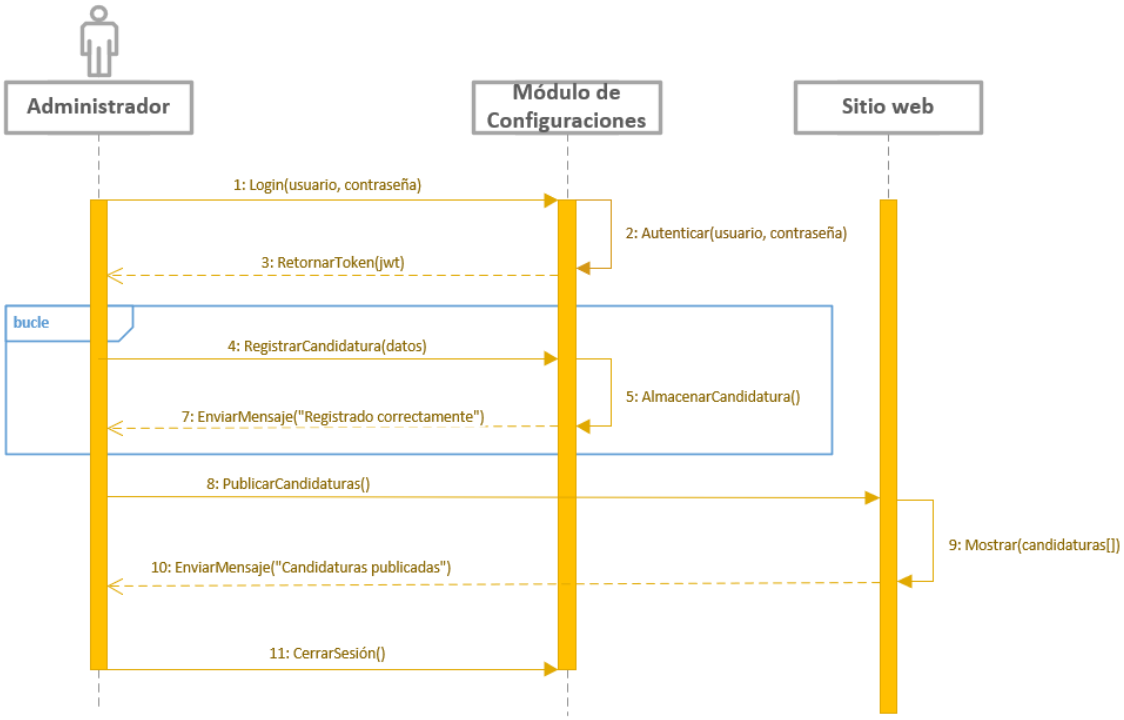


Figura 9. Registro de Candidaturas

El proceso de votación o sufragio se describe en la Figura 10, tiene como primer paso la autenticación del votante con su respectivo usuario y contraseña; luego el módulo de votación se encarga de verificar que no ha votado todavía y le envía un código de verificación mediante SMS, el cual es un factor de seguridad adicional para evitar la suplantación de identidad. Si las credenciales son correctas, se le presenta la papeleta de votación, en la que puede elegir una lista de su preferencia, lo cual será considerado como voto válido; o si desea puede votar nulo o blanco, que se considera como voto no válido. Una vez el votante emite su voto se le pedirá su confirmación para poder almacenarlo en IOTA, retornando el hash del voto para que posteriormente el votante pueda verificar su correcto almacenamiento. Finalmente, se envía el certificado de votación al usuario, para dejar constancia de que ha completado exitosamente el proceso de sufragio.

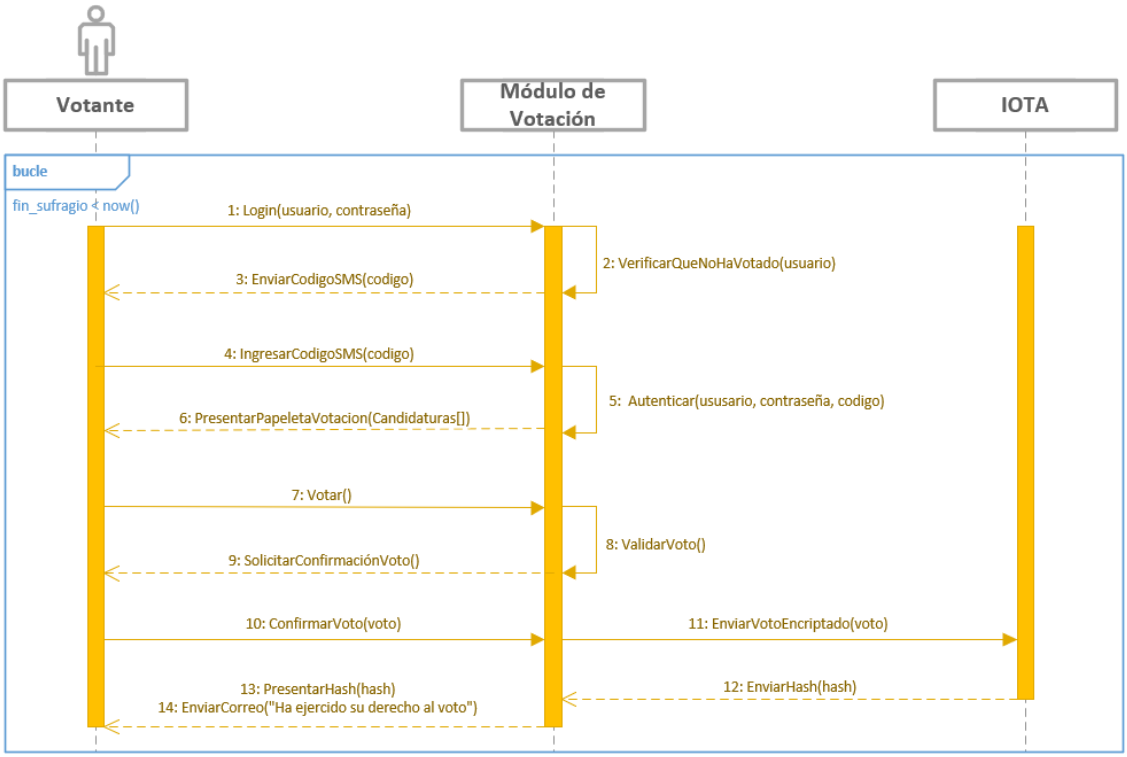


Figura 10. Proceso de sufragio

El proceso de escrutinio lo realiza automáticamente el sistema una vez concluido el tiempo para la votación. Como primer paso solicita los votos almacenados en IOTA, que en el presente caso de aplicación se utiliza como una urna digital. El módulo de votación calcula los resultados con los votos recibidos y procede a publicar en el dashboard los votos y los resultados finales del escrutinio (Fig. 11).

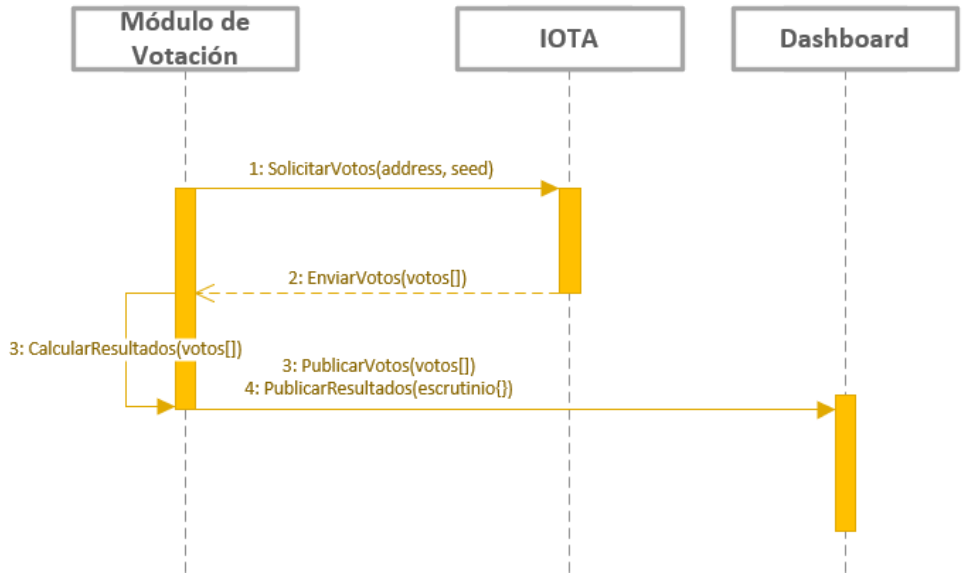


Figura 11. Proceso de Escrutinio y publicación de resultados

2.4.3. Diseño de la base de datos

Las tablas celestes representan a la información requerida desde la base de datos institucional, en donde se almacenan las matrículas de los estudiantes en las distintas carreras que ofrecen las Facultades de la Universidad Técnica de Machala.

Las tablas de color rosado almacenan las configuraciones necesarias para realizar una votación; como la creación de una convocatoria, registro de listas o movimientos estudiantes, y la inscripción de candidaturas. Esta información será gestionada por el usuario con el rol de administrador del sistema.

En el padrón cada votante tiene un código de acceso, válido para una convocatoria; una vez emitido el voto, se cambiará el estatus para que no pueda votar nuevamente. Las tablas de color verde están relacionadas con las votaciones y sus resultados. Los votos se almacenarán de forma segura con una tecnología de contabilidad distribuida.

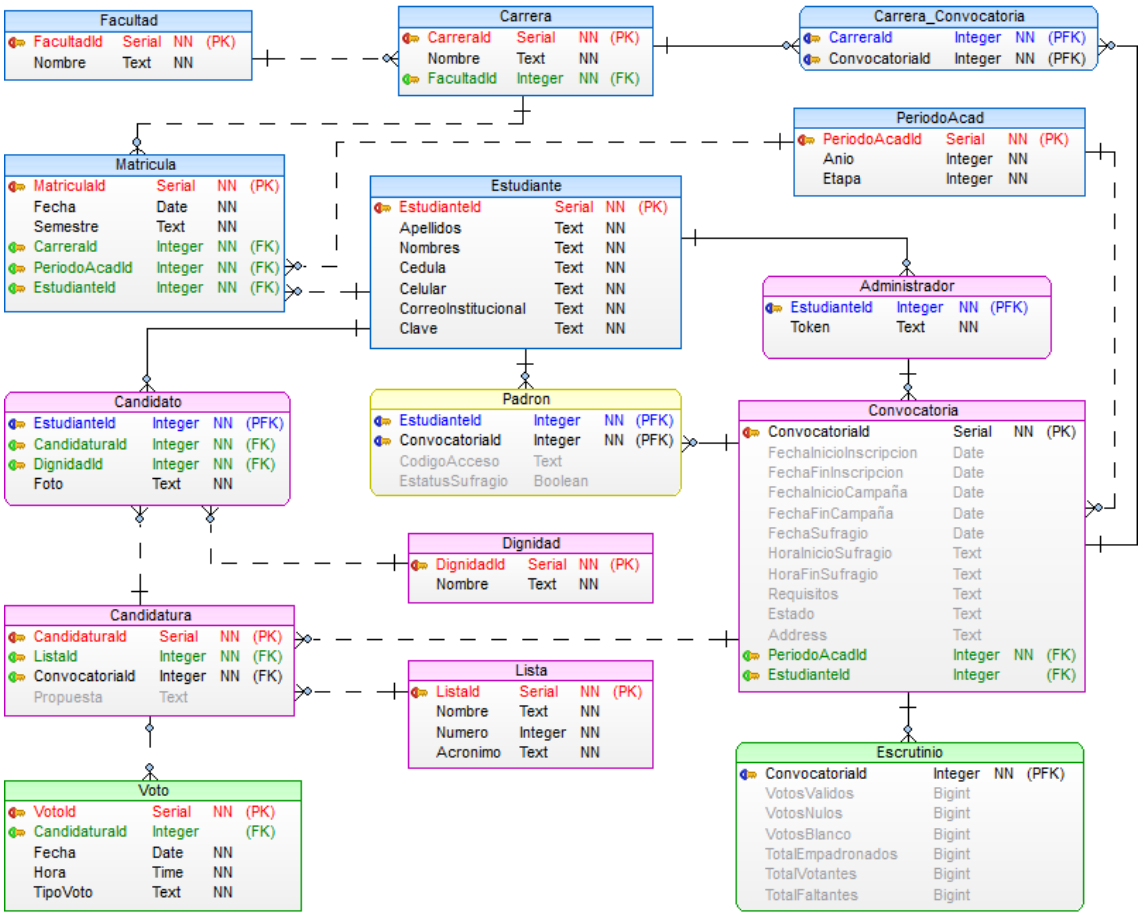


Figura 12. Diagrama de la base de datos

2.5. Ejecución y/o ensamblaje del Prototipo

2.5.1. Configuración del almacenamiento con IOTA

2.5.1.1. Instalación

La aplicación web del sistema de votación propuesto utiliza el almacenamiento de información con IOTA mediante las funciones que ofrece su biblioteca principal. La instalación se realiza abriendo una interfaz de línea de comandos en el directorio del código fuente backend del proyecto, en donde se ejecuta el siguiente comando:

```
npm install @iota/core @iota/converter
```

2.5.1.2. Controlador para el almacenamiento de votos con IOTA

La función sendVote recibe los datos del voto emitido por el estudiante correctamente autenticado en el sistema, se conecta un nodo de la red de desarrollo de IOTA, luego convierte los datos recibidos a Trytes, finalmente los envía y retorna el hash del voto como respuesta al cliente web. En la Figura 13 se utiliza un address y un seed de ejemplo para realizar el test del almacenamiento de votos.

```
const Iota = require('@iota/core');
const Converter = require('@iota/converter');

const dlt = {};
dlt.sendVote = async (req, res) => {
    const { lista, convocatoria, tipo } = req.body;
    const iota = Iota.composeAPI({
        provider: 'https://nodes.devnet.iota.org:443'
    });
    const depth = 3;
    const minimumWeightMagnitude = 9;
    const address = 'GRSVHDEALAWQVWWTUFZWQ9RAIP9OPEQFNDZRHDAZTDBQQNPFEVKYJ9CWEMBIHLEAMNBOB9DIBXSMCGLAC';
    const seed = 'WYTTMVNGPTGWZDQUN9KNMFIZBCAHTYILMTCEIRF9OZSBXPQOXQLFPDVQA9KNBDQCNOUXTABQKFOSEZRJI';
    const message = JSON.stringify([{ "Lista": lista, "Convocatoria": convocatoria, "Tipo": tipo }]);
    const messageInTrytes = Converter.asciiToTrytes(message);
    const transfers = [{
        value: 0,
        address: address,
        message: messageInTrytes
    }];
    iota
        .prepareTransfers(seed, transfers)
        .then(trytes => {
            return iota.sendTrytes(trytes, depth, minimumWeightMagnitude);
        })
        .then(bundle => {
            res.send(bundle[0].hash);
        })
        .catch(err => {
            console.error(err)
        });
};

module.exports = dlt;
```

Figura 13. Controlador para el almacenamiento de votos con IOTA

2.5.2. Sitio web informativo

El sitio web informativo tiene un Home o página de inicio, un dashboard para presentar los resultados de las votaciones y además permite al estudiante autenticarse en el sistema para ingresar al módulo de votación.

A. Home.

Sección 1: Convocatoria. En esta sección del Home se presentan los detalles de la convocatoria, como las fechas de inscripción, campaña y votación.

Figura 14. Convocatoria publicada en el sitio web informativo

Sección 2: Padrón Electoral. Presenta un enlace al padrón electoral, con la finalidad de que el estudiante pueda consultar si se encuentra habilitado para votar en la convocatoria.

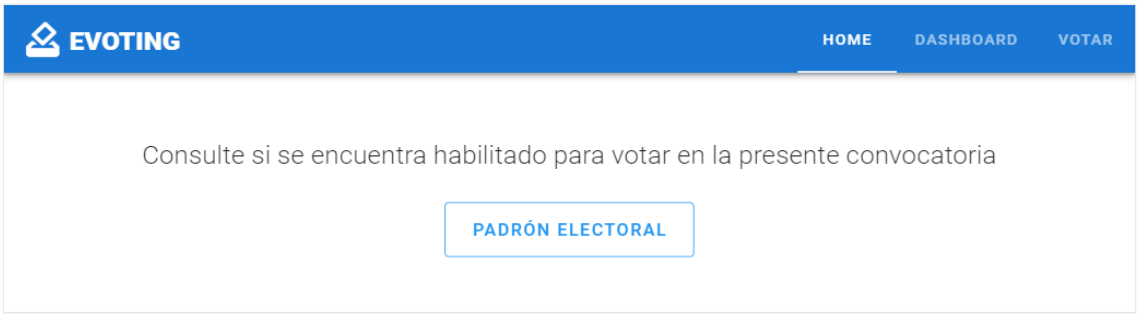


Figura 15. Acceso al padrón electoral desde el sitio web informativo

Sección 3: Candidaturas. Presenta las listas participantes, sus candidatos y un enlace a la propuesta de la candidatura.

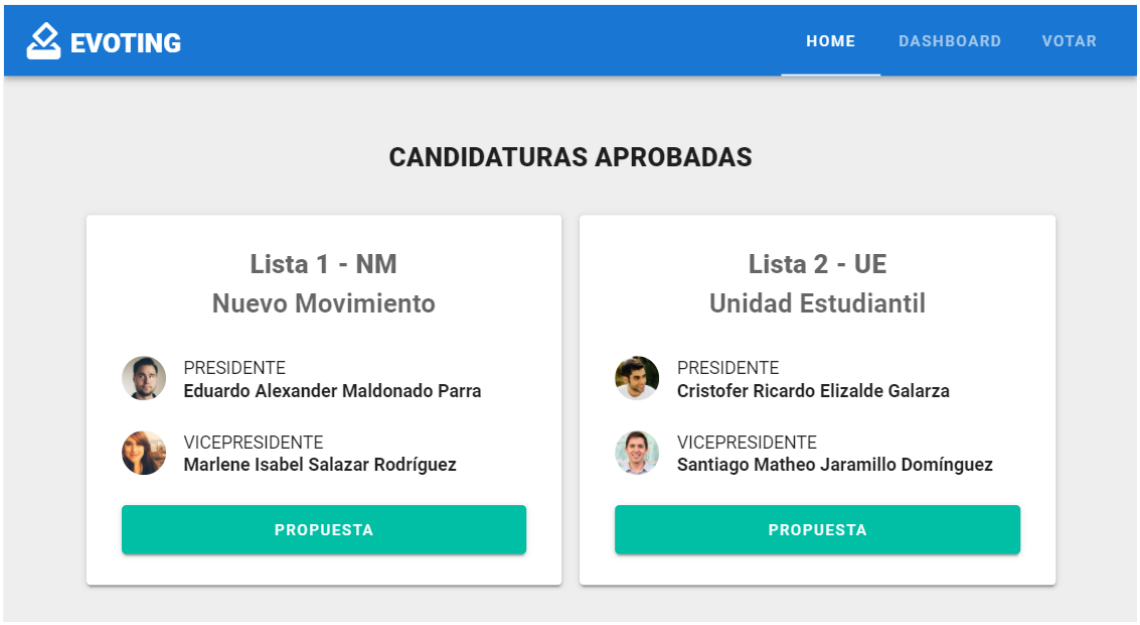


Figura 16. Candidaturas publicadas en el sitio web informativo

B. Dashboard

El dashboard presenta un cronómetro de la cuenta regresiva durante el periodo de votación, el número de estudiantes empadronados y sufragantes, el porcentaje de participación de los electores y los resultados finales del escrutinio de votos.

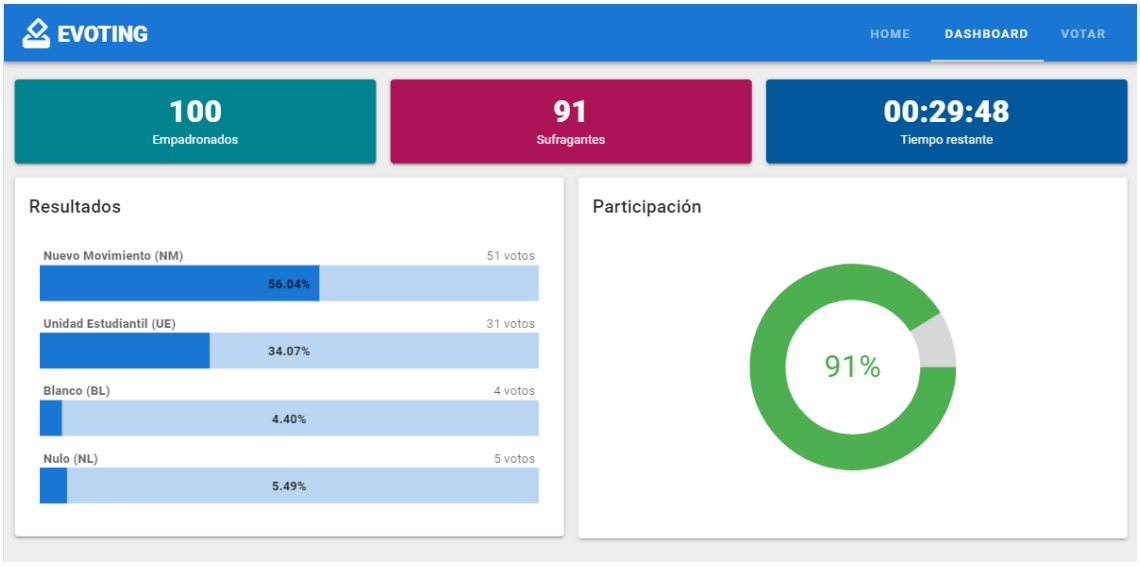


Figura 17. Dashboard de los resultados de la votación

2.5.3. Módulo de configuraciones

A. Autenticación del administrador

Para ingresar al módulo de configuraciones, el administrador debe ingresar sus credenciales en el siguiente formulario, con lo cual podrá autenticarse en el sistema.

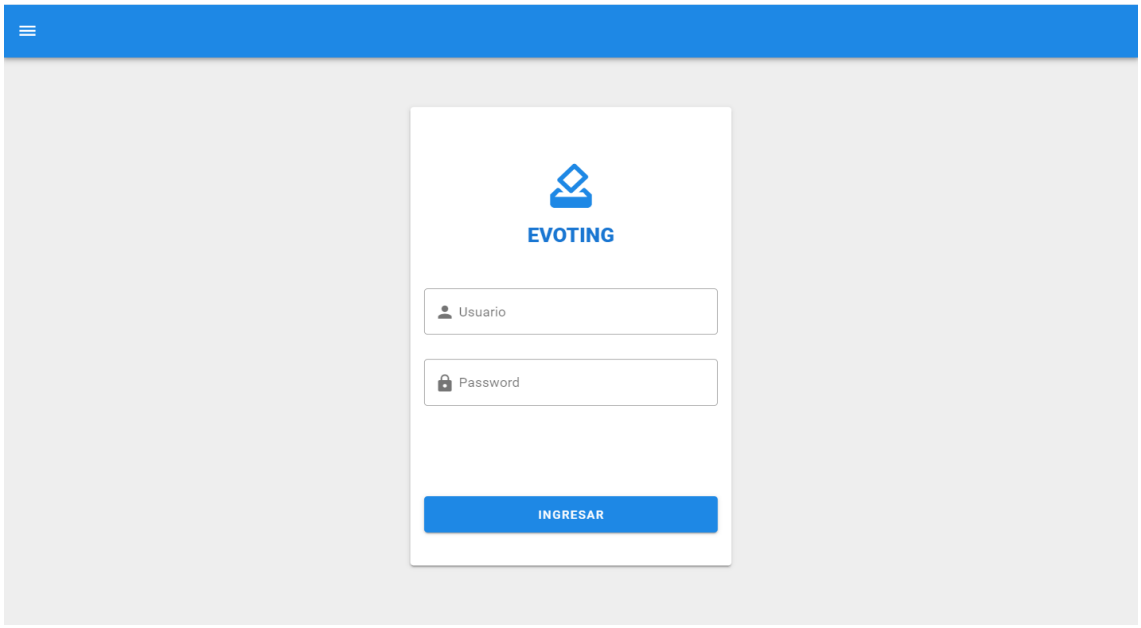


Figura 18. Formulario de autenticación para ingresar al módulo de configuraciones

B. Convocatorias

La configuración de convocatorias se realiza en la siguiente pantalla en donde se tiene un historial de las convocatorias registradas en la plataforma.

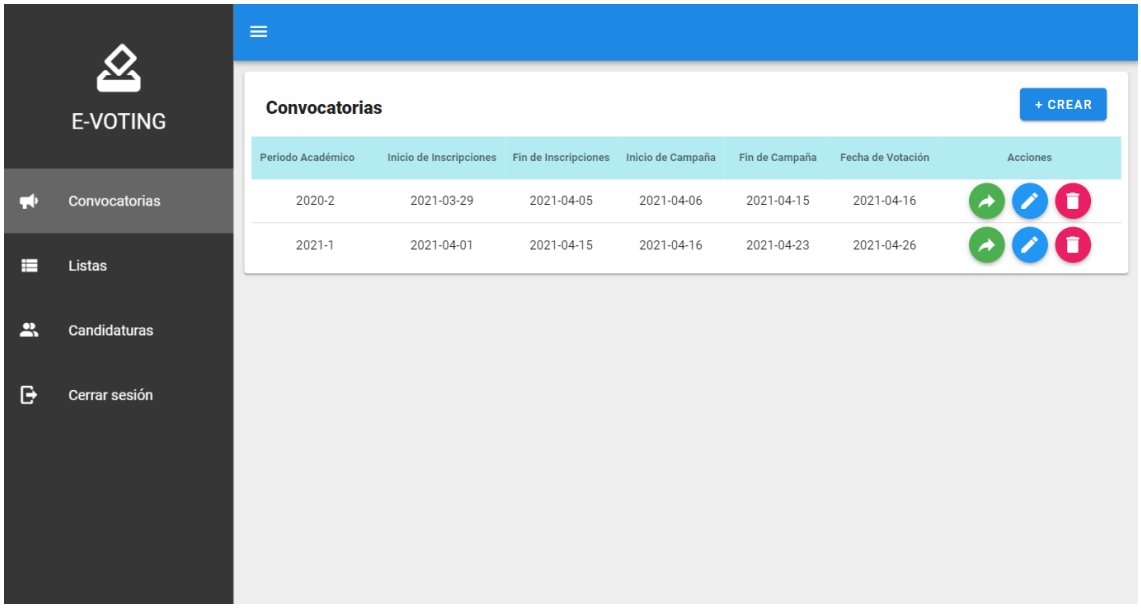


Figura 19. Configuración de convocatorias

Dando clic sobre el botón "+ Crear" en la interfaz de Configuración de convocatorias (Fig. 19), se accede al formulario para crear una nueva convocatoria (Fig. 20).

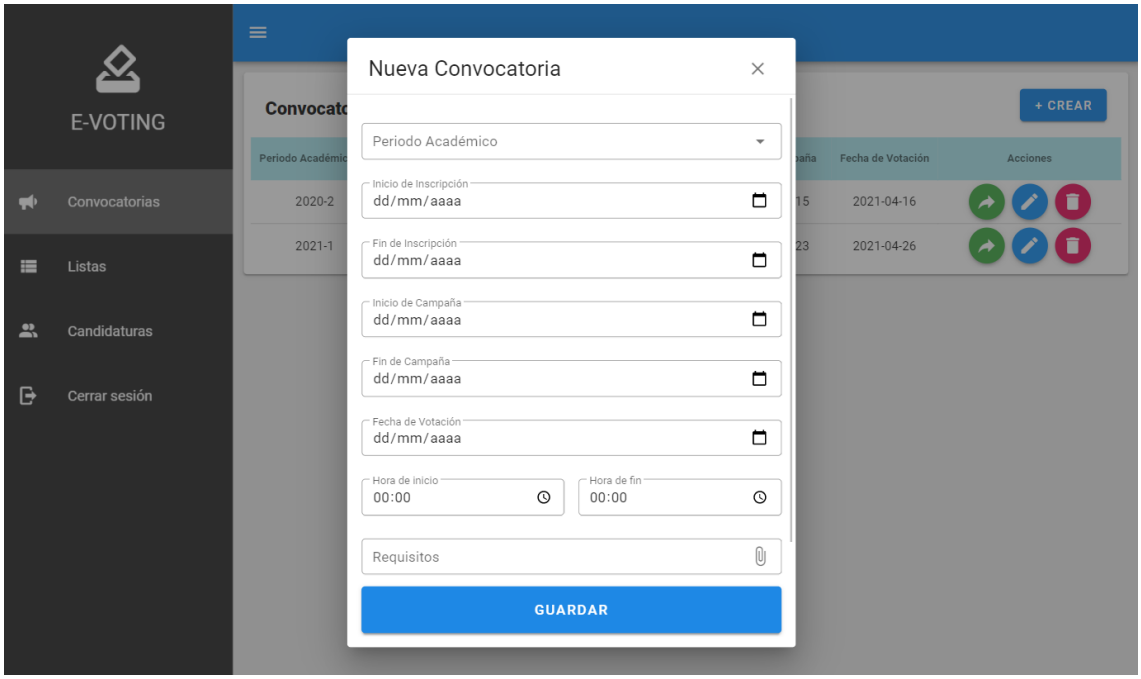


Figura 20. Creación de una convocatoria

C. Registro candidaturas

Luego de haber sido aprobada una candidatura, podrá ser registrada en el sistema por el administrador para ser publicada en el sitio web informativo, y que posteriormente aparezca en la papeleta electrónica para ser elegible el día de la votación.

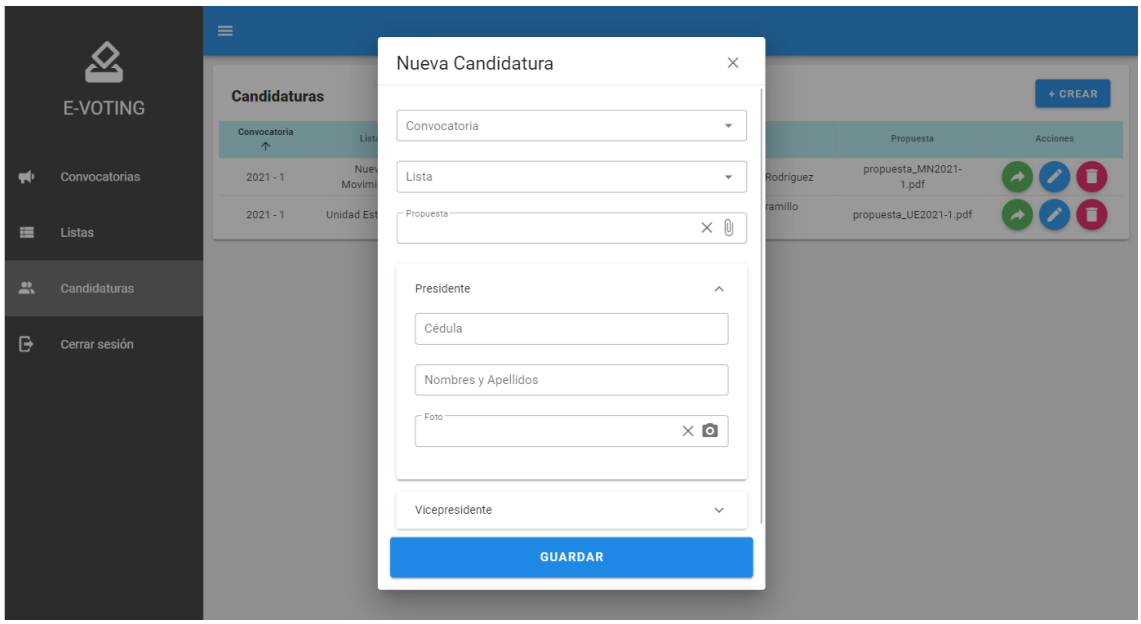


Figura 21. Registro de una candidatura

2.5.4. Módulo de Votación

A. Autenticación del votante

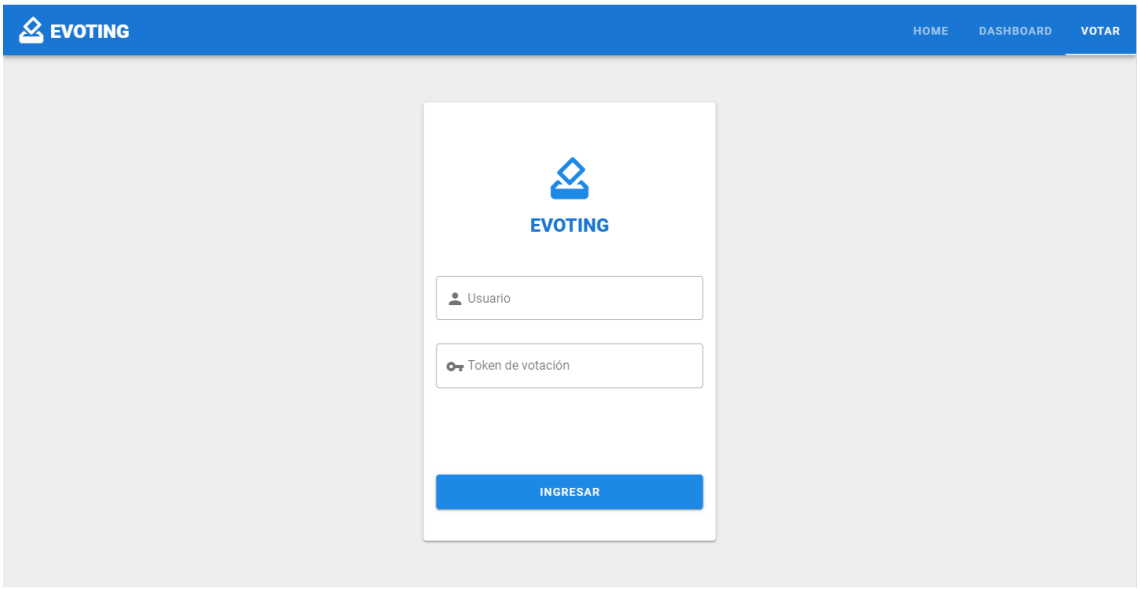


Figura 22. Autenticación del votante

B. Token de acceso enviado al correo institucional

Figura 23. Token de acceso enviado al correo del estudiante empadronado

C. Papeleta de votación

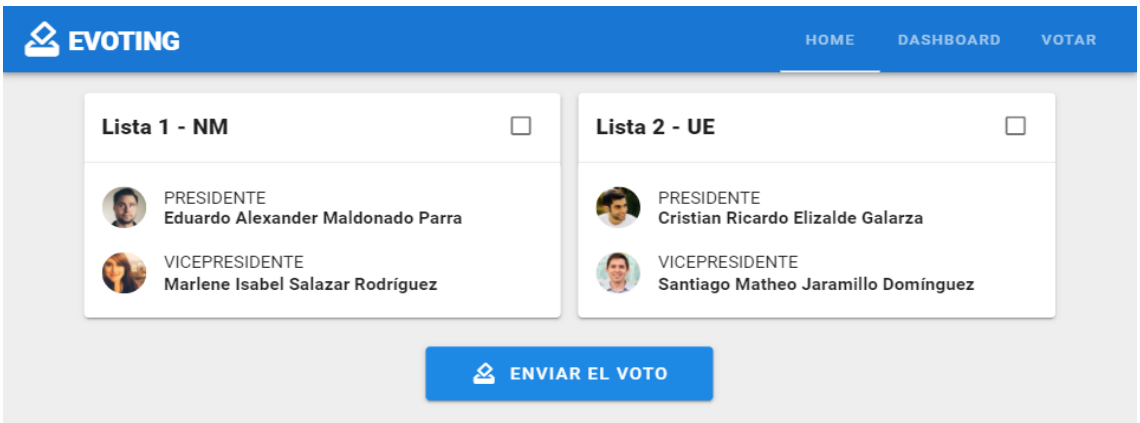


Figura 24. Papeleta de votación

D. Confirmación del voto

Si el votante no ha seleccionado ninguna lista y presiona el botón ‘ENVIAR EL VOTO’, se le presenta una alerta de voto blanco; si el usuario ha seleccionado más de una lista se le presenta una alerta de voto nulo. En caso de haber seleccionado una de las listas participantes, entonces se considera un voto válido.

i. Voto blanco

Figura 25. Voto blanco

ii. Voto nulo

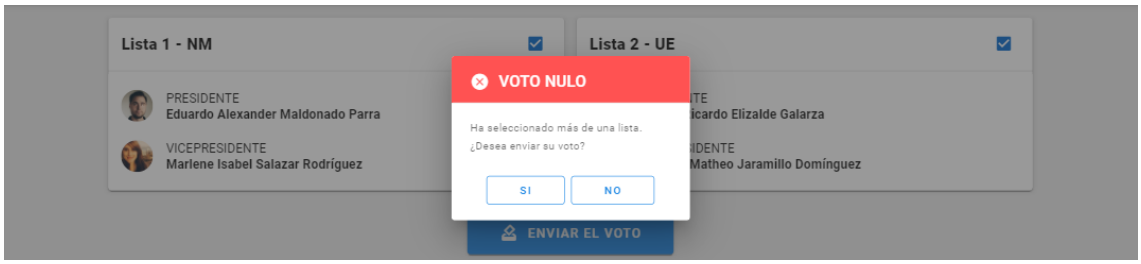


Figura 26. Voto nulo

iii. Voto válido

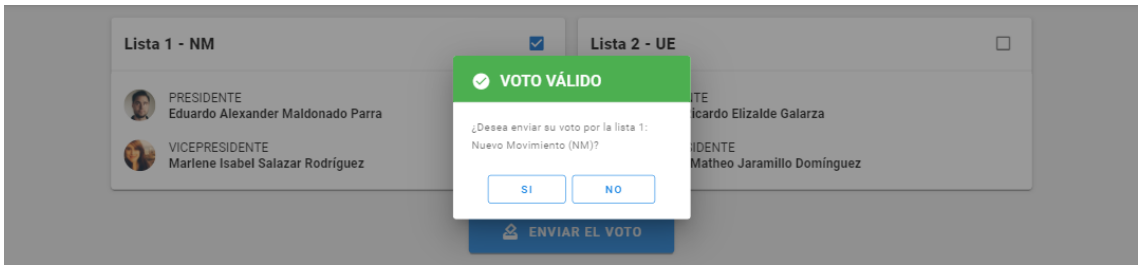


Figura 27. Voto válido – Ejemplo 1

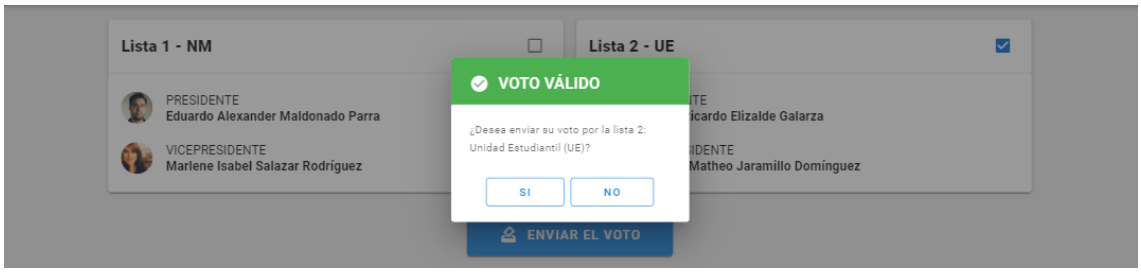


Figura 28. Voto válido – Ejemplo 2

E. Hash del voto almacenado en IOTA

El hash es una cadena de caracteres que sirve para que el usuario pueda verificar que su voto se guardó correctamente. Este hash únicamente se le presenta al votante inmediatamente después de que el sistema envió el voto de forma segura para su almacenamiento en IOTA.

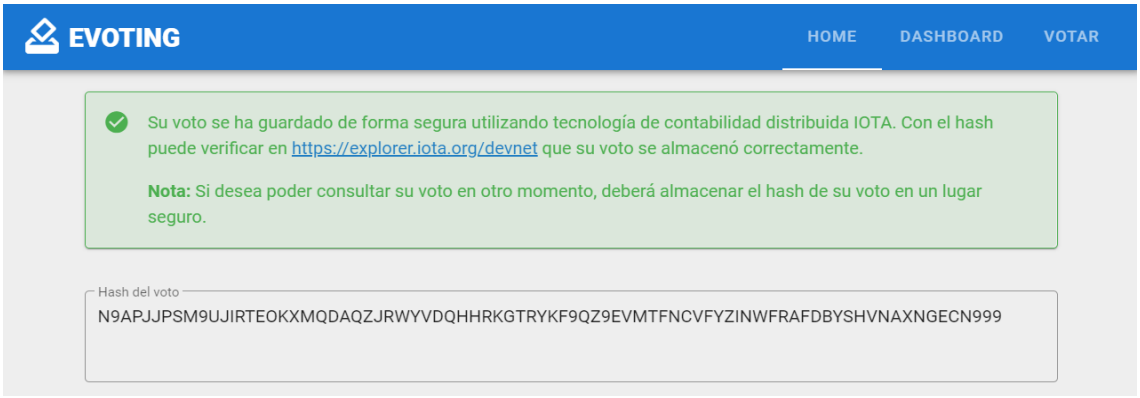


Figura 29. Hash del voto

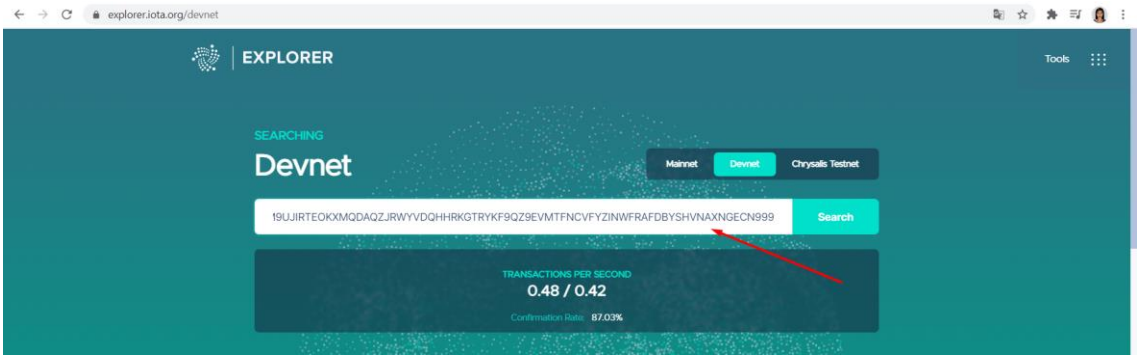


Figura 30. Verificación de un voto mediante el hash

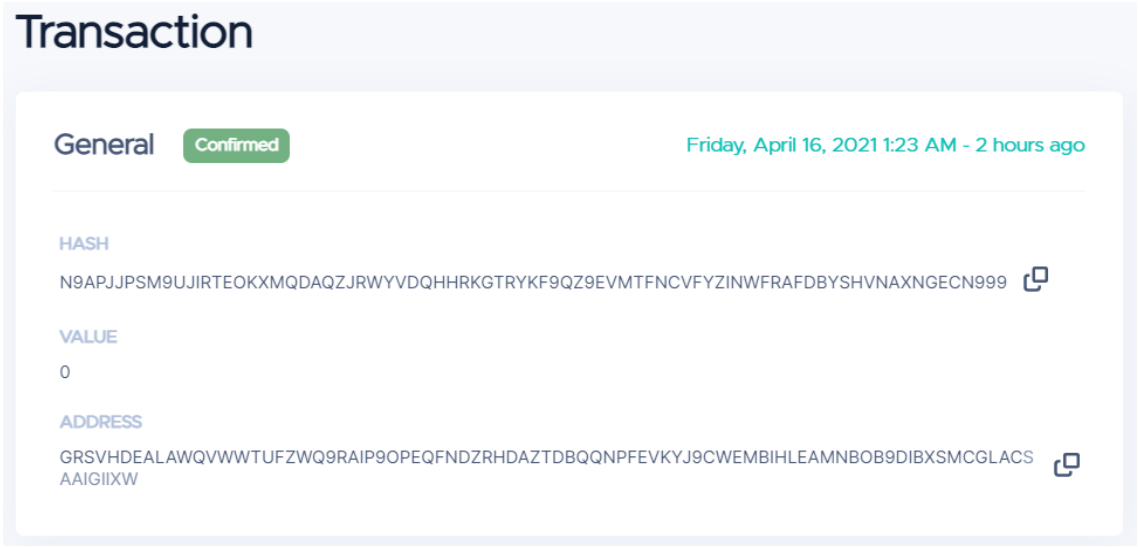


Figura 31. Sección general del voto guardado en IOTA

Figura 32. Contenido de un voto guardado en IOTA

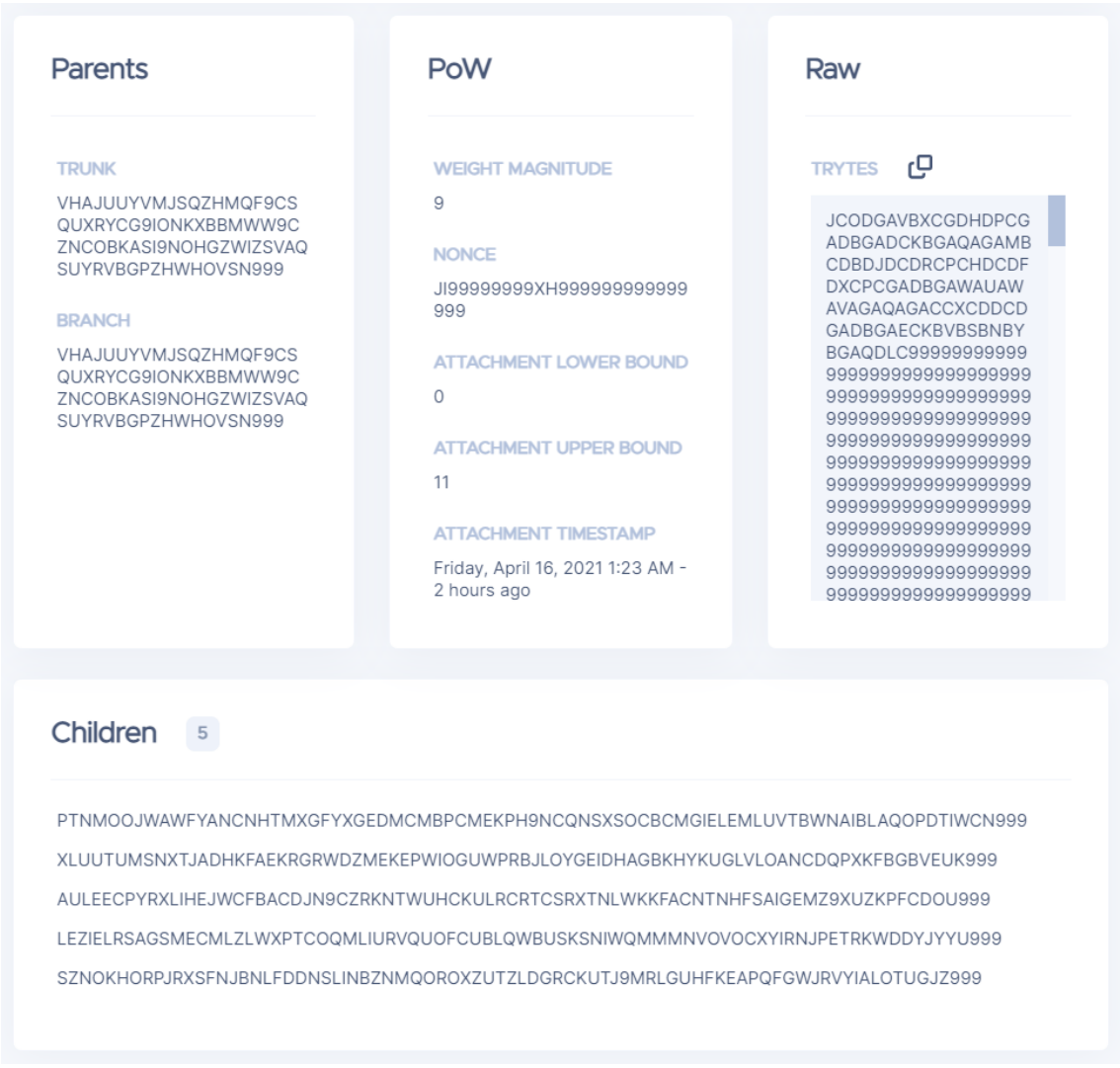


Figura 33. Metadatos de almacenamiento del voto en IOTA

F. Certificado de votación enviado al correo institucional

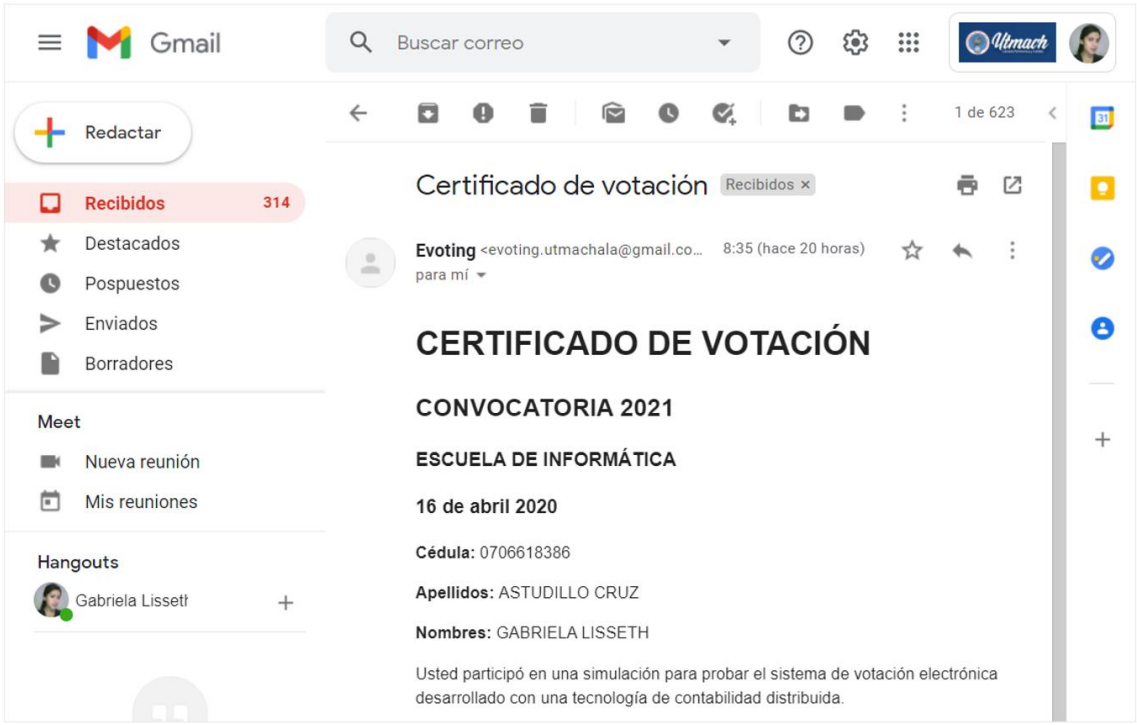


Figura 34. Certificado de votación enviado al correo institucional del votante

G. Revisión de los votos en IOTA Explorer

Las transacciones se pueden verificar en el IOTA Explorer en donde a través de su Address se puede visualizar todas aquellas transacciones que se han almacenado en una votación determinada.

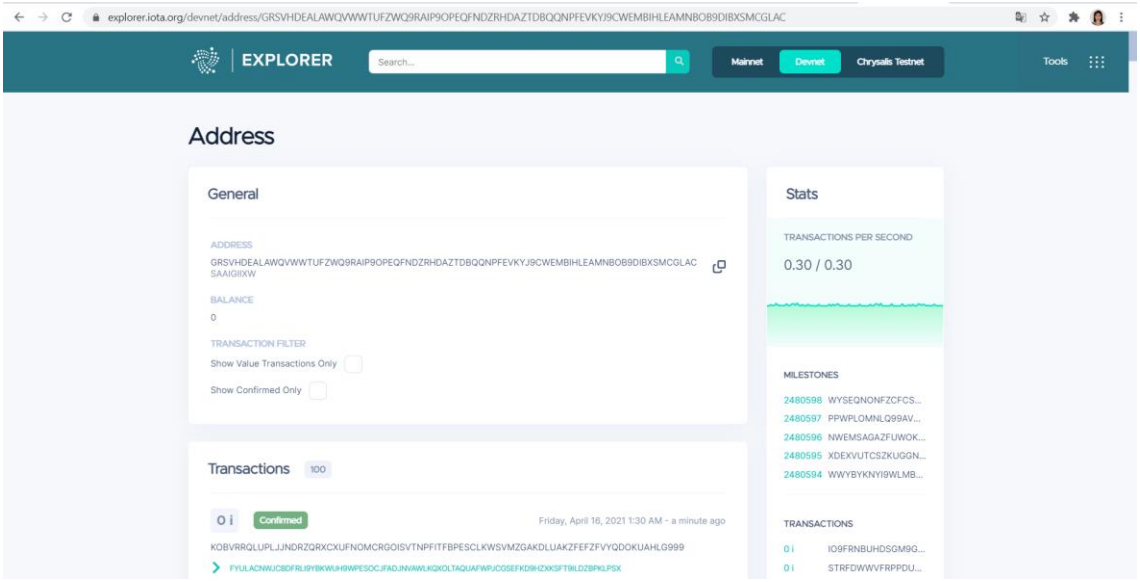


Figura 35. Consulta de todos los votos almacenados en IOTA

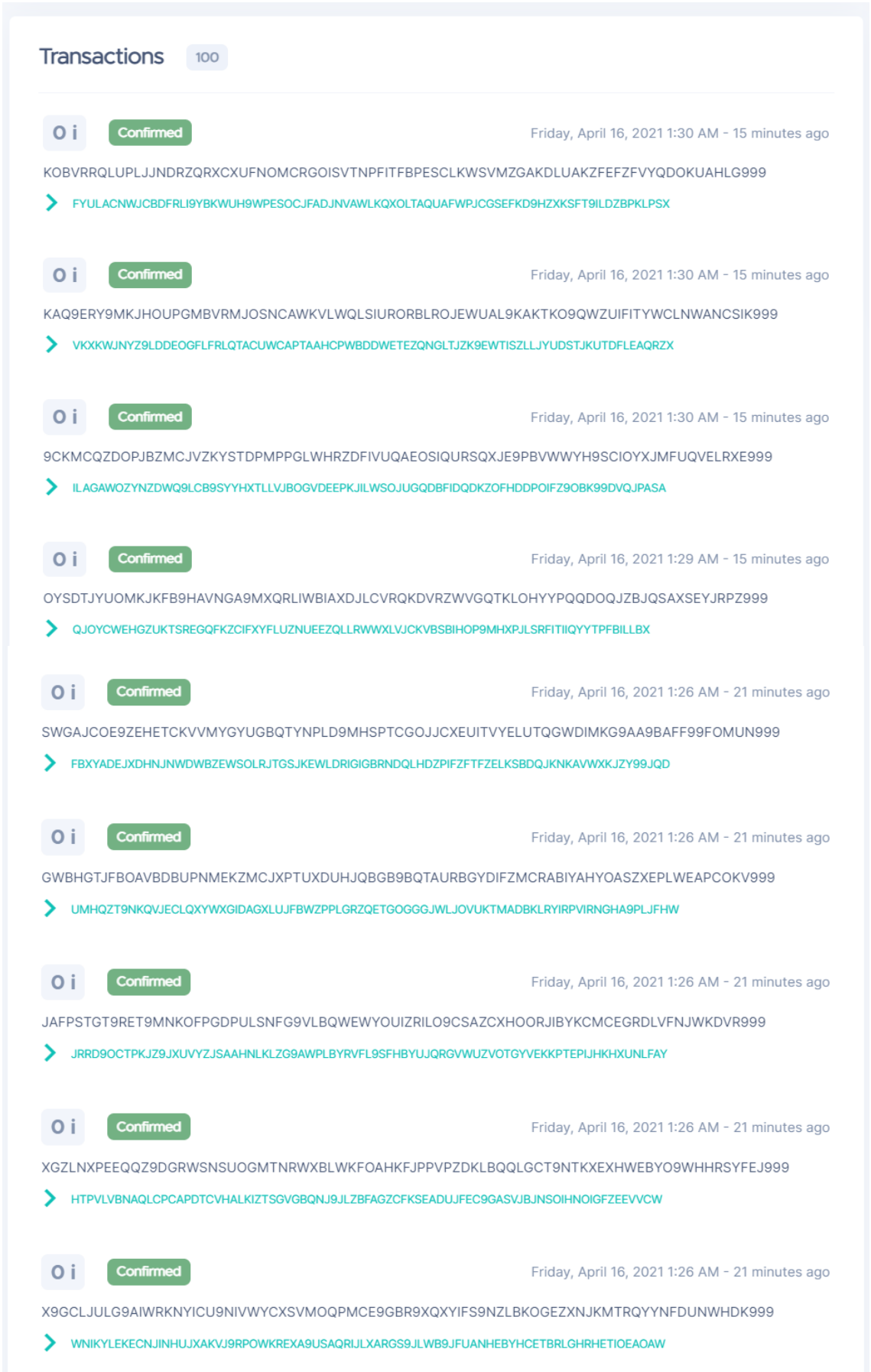


Figura 36. Listado de hashes de los votos registrados en IOTA

3. CAPÍTULO III: EVALUACIÓN DEL PROTOTIPO

3.1. Plan de Evaluación

3.1.1. Plan de Evaluación de Latencia

Para la evaluación de latencia en la comunicación entre Cliente-Servidor-IOTA, se plantea realizar 100 veces el envío de un voto, en donde los tiempos t1, t2, t3 y t4 presentados en la Figura 37, dan un tiempo total de latencia T=t1+t2+t3+t4.

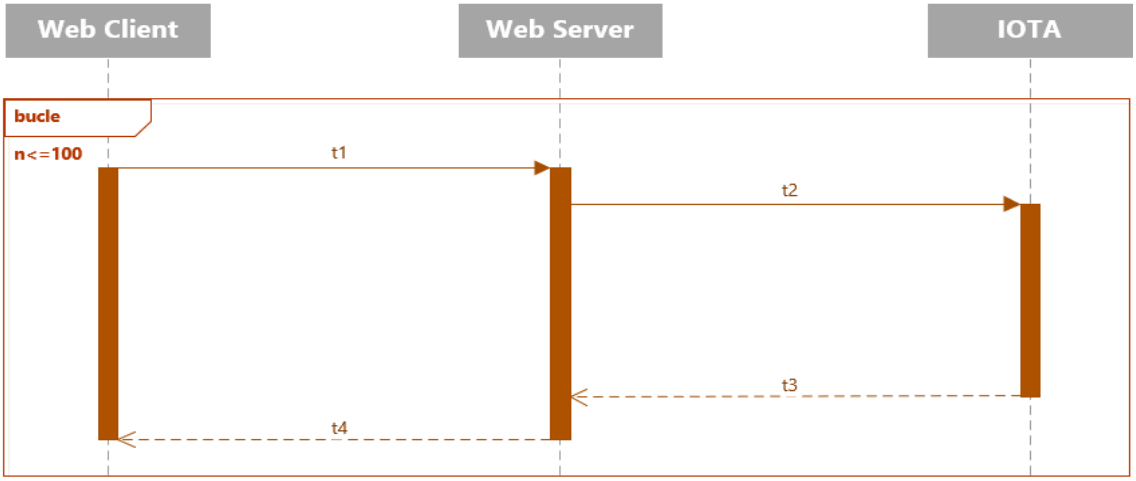


Figura 37. Diagrama de latencia en la comunicación Cliente-Servidor-IOTA

La herramienta seleccionada para la obtención del tiempo total de latencia es el cliente web Postman, el mismo que también ofrece el código de respuesta HTTP de la transacción que retorna como respuesta el hash del voto (Fig. 38).

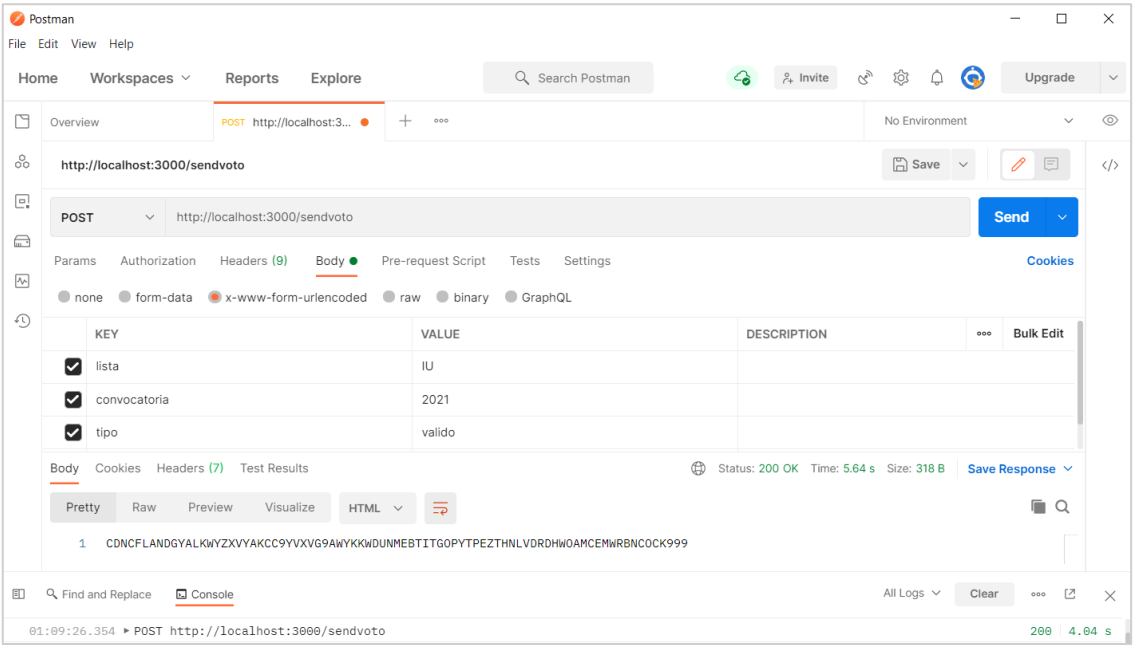


Figura 38. Envío de un voto utilizando el cliente web Postman

3.1.2. Plan de Evaluación de Seguridad

Para la evaluación de seguridad del prototipo desarrollado como propuesta tecnológica en el presente trabajo de titulación, se aspira utilizar tres herramientas online que proveen un análisis gratuito de diferentes factores a considerar en la seguridad de aplicaciones web (Ver Tabla 2).

N°	Herramienta	Link	Descripción
1	SUCURI	**https://sitecheck.sucuri.net/**	Sucuri SiteCheck examinará la URL en busca de malware conocido, software no actualizado, código malicioso o virus, estado de listas negras y errores del sitio web.
2	Qualys	**https://www.ssllabs.com/ssltest/**	Efectúa un análisis profundo de la configuración de cualquier servidor web SSL publicado en internet.
3	Website Vulnerability Scanner	**https://pentest-tools.com/website-vulnerability-scanning/website-scanner#**	Website Vulnerability Scanner realiza un análisis de seguridad web de forma pasiva, lo cual le permite detectar: problemas de seguridad en encabezados HTTP, software de servidor que puede estar desactualizado y cookies inseguras.

Tabla 2. Herramientas a utilizar en la evaluación de seguridad

3.1.3. Plan de Evaluación de Adaptabilidad

Actualmente el acceso a internet es principalmente a través de dispositivos móviles, por lo tanto, es necesario optimizar el diseño de los sitios web para que funcionen correctamente en los diferentes tamaños de dispositivos con los cuales se puede acceder a sus recursos.

Para la evaluación de adaptabilidad del sitio web desarrollado como parte del sistema de votación electrónica, se planea utilizar la herramienta Mobile Friendly Tester de Google disponible en https://search.google.com/test/mobile-friendly, con la cual se comprobará la facilidad que tiene el prototipo para adaptarse a un dispositivo móvil.

3.1.4. Plan de Evaluación de la Calidad en Uso

Se evaluará la calidad en uso de acuerdo a la norma ISO/IEC 25022:2016 [79], con la finalidad de medir el grado en que el sistema de votación propuesto satisface las necesidades de los usuarios. Esta norma evalúa la calidad en uso de acuerdo a cinco características (Ver Fig. 39), cada una de las cuales presenta subcaracterísticas con sus respectivas métricas aplicables a cualquier tipo de sistema.

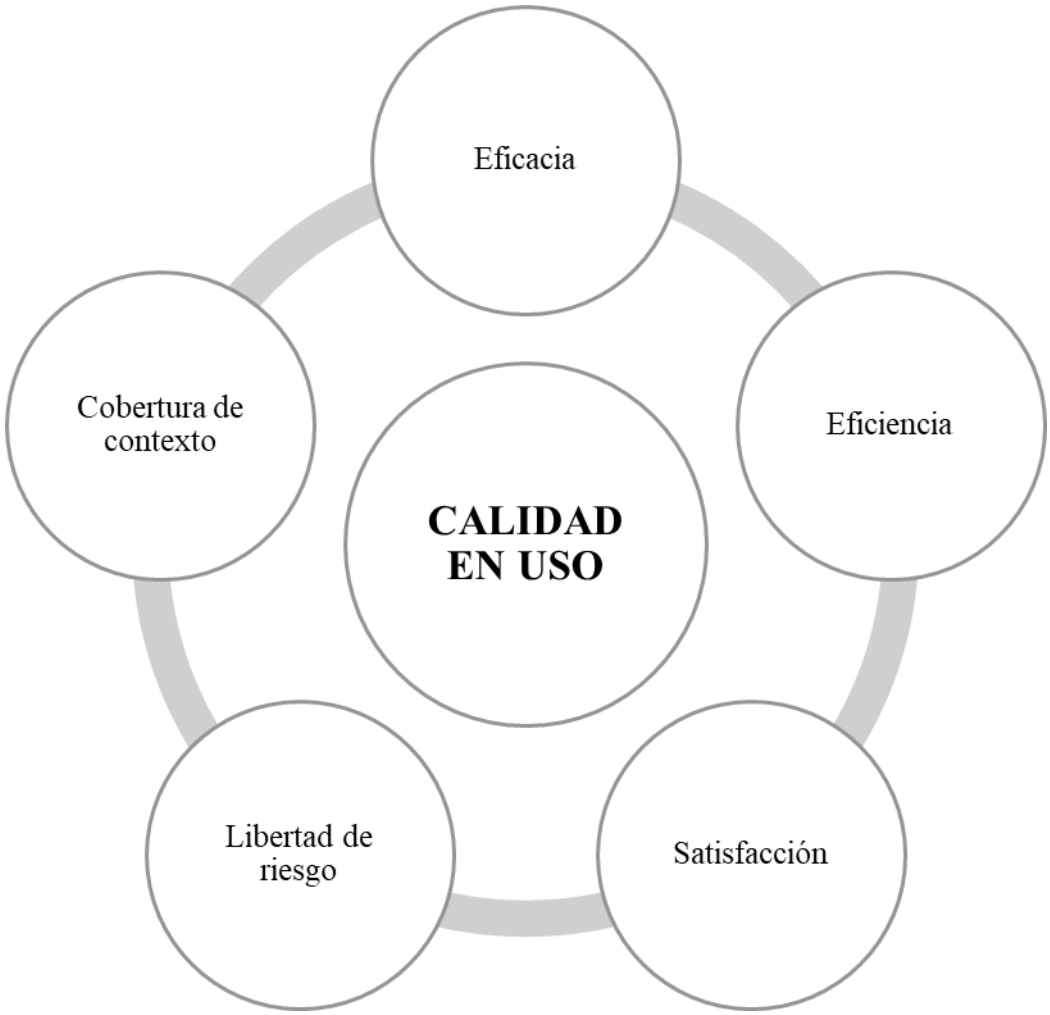


Figura 39. Características de la Calidad en Uso

A continuación, se presenta una descripción de las características de calidad en uso y se detalla las subcaracterísticas, métricas y preguntas para encuestar a los usuarios del sistema de votación, luego de haber realizado una prueba de funcionamiento simulando la elección de representantes estudiantiles en la Escuela de Informática de la UTMACH.

3.1.4.1. Eficacia

Es la capacidad del sistema de votación que permite a los usuarios finales lograr sus objetivos específicos con precisión e integridad para completar las tareas correctamente.

Subcaracterística	Métrica	Preguntas
Completitud Grado con que el sistema de votación provee las funcionalidades necesarias para que el usuario final complete las tareas de forma correcta y sin ayuda.	Tareas completadas	1. ¿Logró autenticarse y votar? 2. ¿Pudo visualizar la convocatoria, padrón electoral, candidaturas y los resultados de la votación en el sitio web informativo?
Corrección Capacidad del sistema de votación para suministrar resultados a los usuarios finales con precisión y exactitud, sin errores.	Informe de errores en las tareas	3. ¿El sistema de votación le informa sobre el ingreso de información inconsistente o errónea?
Pertinencia Capacidad del sistema de votación para proveer un conjunto adecuado de funciones para el desarrollo de las tareas de los usuarios finales.	Funciones adecuadas	4. ¿El sistema de votación presenta las funcionalidades necesarias para la elección de representantes estudiantiles en la Escuela de Informática?

Tabla 3. Plan de evaluación de la calidad en uso con métricas de eficacia

3.1.4.2. Eficiencia

Representa el desempeño del sistema de votación en función del tiempo y la cantidad de recursos utilizados para cumplir su propósito.

Subcaracterística	Métrica	Preguntas
Comportamiento Temporal Tiempo de respuesta, procesamiento y rendimiento del sistema de votación para realizar una tarea.	Tiempo de la tarea	5. ¿El sistema de votación procesa de forma rápida todas las órdenes que usted como usuario final ejecuta para realizar una tarea?
Utilización de Recursos Recursos necesarios para realizar una tarea	Recurso disponible	6. ¿Ha podido ejercer el derecho al voto haciendo uso de un dispositivo electrónico y conexión a internet que ya tenía disponible?

Tabla 4. Plan de evaluación de la calidad en uso con métricas de eficiencia

3.1.4.3. Satisfacción

El grado en que se satisfacen las necesidades de los usuarios finales cuando utilizan el sistema de votación en un contexto específico de uso para cumplir con sus objetivos.

Subcaracterística	Métrica	Preguntas
Utilidad Grado en que el usuario final se siente satisfecho respecto al cumplimiento de una tarea u objetivo específico en el sistema de votación.	Satisfacción general	7. ¿Se siente satisfecho con el sistema de votación electrónica?
	Satisfacción con las características o funciones	8. ¿Siente satisfacción con la funcionalidad del módulo de votación? 9. ¿Siente satisfacción con la información presentada en el sitio web?
Confianza Grado en que el usuario final confía en que el sistema de votación se comportará según lo previsto.	Confianza del usuario	10. ¿Siente confianza al registrar su voto en la aplicación web y navegar por el sitio web?
Complacencia Grado en que el sistema de votación satisface las necesidades del usuario en comparación con otros sistemas.	Complacencia del usuario	11. ¿Considera que el sistema de votación electrónica es mejor que la votación en papel y otros sistemas de votación?
	Acciones innecesarias	12. ¿El sistema de votación no presenta, imágenes, formularios o botones innecesarios?
Comodidad Grado en que el sistema de votación satisface las necesidades de comodidad para operarlo y controlarlo fácilmente.	Comodidad para ser usado	13. ¿Considera que usted maneja con facilidad el sistema de votación?

Tabla 5. Plan de evaluación de la calidad en uso con métricas de satisfacción

3.1.4.4. Libertad de riesgo

El grado en que el sistema de votación presenta medidas de protección para mitigar o evitar riesgos potenciales para el usuario final o la empresa que adquiere el software.

Subcaracterística	Métrica	Preguntas
Mitigación de riesgos para la salud y la seguridad (MRSS) Capacidad del sistema de votación para mitigar los riesgos de salud y seguridad para los usuarios finales.	Medidas para mitigar el impacto en la salud y seguridad del usuario	14. ¿Los colores del sistema de votación son agradables a la vista? 15. ¿El tamaño del texto en sistema de votación es el adecuado, lo que permite que no fuerce la vista? 16. ¿El sistema de votación ofrece un sistema de autenticación seguro? 17. ¿El sistema de votación le ofrece información útil y recomendaciones para el desarrollo de operaciones que requieren un alto nivel de seguridad?

Tabla 6. Plan de evaluación de la calidad en uso con métricas de libertad de riesgo

3.1.4.5. Cobertura de contexto

Es el grado en que el sistema de votación es utilizado con eficacia, eficiencia, satisfacción y libertad de riesgo en diversos contextos de uso y más allá de los que se han expresado al inicio.

Subcaracterística	Métrica	Preguntas
Compleción del contexto Capacidad del sistema de votación para alcanzar los objetivos específicos en diversos contextos de uso.	Integridad del contexto de uso	18. ¿Los niveles de usabilidad presentes en el sistema de votación son aceptables?
Flexibilidad Grado en que un producto o sistema se utiliza en diferentes contextos.	Flexibilidad en el contexto de uso	19. ¿El sistema de votación se adapta de forma eficiente a cualquier tipo de navegador y dispositivo?
	Independencia del dominio	20. ¿El sistema de votación permite que usted como usuario aprenda rápidamente sobre su uso?

Tabla 7. Plan de evaluación de la calidad en uso con métricas de cobertura de contexto

ESCALA DE LIKERT

Cada pregunta de la encuesta será puntuada mediante una escala de Likert del 1 al 5, de acuerdo con el método de valoración de calidad en uso para software web propuesto en [80]. Donde la opción de respuesta "Totalmente en Desacuerdo" será calificada con 1 punto mientras que la opción de respuesta "Totalmente de Acuerdo" será valorada con 5 puntos (Ver Tabla 8).

Opción de respuesta	Abreviatura	Puntuación
Totalmente en Desacuerdo	TD	1
En Desacuerdo	ED	2
Neutral	N	3
De Acuerdo	DA	4
Totalmente de Acuerdo	TA	5

Tabla 8. Escala de Likert para la Evaluación de Calidad en Uso

3.2. Resultados de la Evaluación

3.2.1. Evaluación de Latencia

3.2.1.1. Votación

La latencia de la votación con 100 pruebas de envío de votos y retorno del hash almacenado en IOTA dio como resultado la serie de tiempo en milisegundos que se presenta en la Figura 40; siendo importante destacar que todas las transacciones se ejecutaron correctamente, dando un código 200 como respuesta HTTP.

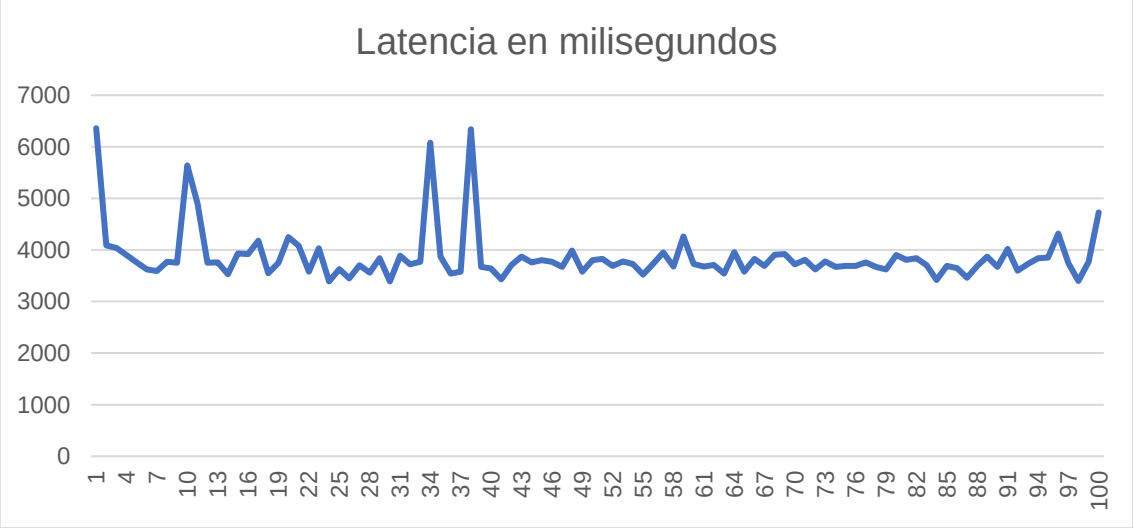


Figura 40. Latencia en milisegundos del proceso de votación con 100 muestras

Ordenando los datos de menor a mayor se obtiene la distribución que se presenta en la Figura 41, donde se puede apreciar que la mayoría de veces dio como resultado una latencia menor a 4 segundos.

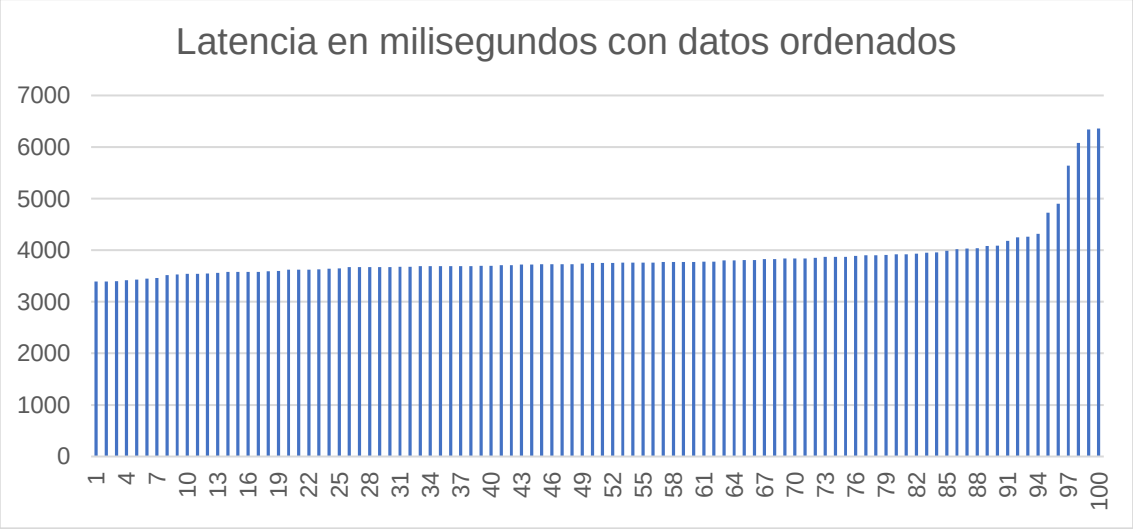


Figura 41. Latencia en milisegundos del proceso de votación con datos ordenados

El análisis descriptivo de los datos refleja que el mínimo tiempo de latencia en el proceso de votación es de 3390 milisegundos, mientras que el valor máximo es de 6360 milisegundos, la media es de 3857,48 milisegundos, la mediana es de 3750, el valor más repetido o moda es 3690 milisegundos, y la desviación estándar es 514,75 (Tabla 9).

ESTADÍSTICA DESCRIPTIVA	
N° datos	100
Mínimo	3390
Máximo	6360
Media	3857,48
Mediana	3750
Moda	3690
Desviación estándar	514,75

Tabla 9. Estadística descriptiva de latencia en la votación

El histograma de los datos consta de 8 clases con un rango de 2970 milisegundos, por lo tanto, el tamaño de clase es de 371.25.

	Frecuencia	*% acumulado*		*Frecuencia*	*% acumulado*
3761,25	56	56,00%	3761,25	56	56,00%
4132,5	34	90,00%	4132,5	34	90,00%
4503,75	4	94,00%	4503,75	4	94,00%
4875	1	95,00%	6360	3	97,00%
5246,25	1	96,00%	4875	1	98,00%
5617,5	0	96,00%	5246,25	1	99,00%
5988,75	1	97,00%	5988,75	1	100,00%
6360	3	100,00%	5617,5	0	100,00%

Tabla 10. Tabla de frecuencias del tiempo de latencia en la votación

En el histograma se observa que los tiempos de latencia se concentran mayoritariamente en las dos primeras clases, el 90% de las transacciones de votación es menor a 4503,75.

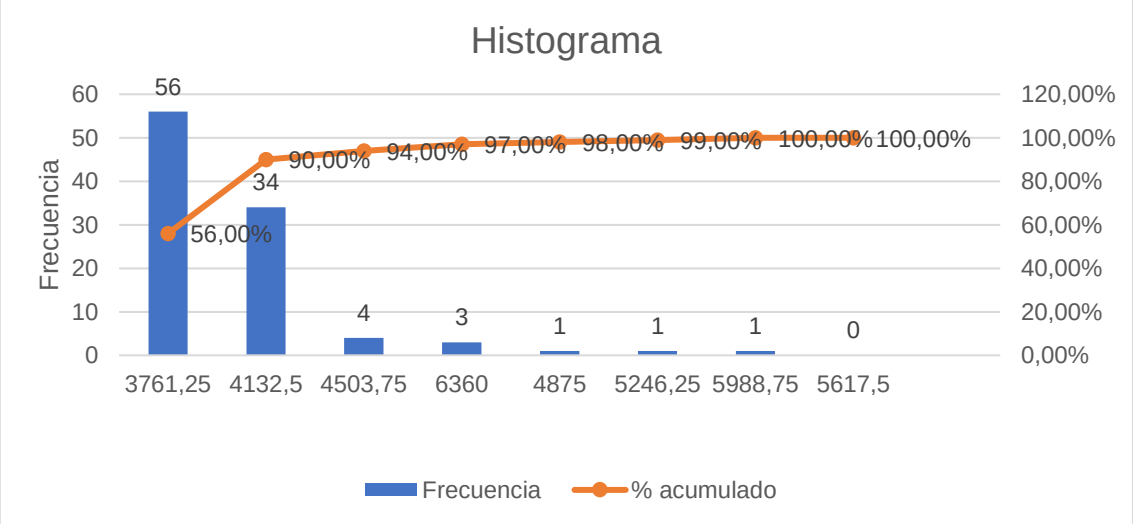


Figura 42. Histograma de latencia en la votación

3.2.1.2. Escrutinio

La latencia del proceso de escrutinio de 100 votos, dio como resultado la serie de tiempo en milisegundos que se presenta en la Figura 43, en donde se presenta el tiempo individual de realizar el cálculo de escrutinio 100 veces, resultando todas las transacciones con un código 200 como respuesta HTTP.

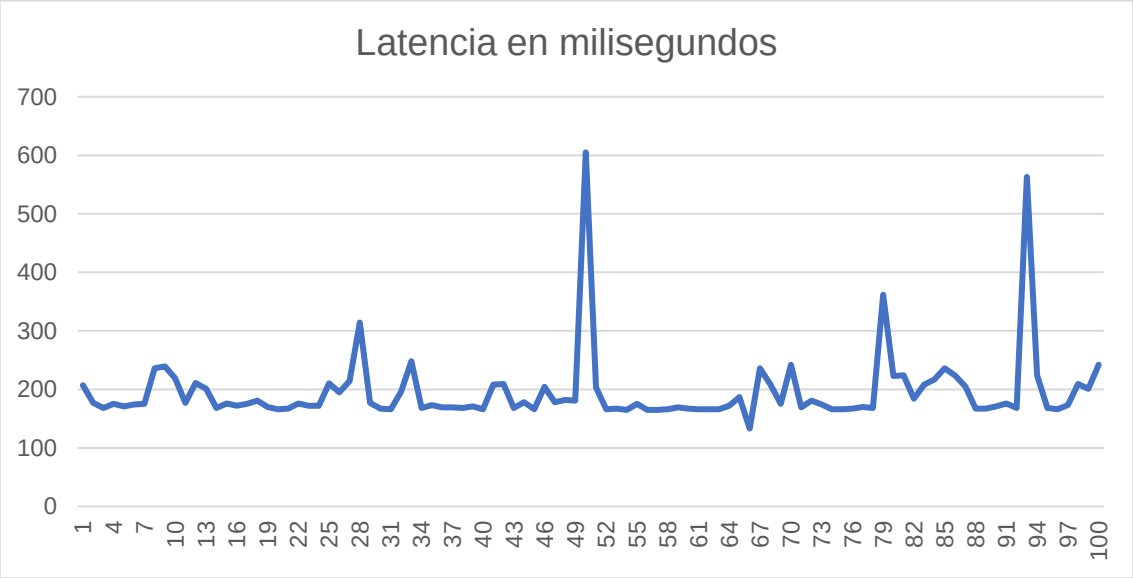


Figura 43. Latencia en milisegundos del proceso de escrutinio con 100 muestras

Ordenando los datos de menor a mayor se obtiene la distribución que se presenta en la Figura 44, donde se puede apreciar que aproximadamente el 70% de pruebas dio como resultado una latencia menor a 200 milisegundos.

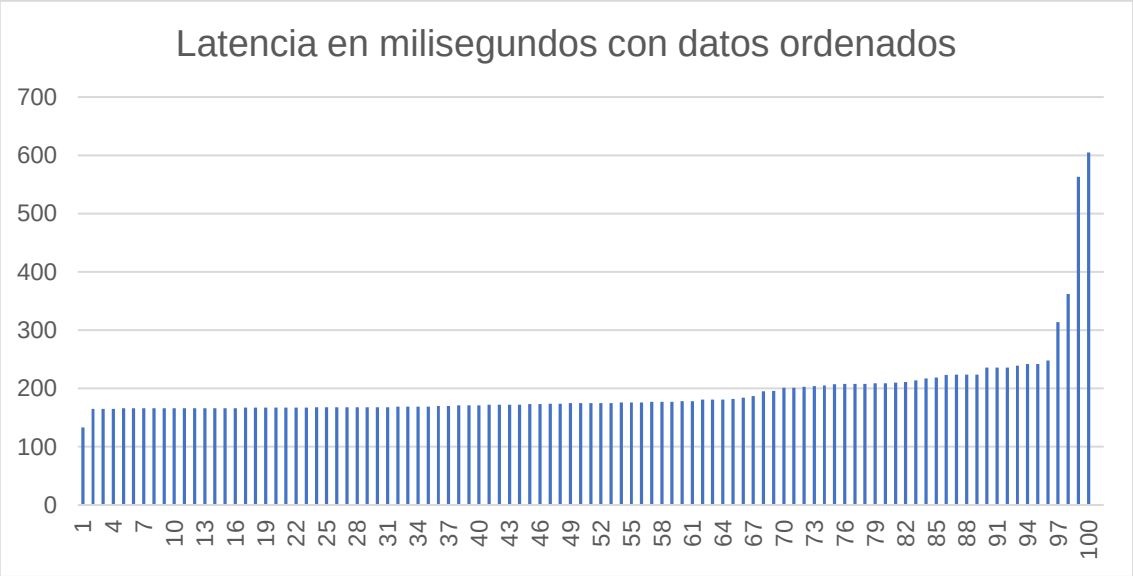


Figura 44. Latencia en milisegundos del proceso de escrutinio con datos ordenados

El análisis descriptivo de los datos refleja que el mínimo tiempo de latencia en el proceso de escrutinio es de 133 milisegundos, mientras que el valor máximo es de 605 milisegundos, la media es de 195,73 milisegundos, la mediana es de 175, el valor más repetido o moda es 166 milisegundos, y la desviación estándar es 64,31 (Tabla 11).

ESTADÍSTICA DESCRIPTIVA	
N° datos	100
Mínimo	133
Máximo	605
Media	195,73
Mediana	175
Moda	166
Desviación estándar	64,31

Tabla 11. Estadística descriptiva de latencia en la votación

El histograma de los datos agrupados consta de 8 clases con un rango de 472 milisegundos, por lo tanto, el tamaño de clase es de 59.

	Frecuencia	*% acumulado*		*Frecuencia*	*% acumulado*
192	67	67,00%	192	67	67,00%
251	29	96,00%	251	29	96,00%
310	0	96,00%	369	2	98,00%
369	2	98,00%	605	2	100,00%
428	0	98,00%	310	0	100,00%
487	0	98,00%	428	0	100,00%
546	0	98,00%	487	0	100,00%
605	2	100,00%	546	0	100,00%

Tabla 12. Tabla de frecuencias del tiempo de latencia en el proceso de escrutinio

En el histograma presentado en la Figura 45, se observa que los tiempos de latencia se concentran mayoritariamente en las dos primeras clases, en las cuales suma el 96%.

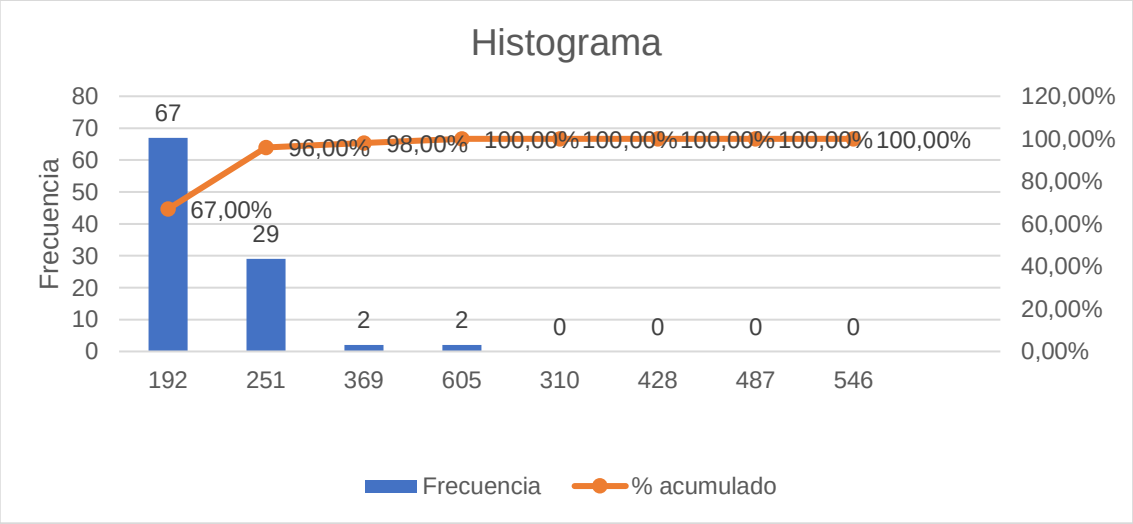


Figura 45. Histograma de latencia en el proceso de escrutinio

3.2.2. Evaluación de Seguridad

La evaluación de seguridad realizada con la herramienta SUCURI SiteCheck, reporta que no se ha encontrado ningún malware dentro del sitio web, tampoco se lo ha encontrado en listas negras. La única recomendación obtenida es redireccionar de HTTP a HTTPS para evitar avisos de seguridad por parte de los navegadores, por lo que esta herramienta informa que el riesgo de seguridad es medio (Fig. 46).

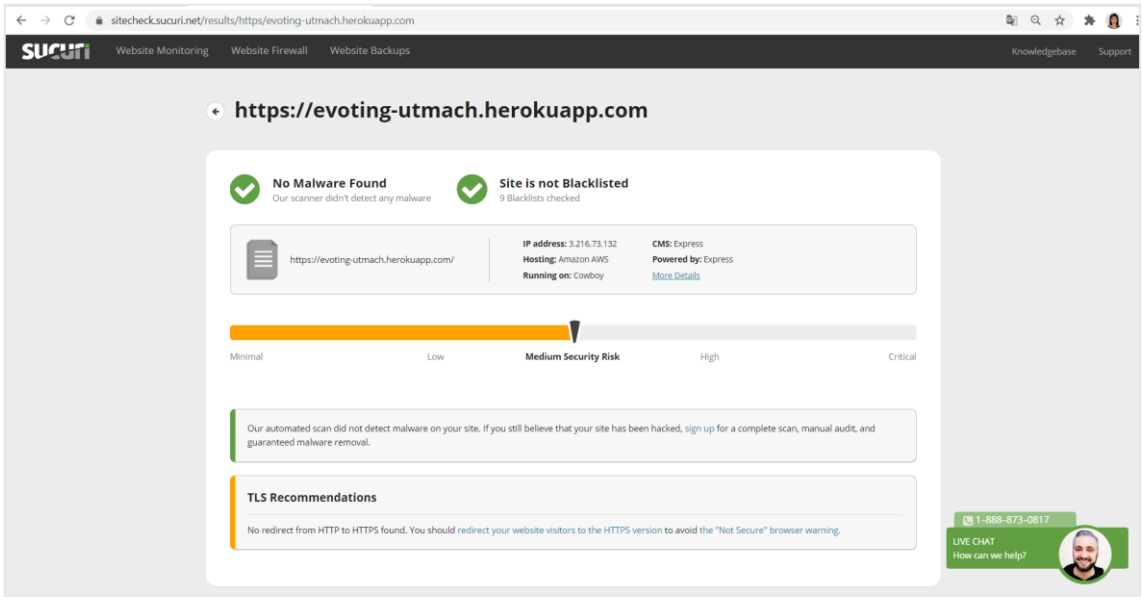


Figura 46. Evaluación de seguridad con la herramienta SUCURI

Con la herramienta Qualys se analizó la seguridad SSL (Secure Socket Layer) de los servidores en donde se encuentra alojada la aplicación web de votación electrónica, dando como resultado un grado B (Fig. 47).

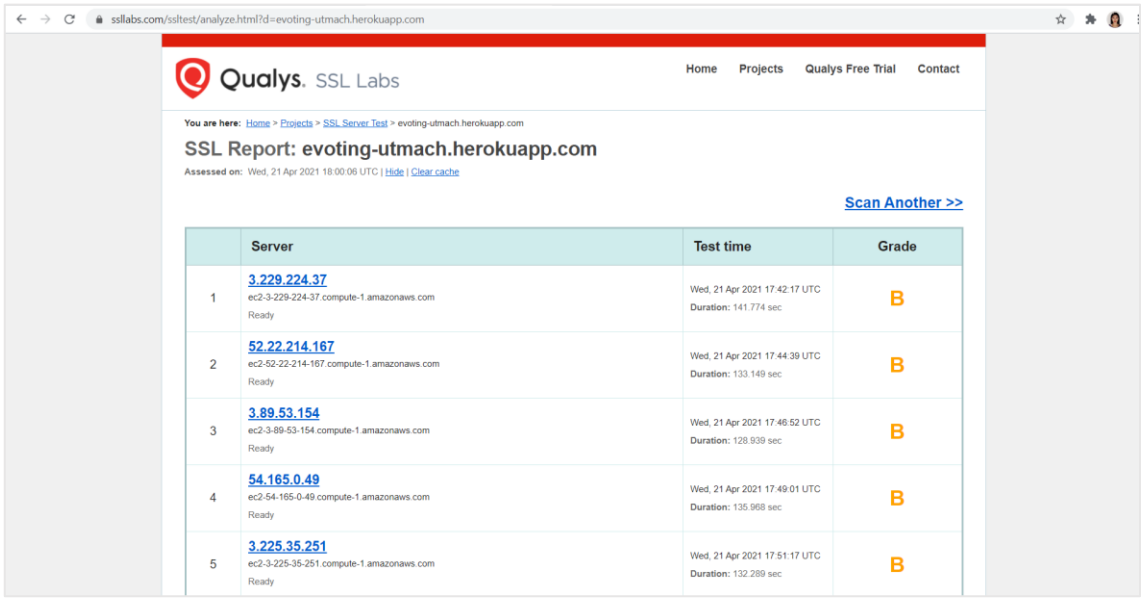


Figura 47. Evaluación de seguridad con la herramienta Qualys

La herramienta Website Vulnerability Scanner del sitio web Pentest-Tools, examinó un total de 17 aspectos de seguridad de los cuales 6 reportaron un riesgo bajo mientras que los otros 11 presentaron un estado óptimo de seguridad (Ver Figs. 48, 49, 50).

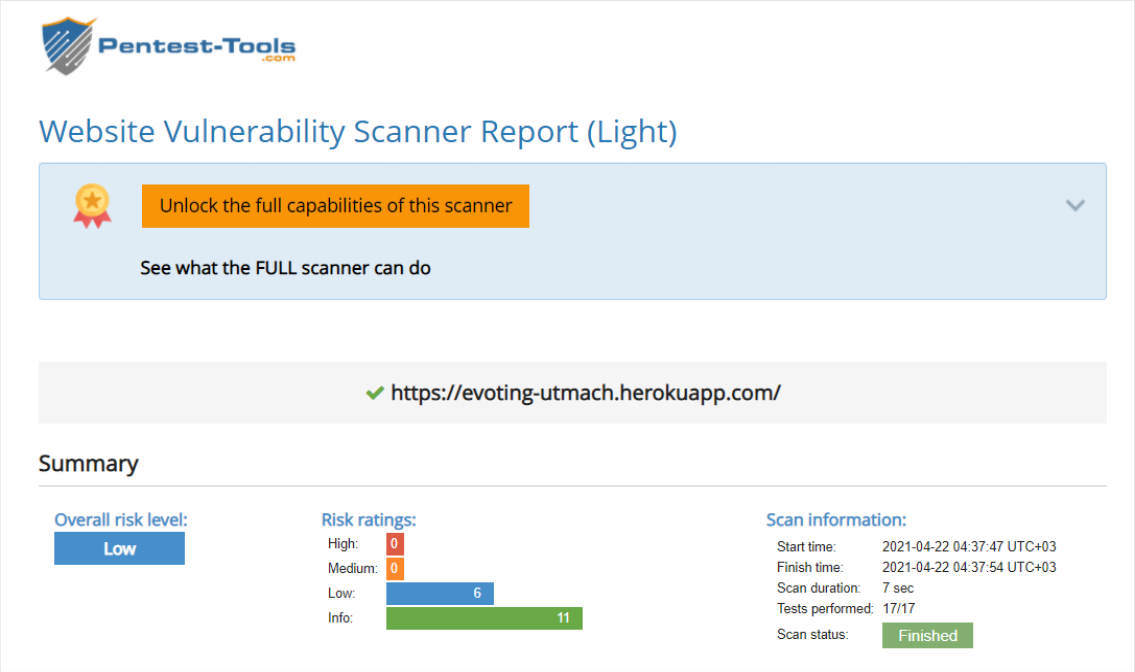


Figura 48. Evaluación de seguridad con Website Vulnerability Scanner

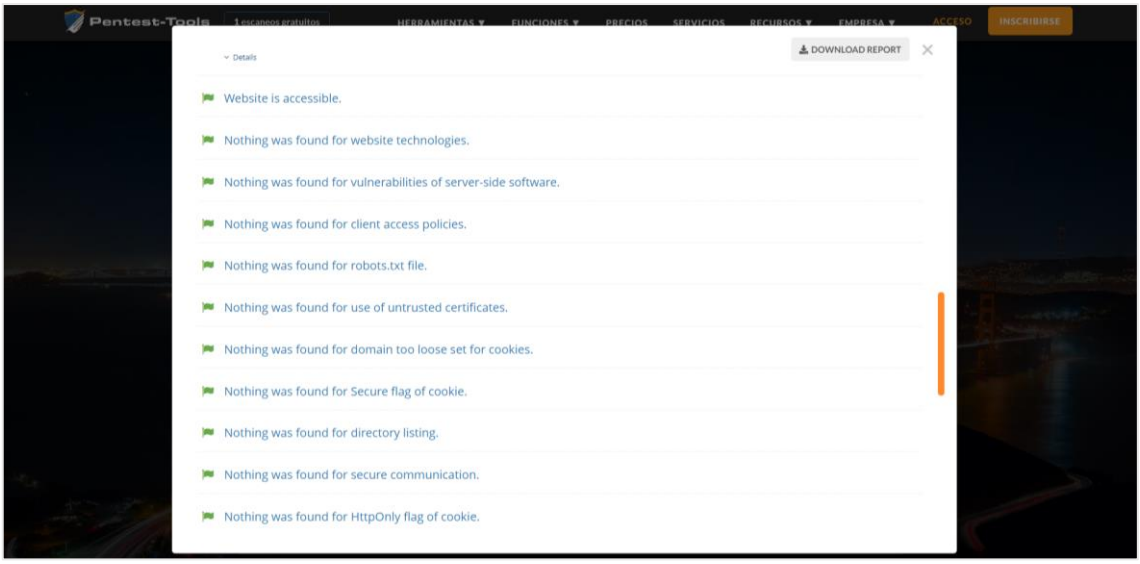


Figura 49. Aspectos del sitio web reportados como seguros por pentest-tools.com

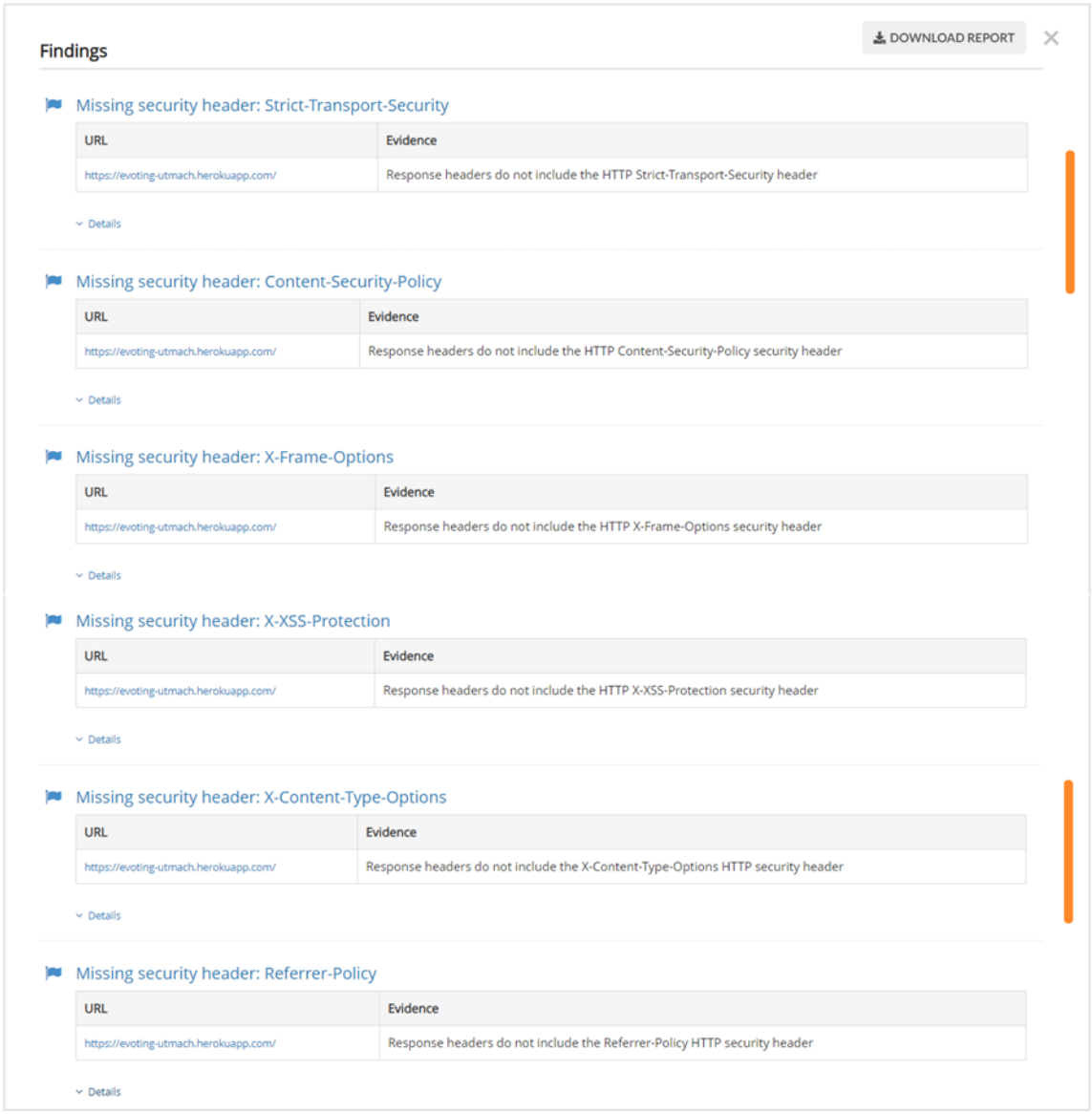


Figura 50. Recomendaciones de seguridad realizadas por pentest-tools.com

3.2.3. Evaluación de Adaptabilidad

La evaluación de adaptabilidad realizada con la herramienta Mobile Friendly Tester de Google, dio como resultado que la página está optimizada para móviles, por lo que es fácil usarla en dispositivos como smartphones y tablets (Ver Figs. 51, 52).

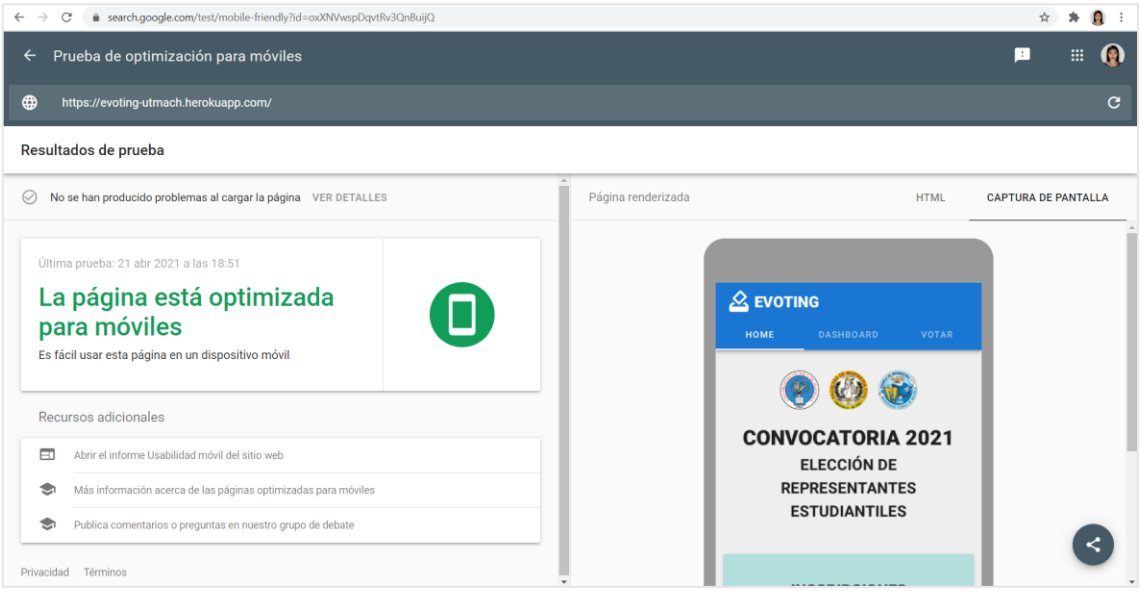


Figura 51. Evaluación de adaptabilidad con la herramienta Mobile Friendly Tester

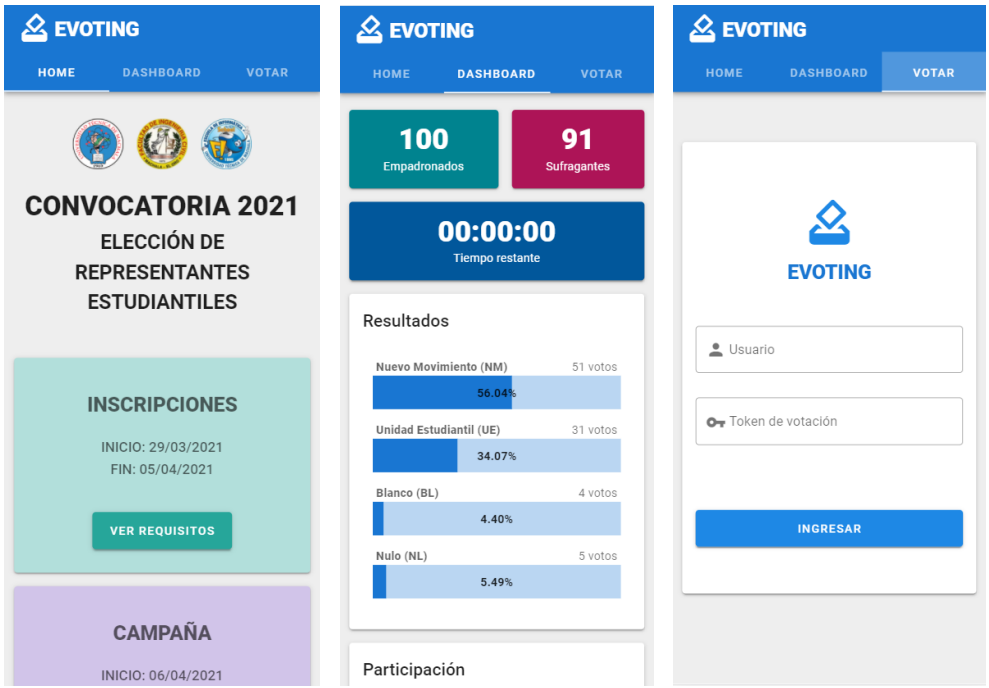


Figura 52. Capturas de pantalla del sitio web en un dispositivo móvil

3.2.4. Evaluación de la Calidad en Uso

Característica	Subcaracterística	Métrica	Preguntas	TD	ED	N	DA	TA	Total	Porcentaje	Resultado
				1	2	3	4	5			
Eficacia	Completitud	Tareas completadas	P-1	1	0	2	10	86	477	95,4%	95,67%
			P-2	1	0	5	7	87	479	95,8%	
	Corrección	Informe de errores en las tareas	P-3	1	1	9	3	86	472	94,4%	
	Pertinencia	Funciones adecuadas	P-4	0	0	3	9	88	485	97,0%	
Eficiencia	Comportamiento Temporal	Tiempo de la tarea	P-5	1	5	10	26	58	435	87,0%	92,60%
	Utilización de Recursos	Recurso disponible	P-6	0	0	0	9	91	491	98,2%	
Satisfacción	Utilidad	Satisfacción general	P-7	1	1	6	9	83	472	94,4%	94,80%
		Satisfacción con las características o funciones	P-8	1	1	4	8	86	477	95,4%	
			P-9	0	0	1	5	94	493	98,6%	
	Confianza	Confianza del usuario	P-10	0	1	7	4	88	479	95,8%	
	Complacencia	Complacencia del usuario	P-11	1	0	0	36	63	460	92,0%	
		Acciones innecesarias	P-12	1	0	5	25	69	461	92,2%	
	Comodidad	Comodidad para ser usado	P-13	1	0	3	12	84	478	95,6%	
Libertad de riesgo	MRSS	Medidas para mitigar el impacto en la salud y seguridad del usuario	P-14	1	1	15	25	58	438	87,6%	86,05%
			P-15	1	1	17	8	73	451	90,2%	
			P-16	2	2	16	6	74	448	89,6%	
			P-17	3	4	28	36	29	384	76,8%	
Cobertura de contexto	Compleción del contexto	Integridad del contexto de uso	P-18	1	1	23	35	40	412	82,4%	88,45%
	Flexibilidad	Flexibilidad en el contexto de uso	P-19	1	1	12	9	77	460	92,0%	
		Independencia del dominio	P-20	0	1	2	8	89	485	97,0%	

Tabla 13. Resultados de la Evaluación de la Calidad en Uso

El resultado obtenido para las características de calidad en uso se realizó promediando el puntaje de las preguntas pertenecientes a cada una de sus métricas. Estos porcentajes serán valorados de acuerdo a la escala de evaluación presentada en la Tabla 14.

Escala	Valor
Excelente	81-100%
Sobresaliente	61-80%
Aceptable	41-60%
Insuficiente	21-40%
Deficiente	0-20%

Tabla 14. Escala de evaluación

Según los porcentajes obtenidos en las características de calidad en uso, el sistema propuesto para la votación electrónica en la Escuela de Informática es excelente para el propósito planteado.

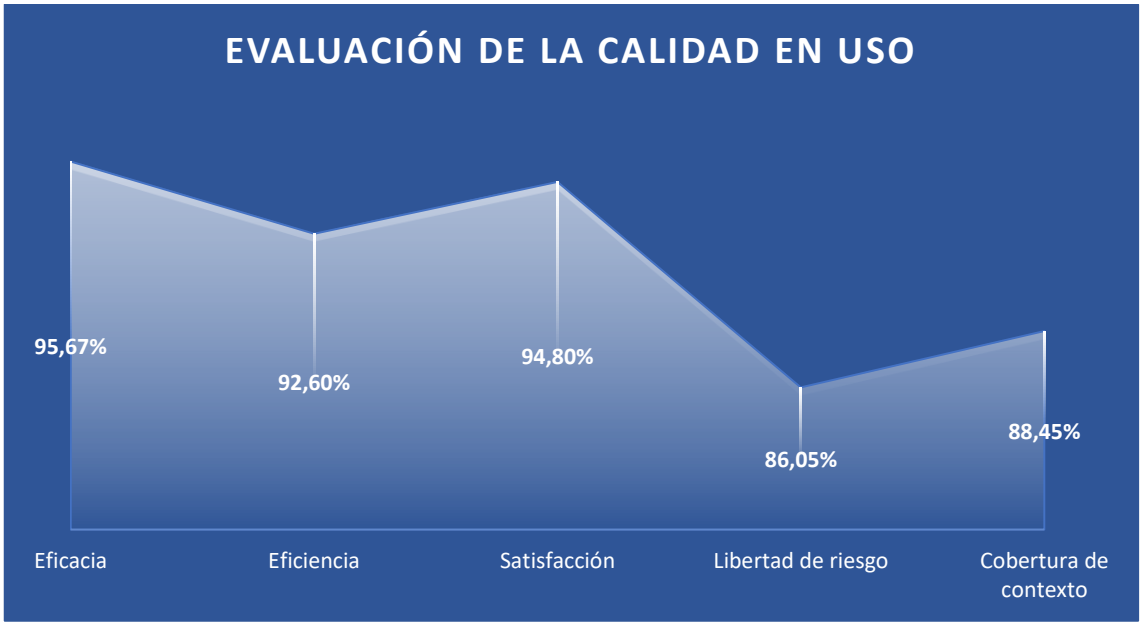


Figura 53. Resultados de la Evaluación de la Calidad en Uso

3.3. CONCLUSIONES

La presente propuesta tecnológica consiste en un sistema de votación electrónica, que se desarrolló utilizando la tecnología de contabilidad distribuida IOTA, con la finalidad de automatizar el proceso de elección de representantes estudiantiles en la Escuela de Informática de la UTMACH. Se propone un sistema respaldado por tecnología, matemática y criptografía, donde los resultados son verificables y mediante un sitio web informativo se gestiona transparentemente la información entorno a las votaciones, por lo cual la evaluación de calidad en uso refleja un alto grado de eficacia, eficiencia y satisfacción.

El análisis comparativo de diferentes plataformas DLT permitió seleccionar la tecnología de contabilidad distribuida IOTA, porque se adapta a los requerimientos del sistema de votación electrónica desarrollado en la presente propuesta tecnológica por su capacidad de transacciones gratuitas y bajo consumo de energía, además de ser de acceso público y *Open Source*.

El sistema desarrollado genera automáticamente el padrón electoral mediante una conexión con la base de datos institucional (simulada en la etapa de prueba), de esta forma se logró incorporar en el padrón electoral únicamente los estudiantes legalmente matriculados en las carreras de la Escuela de Informática de la UTMACH para el periodo académico en el que se realizan las votaciones.

Para la autenticación de los usuarios en el presente sistema de votación electrónica se utilizó JSON Web Token, el cual es un estándar para cifrar la información transmitida en un entorno cliente-servidor, esto permite que solo los estudiantes correctamente autenticados puedan ingresar al módulo de votación y emitir su voto.

El sistema de votación propuesto tiene una interfaz gráfica agradable al usuario y se adapta a los diferentes tamaños de pantalla de los dispositivos electrónicos, como tablets, smartphones, laptops y computadoras de escritorio. Esta característica permite que los estudiantes voten desde cualquier lugar, sin necesidad de acudir a un recinto electoral.

3.4. RECOMENDACIONES

Se recomienda implementar el sistema propuesto para la elección de representantes estudiantiles de la Escuela de Informática de la UTMACH, dado que cumple los requisitos necesarios para llevar a cabo eficazmente el proceso de votación y cuenta con la confianza de los votantes al brindar la posibilidad de verificar que su voto está correctamente registrado y contabilizado.

Sería interesante analizar el desarrollo de un sistema de votación que abarque los procesos de las elecciones universitarias generales como las elecciones de Cogobierno de la Universidad Técnica de Machala, y brinde un mayor nivel de confiabilidad en el proceso electoral, mediante la implementación de tecnologías de contabilidad distribuida, para el almacenamiento seguro de la información.

Para aplicar un sistema de votación electrónica a gran escala se recomienda realizar una capacitación detallada sobre el uso del sistema, ya que se puede contar con usuarios poco familiarizados con el manejo de aplicaciones web y de la tecnología en general, lo cual puede ocasionar que los votantes presenten dificultades al momento de registrar el voto.

En el prototipo desarrollado se utiliza una DLT pública con la cual se demostró la utilidad de la tecnología IOTA, para el almacenamiento seguro de la información en una red distribuida; pero caso de requerir una red privada o federada es recomendable analizar la posibilidad de vincular a varias universidades interesadas en aprovechar los beneficios de un almacenamiento distribuido y seguro, para lo cual cada institución debería contar con un servidor que se convertiría en un nodo verificador. En este tipo de red, cada uno de los nodos se caracteriza por ser conocido y confiable.

Muchos sistemas informáticos y almacenamiento de datos son accedidos por personas no autorizadas, debido a la falta de calidad de autenticación que posee el sistema [81]. Por tal motivo, se recomienda utilizar autenticación de múltiple factor incorporando sistemas biométricos como identificación de huella dactilar y reconocimiento facial, o asignando una credencial física con un código QR único para cada estudiante, con la finalidad de reducir las posibilidades de fraude o suplantación de identidad.

4. BIBLIOGRAFÍA

[1] A. Pinna, G. Baralla, G. Lallai, M. Marchesi y R. Tonelli, «Design of a Sustainable Blockchain-Oriented Software for Building Workers Management,» *Frontiers in Blockchain,* vol. 3, nº 38, pp. 1-19, Octubre 2020.

[2] Red Hat, «Qué son las API y para qué sirven,» [En línea]. Available: https://www.redhat.com/es/topics/api/what-are-application-programming-interfaces. [Último acceso: 16 Abril 2021].

[3] M. Szydlo, «Merkle Tree Traversal in Log Space and Time,» *Advances in Cryptology - EUROCRYPT 2004,* vol. 3027, p. 541–554, 2004.

[4] E. Zaghloul, T. Li, M. W. Mutka y J. Ren, «Bitcoin and Blockchain: Security and Privacy,» *IEEE Internet of Things Journal,* vol. 7, nº 10, Junio 2020.

[5] Y. Marrero Travieso, «La Criptografía como elemento de la seguridad informática,» *ACIMED,* vol. 11, nº 6, 2003.

[6] I. A. Qasse, J. Spillner, M. A. Talib y Q. Nasir, «A Study on ĐApps Characteristics,» *2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS),* nº 20053668, Agosto 2020.

[7] N. Živi, E. Kadušić y K. Kadušić, «Directed Acyclic Graph as Tangle: an IoT Alternative to Blockchains,» *2019 27th Telecommunications Forum (TELFOR),* nº 19315888, 2019.

[8] S. T.-p. T. E. f. E. Assumptions, «Secure Two-party Threshold ECDSA from ECDSA Assumptions,» *2018 IEEE Symposium on Security and Privacy (SP),* Julio 2018.

[9] Kaspersky, «¿Qué Es Un Hash Y Cómo Funciona?,» [En línea]. Available: https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/. [Último acceso: 19 Enero 2021].

[10] MDN, «HTTP,» Mozilla, [En línea]. Available: https://developer.mozilla.org/es/docs/Web/HTTP. [Último acceso: 19 Enero 2021].

[11] IOTA Foundation, «IOTA,» [En línea]. Available: https://www.iota.org/get-started/what-is-iota. [Último acceso: 29 Diciembre 2020].

[12] JWT, «Introduction to JSON Web Tokens,» [En línea]. Available: https://jwt.io/introduction. [Último acceso: 29 Marzo 2020].

[13] Y. Sazaki, M. Mulya y M. Arisandi, «The development android-based SMS security software using ECDSA with boolean permutation,» *2016 2nd International Conference on Wireless and Telematics (ICWT),* nº 16725708, 2019.

[14] IOTA Foundation, «Ternary,» [En línea]. Available: https://docs.iota.org/docs/getting-started/0.1/introduction/ternary. [Último acceso: 30 Enero 2021].

[15] Object Management Group, «Unified Modeling Language (OMG UML),» ISO/IEC, 2012. [En línea]. Available: https://www.omg.org/spec/UML/ISO/19505-1/PDF. [Último acceso: 25 Enero 2021].

[16] T. Fernández-Navia, E. Polo-Muro y D. Tercero-Lucas, «Too afraid to vote? The effects of COVID-19 on voting behaviour,» *European Journal of Political Economy,* Marzo 2021.

[17] A. Sarker, S. Byun, W. Fan, M. Psarakis y S.-Y. Chang, «Voting Credential Management System for Electronic Voting Privacy,» *2020 IFIP Networking Conference (Networking),* 2020.

[18] C. Satizábal, R. Páez y J. Forné, «Secure Internet Voting Protocol (SIVP): A secure option for electoral processes,» *Journal of King Saud University - Computer and Information Sciences,* Enero 2021.

[19] R. Rezwan, H. Ahmed, M. R. N. Biplob, S. M. Shuvo y M. A. Rahman, «Biometrically secured electronic voting machine,» *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC),* 2017.

[20] E. V. Palekha, I. S. Trubchik, O. N. Manaenkova, O. A. Safaryan, V. M. Porksheyan y S. A. Morozov, «Cross-Platforming Web-Application of Electronic On-line Voting System on the Elections of Any Level,» *2019 IEEE East-West Design & Test Symposium (EWDTS),* pp. 1-4, 2019.

[21] S. Gao, D. Zheng, R. Guo, C. Jing y C. Hu, «An Anti-Quantum E-Voting Protocol in Blockchain With Audit Function,» *IEEE Access,* vol. 7, pp. 115304-115316, 2019.

[22] A. L. S. Aguilar, M. Gutiérrez y L. C. P. Howlet, «Voto electrónico: confiabilidad y utilización de tecnología,» *Investigación y Ciencia: de la Universidad Autónoma de Aguascalientes,* nº 70, pp. 77-83, 2017.

[23] K. a. V. R. a. J. H.-A. Zhang, «Deconstructing Blockchains: Concepts, Systems, and Insights,» *Proceedings of the 12th ACM International Conference on Distributed and Event-Based Systems,* p. 187–190, 2018.

[24] H. Yi, «Securing e-voting based on blockchain in P2P network,» *EURASIP Journal on Wireless Communications and Networking,* nº 137, Mayo 2019.

[25] P. Baudier, G. Kondrateva, C. Ammi y E. Seulliet, «Peace engineering: The contribution of blockchain systems to the e-voting process,» *Technological Forecasting and Social Change,* vol. 162, Enero 2021.

[26] S. T. Alvi, M. N. Uddin y L. Islam, «Digital Voting: A Blockchain-based E-Voting System using Biohash and Smart Contract,» *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT),* Octubre 2020.

[27] B. Wang, J. Sun, Y. He, D. Pang y N. Lu, «Large-scale Election Based On Blockchain,» *Procedia Computer Science,* 2018.

[28] M. Bhandary, M. Parmar y D. Ambawade, «A Blockchain Solution based on Directed Acyclic Graph for IoT Data Security using IoTA Tangle,» *2020 5th International Conference on Communication and Electronics Systems (ICCES),* Julio 2020.

[29] D. L. Hernández-Rojas, T. M. Fernández-Caramés, P. Fraga-Lamas y C. J. Escudero, «Design and Practical Evaluation of a Family of Lightweight Protocols for Heterogeneous Sensing through BLE Beacons in IoT Telemetry Applications,» *Sensors,* vol. 18, nº 2, p. 57, 2018.

[30] D. L. Hernández-Rojas, T. M. Fernández-Caramés, P. Fraga-Lamas y C. J. Escudero, «A Plug-and-Play Human-Centered Virtual TEDS Architecture for the Web of Things,» *Sensors,* vol. 18, nº 7, p. 2052, 2018.

[31] B. Mazon-Olivo, D. Hernández-Rojas, J. Maza-Salinas y A. Pan, «Rules engine and complex event processor in the context of internet of things for precision agriculture,» *Computers and Electronics in Agriculture,* vol. 154, pp. 347-360, Noviembre 2018.

[32] UTMACH, «Reglamento de Elecciones y Referendo de la Universidad Técnica de Machala,» [En línea]. Available: https://www.utmachala.edu.ec/archivos/siutmach/documentos/reglamentos/ELECCIONES%20Y%20REFERENDO%20REFORMADO%20SEPT.%20%2024.pdf. [Último acceso: 12 Enero 2021].

[33] N. Faour, «Transparent E-Voting dApp Based on Waves Blockchain and RIDE Language,» *2019 XVI International Symposium "Problems of Redundancy in Information and Control Systems" (REDUNDANCY),* 2019.

[34] H. F. Atlam y G. B. Wills, «Chapter One - Technical aspects of blockchain and IoT,» de *Advances in Computers,* vol. 115, 2019, pp. 1-39.

[35] J. T. P. Chungata, E. R. P. López, O. D. L. Granizo y M. B. Tobar, «Confiabilidad y consideraciones del voto electrónico, una visión global,» *Journal of Science and Research: Revista Ciencia e Investigación,* vol. 2, nº 5, pp. 26-38, 2017.

[36] J.-L. Zhang, J.-Z. Zhang y S.-C. Xie, «A Choreographed Distributed Electronic Voting Scheme,» *International Journal of Theoretical Physics volume,* Junio 2018.

[37] G. Han, Y. Li, Y. Yu, K.-K. R. Choo y N. Guizani, «Blockchain-Based Self-Tallying Voting System with Software Updates in Decentralized IOT,» *IEEE Network,* vol. 4, pp. 166-172, Agosto 2020.

[38] W.-J. Lai y J.-L. Wu, «An efficient and effective Decentralized Anonymous Voting System,» *Cryptography and Security,* Abril 2018.

[39] P. Garcia, «Biometrics on the blockchain,» *Biometric Technology Today,* vol. 2018, nº 5, pp. 5-7, Mayo 2018.

[40] R. V. Clint, «DLT/Blockchain as a Building Block for Enterprise Transformation,» *IEEE Engineering Management Review,* vol. 47, nº 1, pp. 24 - 27, 25 Enero 2019.

[41] J. J. Hunhevic y D. M. Hall, «Do you need a blockchain in construction? Use case categories and decision framework for DLT design options,» *Advanced Engineering Informatics,* vol. 45, nº 101094, Agosto 2020.

[42] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System,» pp. 1-9, 2008.

[43] M. M. D. E. P. Mark C. Ballandies, «Decrypting Distributed Ledger Design -- Taxonomy, Classification and Blockchain Community Evaluation,» *Computers and Society*, nº 3, Enero 2020.

[44] B. Tsvetkov y H. Kostadinov, «DLT smart contract platforms for software lifecycle management,» *AIP Conference Proceedings*, vol. 2164, nº 1, Octubre 2019.

[45] R. ZHANG, R. XUE y L. LIU, «Security and Privacy on Blockchain,» *Cryptography and Security*, Agosto 2019.

[46] J. Moubarak, M. Chamoun y E. Filiol, «On distributed ledgers security and illegal uses,» *Future Generation Computer Systems*, vol. 113, pp. 183-195, 2020.

[47] B. Farahani, F. Firouzi y M. Luecking, «The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions,» *Journal of Network and Computer Applications*, vol. 177, nº 102936, 2021.

[48] A. Singh y K. Chatterjee, «SecEVS : Secure Electronic Voting System Using Blockchain Technology,» *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*, 2018.

[49] Z. Ma, W. Zhao, S. Luo y L. Wang, «TrustedBaaS: Blockchain-Enabled Distributed and Higher-Level Trusted Platform,» *Computer Networks*, vol. 183, nº 107600, Diciembre 2020.

[50] W. F. Silvano y R. Marcelino, «Iota Tangle: A cryptocurrency to communicate Internet-of-Things data,» *Future Generation Computer Systems*, vol. 112, pp. 307-3019, 2020.

[51] Y. Chen, S. Chen, J. Liang, L. W. Feagan, W. Han, S. Huang y X. S. Wang, «Decentralized data access control over consortium blockchains,» *Information Systems*, vol. 94, 2020.

[52] S. M. H. Bamakan, A. Motavali y A. B. Bondarti, «A survey of blockchain consensus algorithms performance evaluation criteria,» *Expert Systems with Applications*, vol. 154, nº 113385, 2020.

[53] A. Gervais, G. K. K. Wüst, V. Glykantzis, H. Ritzdorf y S. Capkun, «On the Security and Performance of Proof of Work Blockchains,» *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016.

[54] B. Cao, Z. Zhang, D. Feng, S. Zhang, L. Zhang, M. Peng y Y. Li, «Performance analysis and comparison of PoW, PoS and DAG based blockchains,,» *Digital Communications and Networks*, vol. 6, nº 4, pp. 480-485, Noviembre 2020.

[55] X. Li y C. A. Wang, «The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin,» *Decision Support Systems*, vol. 9, pp. 49-60, 2017.

[56] F. Dzulfikar y A. Susanto, «Implementation of Smart Contracts Ethereum Blockchain in Web-BasedElectronic Voting (e-voting),» *TRANSFORMTIKA*, vol. 18, nº 1, pp. 56-62, Julio 2020.

[57] V. Buterin, «Ethereum Whitepaper,» 2013 . [En línea]. Available: https://ethereum.org/en/whitepaper/. [Último acceso: 17 Diciembre 2020].

[58] L. Hang y D.-H. Kim, «Optimal Blockchain Network Construction Methodology Based on Analysis of Configurable Components for Enhancing Hyperledger Fabric Performance,» *Blockchain: Research and Applications*, nº 100009, Marzo 2021.

[59] S. Aggarwal y N. Kumar, «Chapter Sixteen - Hyperledger,» de *Advances in Computers*, vol. 121, Elsevier, 2021, pp. 323-343.

[60] Hedera, «The 3rd generation public ledger,» [En línea]. Available: https://hedera.com/. [Último acceso: 3 Enero 2021].

[61] B. Shabandri y P. Maheshwari, «Enhancing IoT Security and Privacy Using Distributed Ledgers with IOTA and the Tangle,» *2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)*, 13 Mayo 2019.

[62] T. Janečko y I. Zelinka, «Impact of Security Aspects at the IOTA Protocol,» *Proceedings of the Third International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'18),* pp. 41-48, 5 DIciembre 2018.

[63] G. d. R. Ikram Ullah, N. Meratnia y P. Havinga, «Threat Modeling—How to Visualize Attacks on IOTA?,» *Sensors*, vol. 21, nº 5, p. 1834, Marzo 2021.

[64] G. Bu, W. H. y M. Potop-Butucaru, «Metamorphic IOTA,» *ArXiv*, 8 Julio 2019.

[65] F. Guo, X. Xiao, A. Hecker y S. Dustdar, «Characterizing IOTA Tangle with Empirical Data,» *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, 25 Enero 2021.

[66] G. D. Roode, I. Ullah y P. J. M. Havinga, «How to Break IOTA Heart by Replaying?,» *2018 IEEE Globecom Workshops (GC Wkshps)*, 2018.

[67] A. Roman , IOTA - Introduction to the Tangle Technology: Everything you need to know about the revolutionary blockchain alternative, 2018.

[68] J. Sedlmeir, H. U. Buhl, G. Fridgen y R. Keller, «The Energy Consumption of Blockchain Technology: Beyond Myth,» *Business & Information Systems Engineering*, 2020.

[69] S. Sanju, S. Sankaran y K. Achuthan, «Energy Comparison of Blockchain Platforms for Internet of Things,» *2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS)*, 2018.

[70] L. M. M. Tonelli, «ABCDE–agile block chain DApp engineering,» *Blockchain: Research and Applications*, nº 100002, 2020.

[71] S. Keshav, «Paradoxes of Internet Architecture,» *IEEE Internet Computing*, vol. 22, nº 1, pp. 96-102, Febrero 2018.

[72] Y. Liu, «JSOptimizer: An Extensible Framework for JavaScript Program Optimization,» *2019 IEEE/ACM 41st International Conference on Software Engineering: Companion Proceedings (ICSE-Companion)*, Agosto 2019.

[73] F. S. Ocariza, K. Bajaj, K. Pattabiraman y A. Mesbah, «A Study of Causes and Consequences of Client-Side JavaScript Bugs,» *IEEE Transactions on Software Engineering* , vol. 43, nº 2, pp. 128 - 144, Febrero 2017.

[74] L. Liang, L. Zhu, W. Shang, D. Feng y Z. Xiao, «Express supervision system based on NodeJS and MongoDB,» *2017 IEEE/ACIS 16th International Conference on Computer and Information Science (ICIS)*, Junio 2017.

[75] A. Sterling, «NodeJS and Angular Tools for JSON-LD,» *2019 IEEE 13th International Conference on Semantic Computing (ICSC)*, Marzo 2019.

[76] S. Wang, L. Zhu y M. Cheng, «Docker-based Web Server Instructional System,» *2019 IEEE/ACIS 18th International Conference on Computer and Information Science (ICIS)*, Diciembre 2019.

[77] F. Altamimi, W. Asif y M. Rajarajan, «DADS: Decentralized (Mobile) Applications Deployment System Using Blockchain : Secured Decentralized Applications Store,» *2020 International Conference on Computer, Information and Telecommunication Systems (CITS)*, Octubre 2020.

[78] S. Sultana y S. Dixit, «Indexes in PostgreSQL,» *2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, p. Julio, 2017.

[79] ISO, «ISO/IEC 25022:2016 Systems and software engineering — Systems and software quality requirements and evaluation (SQuaRE) — Measurement of quality in use,» 2016. [En línea]. Available: https://www.iso.org/standard/35746.html. [Último acceso: 16 Marzo 2021].

[80] M. Contento, «DESARROLLO DE UN MÉTODO DE VALORACIÓN DE CALIDAD EN,» Repositorio Digital de la UTMACH, Machala, 2019.

[81] L. Alexander, A. Kusnadi, W. Wella, R. Winantyo y I. Z. Pane, «Authentication System Using 3D Face With Algorithm DLT and Neural Network,» *2018 Joint 10th International Conference on Soft Computing and Intelligent Systems (SCIS) and 19th International Symposium on Advanced Intelligent Systems (ISIS)*, 19 Mayo 2019.

5. ANEXOS

Anexo 1: Modelo de encuesta

ENCUESTA CON FINES ACADÉMICOS

Objetivo: Conocer el grado de confianza en el sistema de votación actual y la perspectiva hacia la implementación de un sistema de votación electrónica que posibilite ejercer el derecho al voto de manera remota en la Escuela de Informática de la Universidad Técnica de Machala.

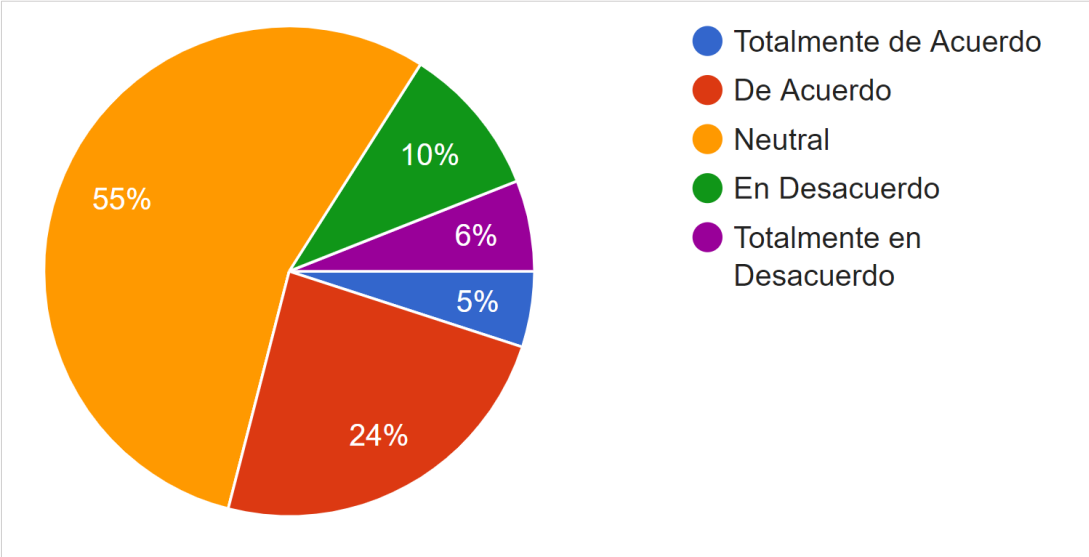
1. ¿Conoce el proceso actual para la elección de Gobierno Estudiantil?
    a. Totalmente de Acuerdo
    b. De Acuerdo
    c. Neutral
    d. En desacuerdo
    e. Totalmente en Desacuerdo
2. ¿Considera confiable el proceso de elección del Gobierno Estudiantil y los resultados obtenidos?
    a. Totalmente de Acuerdo
    b. De Acuerdo
    c. Neutral
    d. En desacuerdo
    e. Totalmente en Desacuerdo
3. ¿Acudiría a la Universidad para votar en las elecciones de gobierno estudiantil, si no fuera obligatorio?
    a. Sí
    b. No
4. ¿Participaría en las votaciones si pudiera realizarlo remotamente, desde cualquier lugar a través de un dispositivo que se conecte a internet?
    a. Sí
    b. No
5. Señale el tipo de dispositivo que utilizaría para realizar una votación online.
    a. Smartphone
    b. Tablet
    c. Laptop

d. Computadora de escritorio

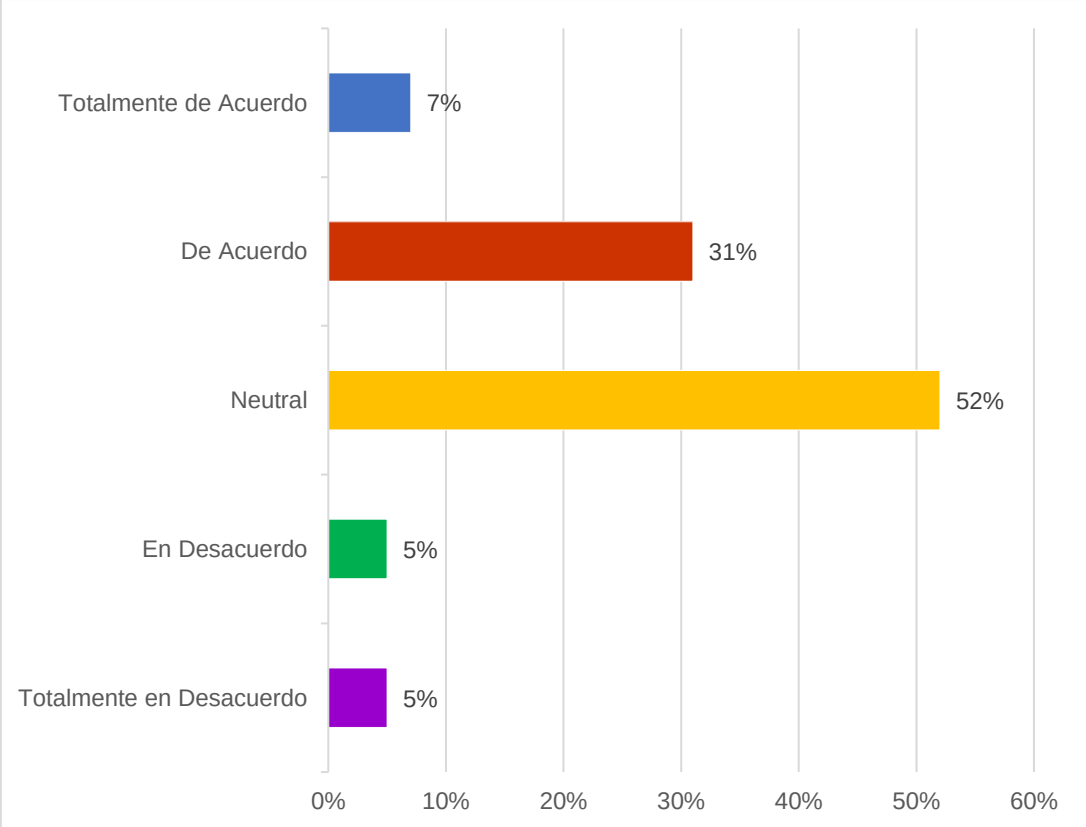
6. ¿Tiene usted conocimiento acerca de la tecnología blockchain como un método seguro para el almacenamiento de información?
    a. Totalmente de Acuerdo
    b. De Acuerdo
    c. Neutral
    d. En desacuerdo
    e. Totalmente en Desacuerdo
7. ¿Estaría de acuerdo en que se implemente un sistema de votación electrónica con una tecnología como blockchain para el almacenamiento encriptado e inmutable de la información?
    a. Totalmente de Acuerdo
    b. De Acuerdo
    c. Neutral
    d. En desacuerdo
    e. Totalmente en Desacuerdo
8. ¿Considera que el voto electrónico con tecnología blockchain brindaría mayor seguridad y confianza a los procesos electorales?
    a. Totalmente de Acuerdo
    b. De Acuerdo
    c. Neutral
    d. En desacuerdo
    e. Totalmente en Desacuerdo
9. ¿En un sistema de votación electrónica considera necesario incluir autenticación facial para reforzar la seguridad?
    a. Totalmente de Acuerdo
    b. De Acuerdo
    c. Neutral
    d. En desacuerdo
    e. Totalmente en Desacuerdo
10. Añada cualquier sugerencia que considere importante tener en cuenta en un proceso de votación democrático dentro de la UTMACH.

Anexo 2: Resultados de la encuesta

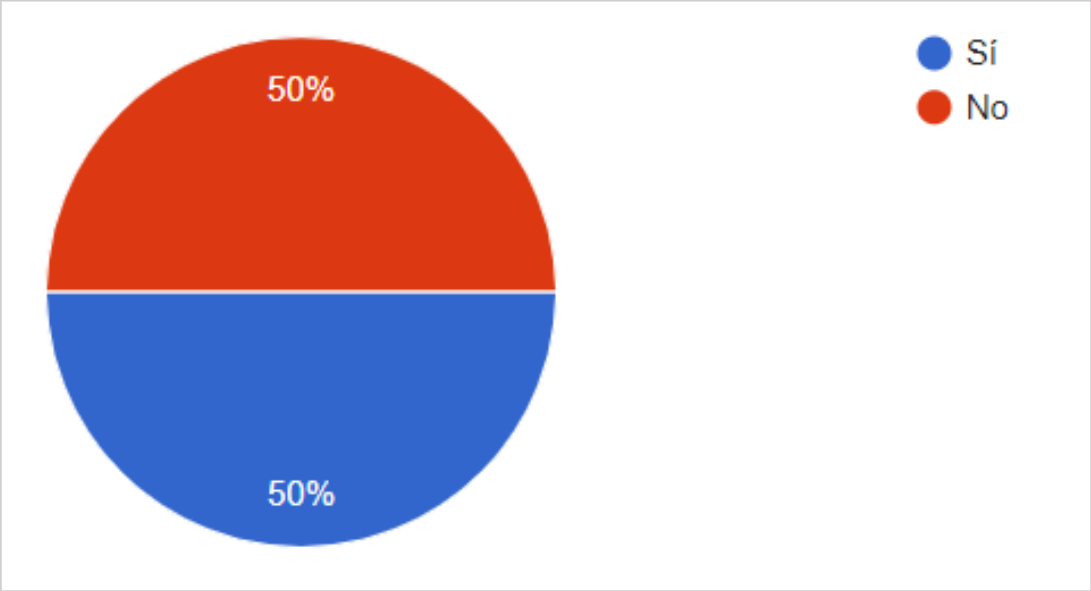
1. **¿Conoce el proceso actual para la elección de Gobierno Estudiantil?**



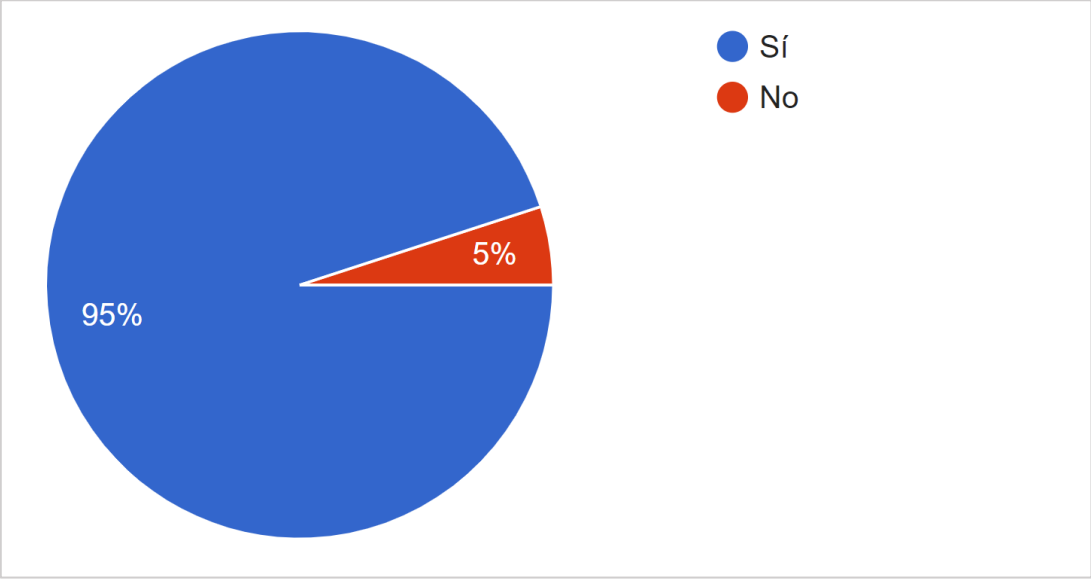
2. **¿Considera confiable el proceso de elección del Gobierno Estudiantil y los resultados obtenidos?**



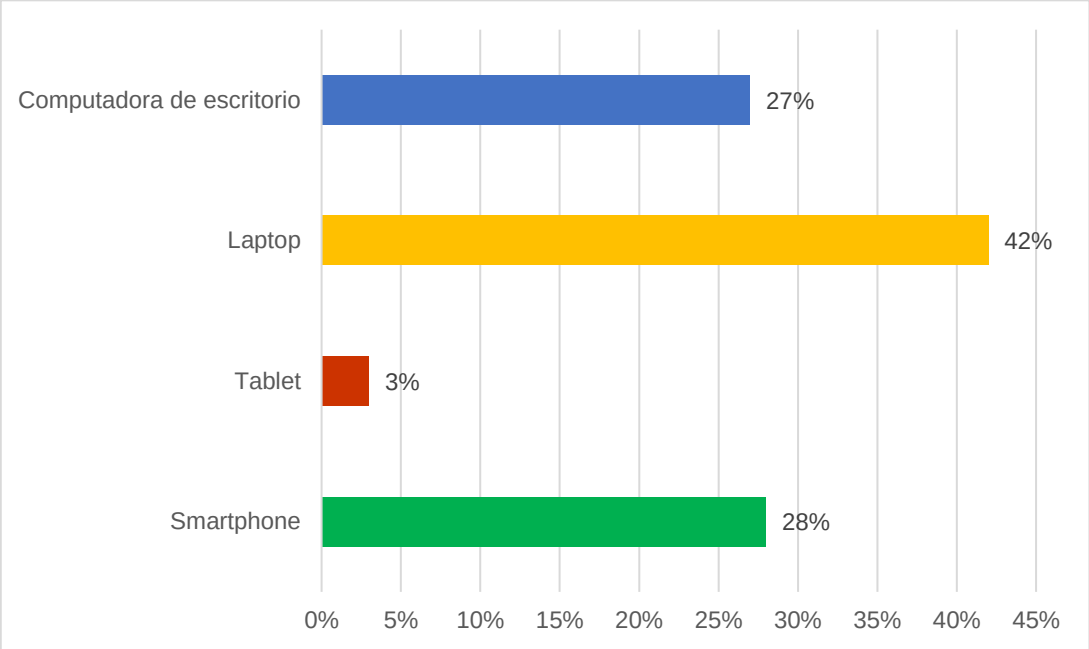
3. **¿Acudiría a la Universidad para votar en las elecciones de gobierno estudiantil, si no fuera obligatorio?**



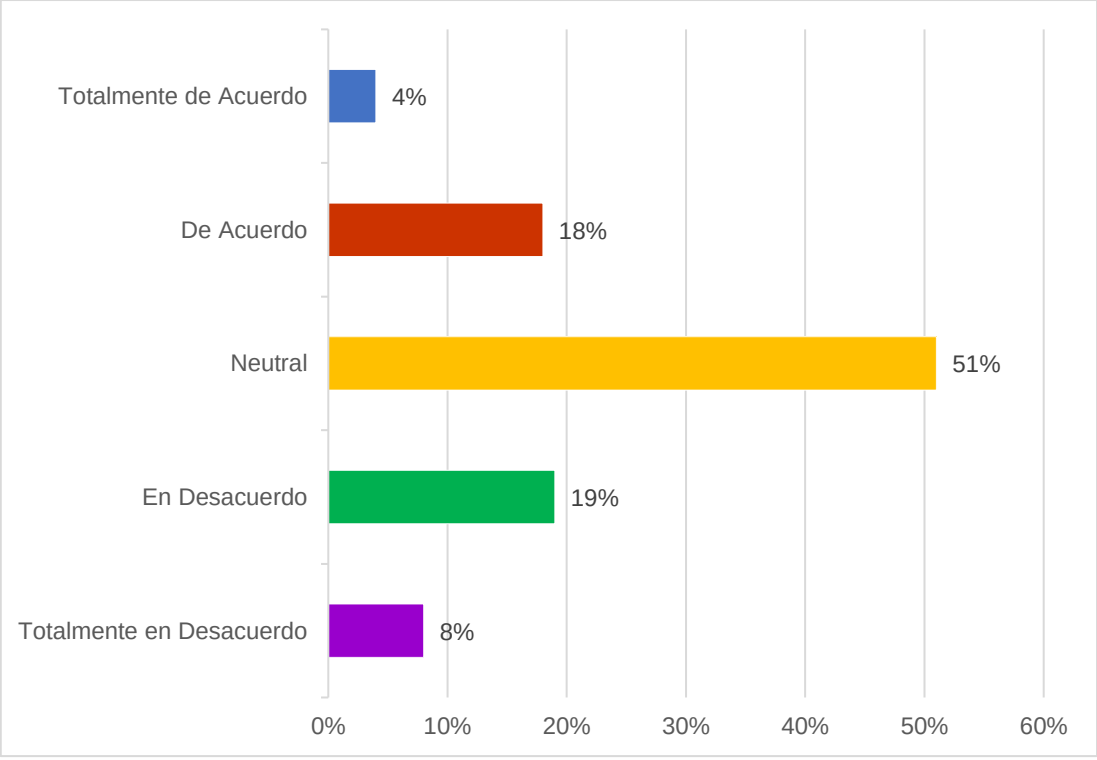
4. **¿Participaría en las votaciones si pudiera realizarlo remotamente, desde cualquier lugar a través de un dispositivo que se conecte a internet?**



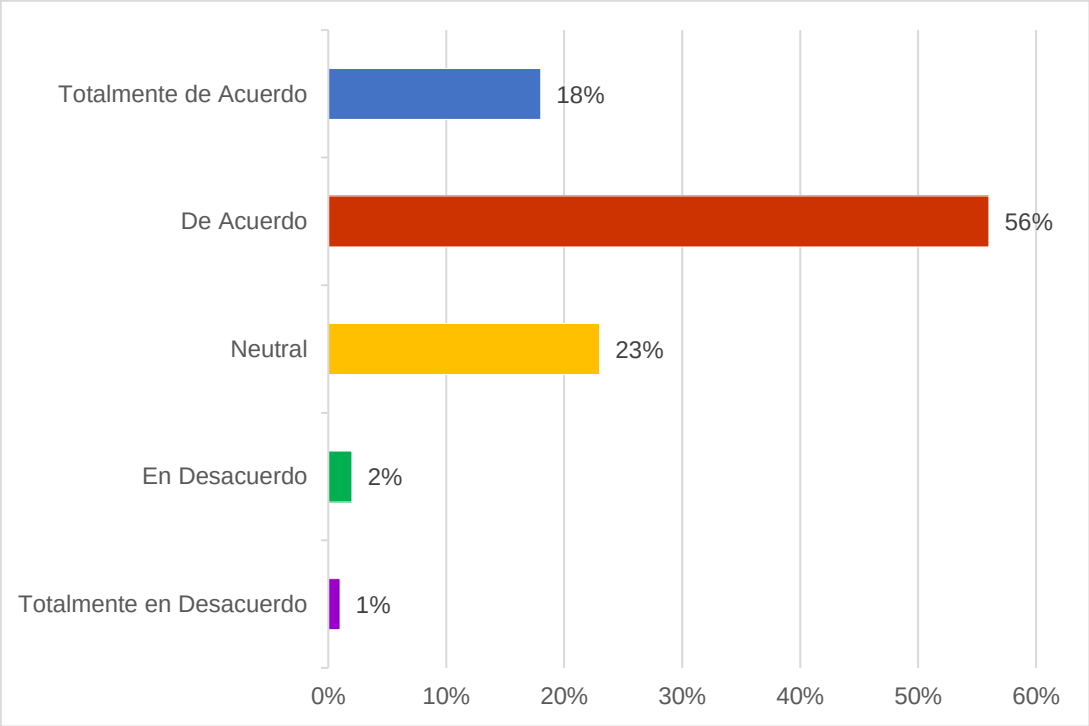
5. **Señale el tipo de dispositivo que utilizaría para realizar una votación online.**



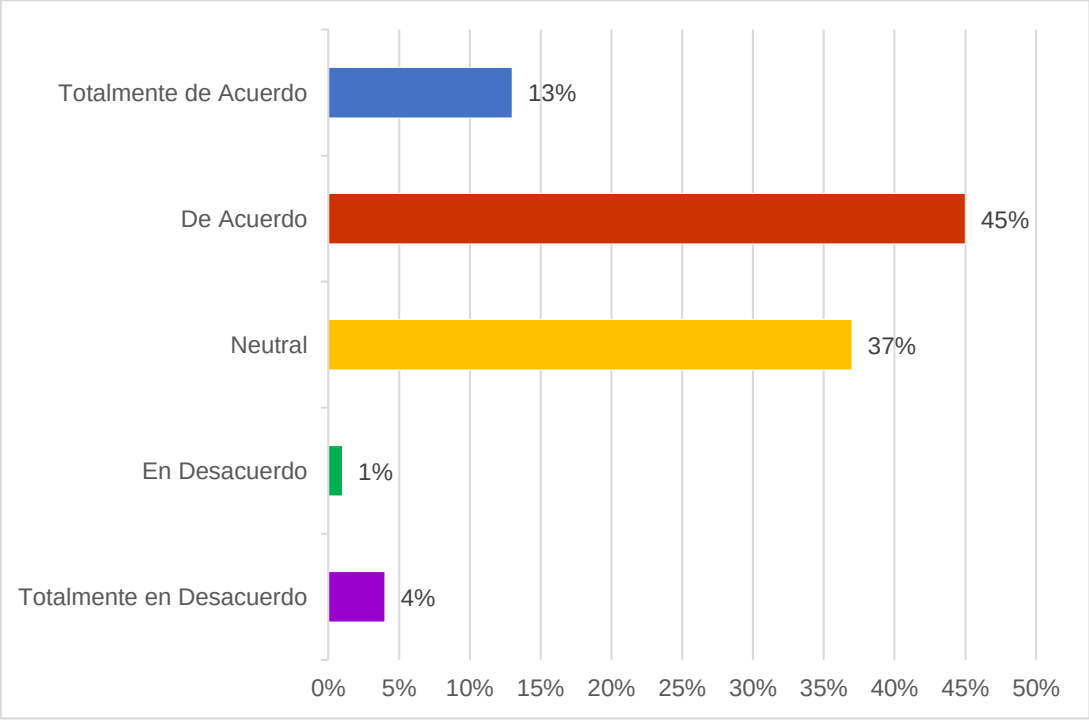
6. **¿Tiene usted conocimiento acerca de la tecnología blockchain como un método seguro para el almacenamiento de información?**



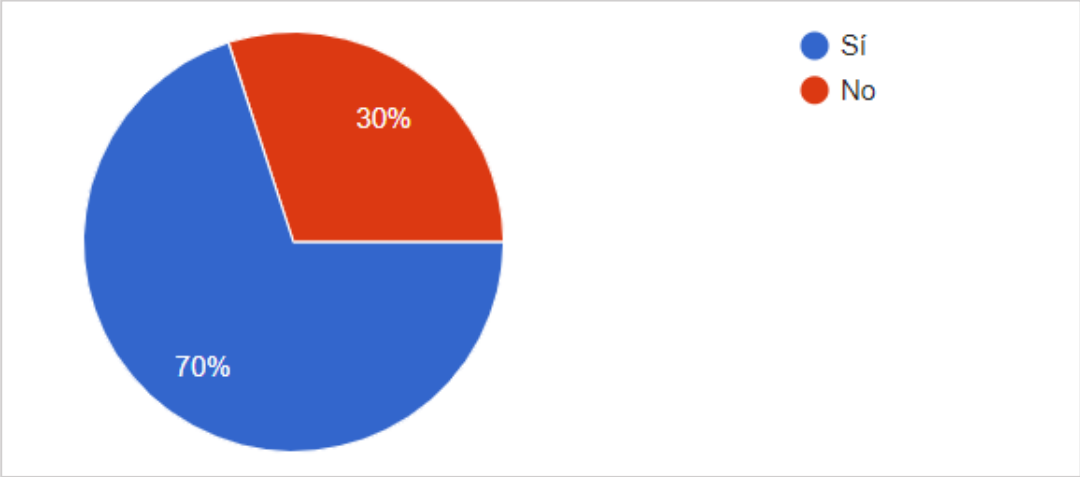
7. **¿Estaría de acuerdo en que se implemente un sistema de votación electrónica con una tecnología como blockchain para el almacenamiento encriptado e inmutable de la información?**



8. **¿Considera que el voto electrónico con tecnología blockchain brindaría mayor seguridad y confianza a los procesos electorales?**



9. **¿En un sistema de votación electrónica considera necesario incluir autenticación facial para reforzar la seguridad?**



10. **Añada cualquier sugerencia que considere importante tener en cuenta en un proceso de votación democrático dentro de la UTMACH.**
    - Mostrar transparente y eficazmente los procesos electorales
    - Tratar de hacer un sistema ordenado y fácil de votar
    - Una plataforma estable que no colapse por la cantidad de usuarios que ingresan el mismo día
    - Incluir verificación de voto, puede que por error voto incorrectamente
    - Más seguridad en los votos
    - Utilizar computación on-demand en servicios de cloud computing para evitar caídas/ineficiencia de los servicios por el flujo masivo de datos.
    - Organización. No llevo mucho tiempo como estudiante, pero he asistido a un sufragio y fue decepcionante; los estudiantes aglomerados, esperamos más de una hora porque empezaron tarde, estudiantes de otras carreras también esperaron. Sería más conveniente que el voto sea en las facultades y por año o apellido.
    - Tener un sistema electrónico para contabilizar bien los resultados
    - Que se aplace 1 hora más para votar
    - Se debe hacer el conteo de votos de forma honesta y muy precisa
    - Ver las propuestas al momento de las votaciones porque no se le entendía al momento que los candidatos llegaron a la clase

- Ser más eficientes en el momento de las elecciones para no ver ninguna dificultad.
- Dar a conocer, más sobre el tema de votaciones, porque existen algunos estudiantes que no saben algo respecto al tema.
- Seguridad por huella dactilar.
- Uso de huella digital con alguna tecnología de internet de las cosas y reconocimiento facial para registrar los votos.
- Poder conocer los candidatos antes de las elecciones para tener previamente definido a quién se lo considera idóneo
- Una mejor orientación a los de primer semestre.

Anexo 3: Historias de usuario

Historia de usuario #1		
Título: Módulo de configuraciones		
Usuario: Administrador		
Iteración asignada: 1	**Puntos estimados:** 7	**Prioridad:** Alta
Descripción: 1. El sistema debe requerir la autenticación para entrar al módulo de configuraciones, en donde solo un usuario con el rol de administrador tendrá acceso luego de ingresar correctamente su número de cédula y clave. 2. El usuario administrador requiere poder crear una convocatoria estableciendo el periodo de inscripción, campaña y votación; además requiere poder visualizar un listado de todas las convocatorias registradas en el sistema, en donde cada registro podrá ser editado o eliminado. 3. El usuario administrador requiere poder crear una lista y visualizar las listas registradas en el sistema, en donde tendrá las opciones de editar o eliminar una determinada lista. 4. El usuario administrador requiere poder crear una candidatura en la cual podrá seleccionar la lista, la convocatoria, los candidatos y podrá cargar la propuesta en formato pdf; además requiere poder visualizar un listado de todas las candidaturas registradas en el sistema, en donde cada registro podrá ser editado o eliminado.		

Tabla 15. Historia de usuario para el desarrollo del Módulo de Configuraciones

Historia de usuario #2		
Título: Módulo de Votación		
Usuario: Votante		
Iteración asignada: 2	**Puntos estimados:** 7	**Prioridad:** Alta

Descripción:

1. El usuario votante se autentica, ingresando el código de acceso que el sistema le envía, el cual será válido para ejercer su derecho al voto en una determinada convocatoria.

2. El sistema debe mostrar el listado de candidaturas registradas para una convocatoria específica, de forma similar a como se presentan en las papeletas de votación tradicionalmente usadas.

3. El sistema debe permitir al votante seleccionar un candidato de acuerdo a su afinidad, a su vez optar por el voto nulo o blanco si así lo desea el votante.

4. El sistema debe permitir enviar el voto con la opción seleccionada, lo cual equivale a depositar la papeleta en una urna.

5. El sistema debe mostrar un mensaje informando la selección del votante y pedir la confirmación de dicha selección, antes de ser guardado el voto de forma permanente e irrevocable.

6. El sistema debe enviar un correo electrónico luego de que un usuario ha enviado su voto, para certificar que este se ha guardado correctamente y que por lo tanto será contabilizado al final de la votación.

Tabla 16. Historia de usuario para el desarrollo del Módulo de Votación

Historia de usuario #3		
Título: Sitio web		
Usuario: Administrador, Votante		
Iteración asignada: 3	**Puntos estimados:** 7	**Prioridad:** Alta
Descripción: 1. El sistema debe mostrar en un sitio web la información sobre los plazos de inscripción, periodo de campaña, la fecha y horario de la votación para la convocatoria vigente. 2. El sistema debe mostrar el padrón electoral con los estudiantes que tienen registrada una matrícula en la base de datos institucional para el mismo periodo de la convocatoria vigente, en las carreras de Ingeniería de Sistemas y Tecnologías de la Información, las cuales integran la Escuela de Informática. 3. El sistema debe mostrar las candidaturas que se encuentran participando en la convocatoria vigente. 4. Luego de finalizada la etapa de votación, el sistema debe contabilizar los votos almacenados en la DLT y mostrarlos en un dashboard dentro del sitio web.		

Tabla 17. Historia de usuario para el desarrollo del Sitio web