Universidad APEC

UNAPEC

DECANATO DE INGENIERÍA E INFORMÁTICA

ESCUELA DE INFORMÁTICA

“TRABAJO DE GRADO PARA OPTAR POR EL TÍTULO DE INGENIERO DE SOFTWARE”

“ANÁLISIS Y DISEÑO DE UN SISTEMA DE VOTACIÓN ELECTRÓNICO BASADO EN CADENA DE BLOQUES PARA LA JUNTA CENTRAL ELECTORAL DE LA REPUBLICA DOMINICANA PARA EL AÑO 2024”

SUSTENTANTES:

REINIS ESPINAL CRUZ 2015-0395

VICTOR D. MONTERO ADAMES 2015-0569

ASESOR:

ING. EDDY GUZMÁN ALCÁNTARA SOLANO, MSc

Santo Domingo, D.N.

2019

Los conceptos expuestos en esta investigación son de exclusiva responsabilidad de su(s) autor(es)

ANÁLISIS Y DISEÑO DE UN SISTEMA DE VOTACIÓN ELECTRÓNICO BASADO EN CADENA DE BLOQUES PARA LA JUNTA CENTRAL ELECTORAL DE LA REPUBLICA DOMINICANA PARA EL AÑO 2024

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

TABLA DE FIGURAS

AGRADECIMIENTOS

Agradezco ante todo a Dios, el cual nunca me ha abandonado y me ha dado la fuerza para continuar y la gracia para seguir, que me ha provisto y me provee hasta el día de hoy. A mi madre, padre y mi hermano, que estuvieron ahí apoyándome y soportándome. A mi familia extendida: la iglesia, por su apoyo y sus oraciones.

Quiero agradecer a mi compañero Reinis Espinal, por su esfuerzo y aporte para completar este trabajo, además al profesor Ingeniero Eddy Alcántara, por su asesoría, que fue de mucha ayuda para completar este trabajo.

Además, quiero agradecer a Camilo Sánchez y Leonel Santiago, que juntos fuimos los autores originales de esta idea y a los profesores y compañeros de UNAPEC, que de alguna manera han contribuido al desarrollo de nuestro trabajo.

Y por último, quiero agradecer a la JCE por su aporte y por su cooperación en proveernos de información vital para llevar a cabo este trabajo.

Victor D. Montero Adames

Deposito mi agradecimiento sobre todo a nuestro Dios por haberme dado fuerzas para llegar a donde estoy ahora, por asignarme unos padres tan amorosos y preocupados por mi bienestar en todos los ámbitos desde pequeño, además de haber hecho ese esfuerzo de ayudarme en lo económico para el pago de mis estudios y de esa manera nutrirme de conocimientos y llegar hacer el profesional que tanto he anhelado.

Le agradezco a mis seres querido más cercano, porque han aportado tanto directa como indirectamente para que yo Reinis Espinal Cruz tenga el conocimiento para culminar este tema de investigación. También le agradezco a mi asesor de tesis Eddy Alcántara y a mi compañero Victor Montero por haber compartido conmigo esta última experiencia educativa, haber entregado tiempo, dedicación y esfuerzo en la elaboración de este trabajo de grado.

Gracias le doy a mis hermanos: Shadia Espinal Cruz y Chaniel Espinal Cruz por darme motivaciones, a mis tíos: Leo Espinal, Sonia Cruz, Celia Espinal, Kiara Espinal, Yolanda Espinal, Emmanuel Espinal, Jacobo Espinal, Freddy Guarionex Cruz y mis abuelos Freddy Cruz y Rita Donovan que de una u otra manera me mantenían presente y me brindaban su apoyo. También le doy gracias a mi pareja sentimental Stefany Muñoz Durán por haberme ayudado desde el inicio de todo y haberme brindado todo su apoyo, siempre estuvo ahí para brindarme amor y compañía.

Reinis Espinal Cruz

DEDICATORIAS

Dedico este trabajo a mi familia, en especial a mi madre Elizandra Adames y también a mi familia espiritual y extendida, que es la iglesia. Mi madre, así como mis hermanos en la fe, que siempre me han apoyado y soportado.

Victor D. Montero Adames

Dedico este trabajo a Dios sobre todas las cosas, mi papá Elvin Antonio Espinal Cruceta, a mi madre Glenys Lissette Cruz Donavan y a mi pareja sentimental Stefany Del Carmen Muñoz Durán. Estas personas estuvieron vinculadas muy estrechamente para la culminación mis estudios universitarios, apoyándome para alcanzar unas de mis mayores metas en la vida, depositándome su confianza y manteniendo mis motivaciones por los altos para que con esfuerzo esté aquí presente terminando mi tesis junto a mi compañero Victor montero. Fue un proceso fuerte y sin tiempo de descanso, por esto le agradezco muchísimo a las personas mencionadas por hacerme sentir con fuerzas, muchas gracias.

Reinis Espinal Cruz

RESUMEN EJECUTIVO

El presente trabajo de investigación se enfoca en proveer una solución para los diferentes problemas que se presentan durante las elecciones nacionales. Estos problemas se presentan como disputas entre los delegados de los partidos ya sea por boletas desaparecidas o por boletas declaradas como nulas por alguna razón, esto provoca discusiones entre los delegados, los directivos de la elección y los miembros del colegio, lo cual provoca pérdida de tiempo innecesaria. A esto se le suma los problemas de inconsistencias en los resultados obtenidos durante el periodo de escrutinio y conteo.

La JCE ha tratado de resolver estos inconvenientes, utilizando equipos tecnológicos que permitieran reducir el tiempo de conteo y escrutinio, sin embargo, estos no fueron lo suficientemente efectivos, por motivos como: falla en los equipos al escanear las boletas, entre otros.

Realizando investigaciones y analizando sistemas de votación que pudieran resolver o mitigar este tipo de inconvenientes, hemos encontrado que los sistemas más seguros y eficientes son los sistemas de votación electrónica que están basados en cadena de bloques, ya que todavía los sistemas de votación electrónica convencionales, como los de Estonia, Noruega y South Wale, Australia; presentan brechas de seguridad.

Los sistemas de votación electrónica basados en cadena de bloques como el propuesto, presentan mayor seguridad que los convencionales, ya que estos explotan las características que la Cadena de Bloques proveen. Esta propuesta consiste en el análisis y diseño de un sistema de votación electrónico que permita realizar votos de

manera segura, administrar candidatos y obtener resultados confiables y veraces; además de la capacidad de integrarse con el sistema de votación clásico basado en boletas.

Palabras Claves: Sistema de Votación Electrónica, Cadena de Bloques, Boletas, Caso de Uso, Diagramas de Modelado, Criptografía, Datos Biométricos, Llave Privada.

INTRODUCCIÓN

La democracia es una un aspecto importante de una república. Es la democracia la que nos mantiene lejos de un gobierno dictatorial. Es un acto de confianza colectivo que le da el poder al pueblo de decidir por quienes quieren ser dirigidos y gobernados. Los seleccionados deberían sentirse honrados por la responsabilidad que les fue encargada.

Para alcanzar la democracia, los países han diseñado sistemas para realizar la elección de sus dirigentes. Estos sistemas permiten realizar las elecciones de manera organizada y efectiva. Sin embargo, estos sistemas no han demostrado ser lo suficientemente veraces y seguros, además de que estos involucran mucha intervención humana, lo cual puede introducir falta de confianza y otros problemas.

Ante el gran avance tecnológico alcanzado tanto en el siglo pasado y el presente. Algunos países han optado por modernizar estos sistemas de votación, haciendo una transición de sistemas de votación basados en papel a sistemas de votación electrónicos, lo cuales explotan las nuevas tecnologías.

Estonia fue el primero de estos países en implementar el voto electrónico. Su sistema permite a los ciudadanos estonios votar desde cualquier computador con acceso a internet. Este sistema hace uso de varias tecnologías y técnicas de encriptación y autenticación. Sin embargo, la falta de adherencia a los procedimientos y otras fallas en el manejo de la información por parte del personal a cargo del sistema, lo hace vulnerable.

En América latina se han utilizado sistemas de votación electrónico, pero con flexibilidad, para obtener mayor seguridad. En Venezuela, se han utilizado sistemas que aun utiliza boletas físicas, pero con la excepción de que estas son digitalizadas. En Brasil, Ecuador, Costa Rica, Paraguay y más tarde en Venezuela, se han utilizado sistemas de votación electrónico, donde se han eliminado por completo las boletas físicas, siendo sustituidas por maquinas con pantallas táctiles que permite elegir a los candidatos solo pulsando sobre su imagen.

En República Dominicana, la JCE ha utilizado varios sistemas para automatizar las elecciones, siguiendo el paso de la tecnología. En un principio, en las elecciones del 2012 se utilizaron las unidades de “Escaneo y Transmisión” (EyT), las cuales permiten escanear y transmitir las boletas una vez escaneadas. Luego, para las elecciones del 2016 trataron de integrar los escáneres de INDRA, los cuales no fueron tan efectivos como se esperaba. Para las elecciones del 2020, se tiene planeado utilizar otro sistema que, en lugar de usar boletas físicas, usara pantallas táctiles, tal y como los sistemas de Brasil o Costa Rica.

Aun contando sistemas electrónicos de votación automatizados, existen vulnerabilidades, que pueden ser explotadas por ciber-criminales. Estos ciber-criminales son capaces de desviar y alterar los resultados finales.

El tema objeto de estudio procura proponer el análisis y diseño de un sistema de votación electrónico utilizando la tecnología *“BlockChain”* (Cadena de bloques); la cual procede del Bitcoin (Moneda virtual o criptodivisa creada por Satoshi Nakamoto en el año 2009) diseñada para desempeñarse como un procedimiento de intercambio que

aplica metodologías de encriptación generando una revolución tanto en lo económico como en lo tecnológico debido a su protocolo “BlockChain”.

La tecnología brinda la identificación de manera digital almacenando los datos de forma descentralizada. Es un registro incapaz de ser alterado, lo que permite que el voto no se pueda hackear; este es un mecanismo conveniente para proteger el sufragio de los dominicanos en un procedimiento electoral debido a que maneja la transparencia y la corrupción; factores que son vitales en las elecciones electorales de la Republica Dominicana.

BlockChain va a favor del arduo intento de parte de la Junta Central Electoral de buscar una solución moderna, confiable, rápida y clara de realizar las elecciones electorales. Por consiguiente, es necesario visualizar en un futuro próximo la tecnología BlockChain como parte del sistema de votación electrónico en la Republica Dominicana para garantizar una elección electoral confiable. Se considera el objeto de estudio idóneo como para brindar un arquetipo, preservar la identidad del ciudadano y para certificar un sistema incorruptible.

CAPÍTULO I: ASPECTOS INTRODUCTORIOS

DEL PROYECTO

1.1. Introducción

El sistema de votación de la Junta Central Electoral (JCE) de la Republica Dominicana ha tenido variaciones de procedimientos de votación con el tiempo; procedimientos poco confiables para la población dominicana, la cual ha aceptado los cambios para que cada fase hacia el poder presidencial sea transparente y eficaz.

La JCE aún persiste buscando nuevas maneras con fines de garantizar un proceso diáfano y, por consiguiente, proponemos una de las mejores tecnologías a nivel mundial que maneja datos encriptados conocida como “BlockChain” (Cadena de bloques) para aplicar la misma en nuestro sistema de votación.

El BlockChain integrado en nuestro sistema de votación permitirá almacenar data encriptada en una base de datos descentralizada con total anonimidad compartiendo la información en máquina, distribuidas sin posibilidad de alterar información existente, por lo que esta propuesta está enfocada en el estudio y planeamiento para una futura implementación teniendo encuentra todos los puntos clave.

1.2. Justificación

Se propone un diseño para un sistema de votación electrónico basado en la tecnología cadena de bloques (Blockchain) para las elecciones del 2024 en República Dominicana, teniendo en cuenta que nuestro país carece de procedimientos veraces y transparentes en cuanto a los sufragios se refiere. La tecnología de la cadena de bloques (Blockchain) nos permite hacer unas elecciones verídicas y totalmente transparentes ya que esta consiste en tener un registro inalterable de cualquier dato mediante un proceso de encadenamiento en bloques.

En previas ocasiones las elecciones han presentado dificultades, por ejemplo, a la hora de verificar los resultados, llevando esto a conflictos entre la sociedad y los delegados y hasta los mismos candidatos. Es por esto por lo que se decidió elaborar una propuesta para el uso de cadena de bloques (Blockchain) en las elecciones del país.

Un sistema como este podría acabar con las “elecciones casi arbitrarias” por parte de los gobiernos en curso, dando un resultado más concreto y válido a la hora de elegir nuestros representantes, quienes son los encargados de llevar nuestro país a la mejora continua y/o desarrollo.

1.3. Delimitación del Tema y Planteamiento del problema

La Junta Central Electoral (JCE) es un organismo autónomo, encargado de realizar y organizar elecciones de diferentes niveles. Esto incluye la recolección de votos, conteo de estos y además de emitir los resultados. (Constitución de la republica Dominicana, 2010)

La República Dominicana se encuentra afectada de forma muy notable por la corrupción en todos los niveles y procesos gubernamentales. Unos de estos procesos son el de las elecciones electorales, donde sufragio tras sufragio los resultados obtenidos en la misma se ponen en tela de juicio debido a los métodos obsoletos y de fácil manipulación que se utilizan para recolectar las votaciones. Debido a esto todos los procesos y métodos anteriormente usados resultan ser de poca veracidad para el pueblo dominicano y los mismos candidatos, en especial lo que no salen victoriosos.

Un ejemplo claro y en el cual está basada la investigación son los constantes fraudes electorales que ocurren al utilizar dispositivos electrónicos para la recolección

de los votos. Una vez uno de estos dispositivos es vulnerado, todos los demás dispositivos con las mismas características pueden serlo por igual.

Que un atacante logre vulnerar un dispositivo de votación masiva en el justo momento que se están presentando los votos de una nación pone en riesgo urgente la seguridad nacional y el futuro de esta. Considerando esto, es de suma importancia la utilización de tecnologías que permitan mantener la integridad de dicha actividad en donde sea que ocurran elecciones electrónicas, pero en el caso de nuestra investigación enfocado a la República Dominicana.

La mejor tecnología para llevar procesos de ese tipo que permitan la escalabilidad y presten primordial importancia a la integridad de los datos es conocida como BlockChain o cadena de bloques. Implementando esta tecnología se lograría asegurar la integridad de los datos que se manipulan en el proceso.

1.4. Alcance

Esta investigación consiste en la propuesta de un diseño de un sistema de votación electrónico basado en cadena de bloques, para la Junta Central Electoral, para las elecciones del 2024.

1.5. Objetivos

1.5.1. Objetivo General

- Proponer un análisis y diseño de un sistema de votación electrónico utilizando Cadena de Bloques, en las elecciones electorales de la Republica Dominicana en el año 2024.

1.5.2. Objetivos Específicos

- Diagnosticar el proceso de elecciones de la República Dominicana en los últimos 12 años.
- Analizar los sistemas de votaciones electrónicos utilizados por la JCE anteriormente.
- Determinar las ventajas y desventajas de un sistema de votación electrónico.
- Analizar teóricamente la tecnología de cadena de bloques.
- Analizar un sistema de votación más seguro.
- Diseñar un sistema de votación más seguro.

1.6. Marco Teórico

1.6.1. Antecedentes del problema

Los sistemas de votos electrónicos no son algo nuevo o solo de este siglo. De hecho, en los años 80 David Shaum diseñó un sistema de votación que usa criptografía de llave pública. Este sistema mantenía la identidad de los votantes anónima, para desvincularlos de las boletas. (Ayed, 2017)

Estonia fue el primer país en el mundo en implementar un sistema de votación electrónico. Estonia lo ha estado utilizando desde el año 2007, y le ha resultado beneficioso. Aunque este sistema no utiliza Blockchain como medio para persistir los votos. Este sistema utiliza la identificación que todos los ciudadanos estonios tiene, la cual tiene un chip integrado que el sistema utiliza para procesar votos. (Ayed, 2017)

Otros países han optado por un sistema electrónico de votación, tales como: Estados Unidos y Noruega.

Desde el año 2000 la Junta Central Electoral (JCE), ha estado realizando esfuerzos para automatizar las elecciones. En el 2002 la JCE introduce el escaneo de las Actas de Votación y en el año 2004 introduce el mecanismo de digitación ciega y aleatoria el cual consiste en mostrar parcialmente la boleta al digitador, de modo que los datos sensitivos sean protegidos. Luego en el año 2008 la JCE pudo integrar un dispositivo portátil, robusto que permitiera realizar casi todo el proceso de escanear, analizar y transmitir las boletas. A este dispositivo se nombró como “EyT” y este fue utilizado en las elecciones del 2012 de forma exitosa. (Junta Central Electoral, 2017)

La JCE, en busca de mejorar el proceso de las elecciones, de reducir el tiempo de respuesta y disminuir la complejidad del proceso de las elecciones Congresuales y Municipales, contrato los servicios de Indra Sistemas, S.A, para automatizar las elecciones del 2016. Estos equipos no cumplieron su objetivo, resultando en fracaso: En ninguna prueba se pudo conseguir que se transmitiera más del 74% de los Colegios Electorales que participaban en cada prueba. (Junta Central Electoral, 2017)

Recientemente, se ha acordado entre varios partidos y la JCE, el uso de un sistema de voto automático. Este no tiene nombre comercial, pero es un sistema desarrollado por la JCE para realizar las votaciones de las primarias, tanto abiertas como cerradas. Si bien este sistema será el que se utilizará en las primarias, se está contemplando su uso en las elecciones del 2020.

1.6.2. Definición de términos básicos o glosario

Sistema de Votación Electrónico (SVE): “Un sistema de votación electrónico (e-voting) es un sistema de votación en el cual los datos de las elecciones son

almacenados, persistidos y procesados en primer lugar como información digital" (Gritzalis, 2002 como citado en VoteHere, Inc., 2002)

Sistema Electrónico de Captación Directa (DRES): Son SVE que solo permiten realizar votos desde los centros electorales.

i-Voting: Se refiere a la capacidad de realizar votos desde cualquier dispositivo con conexión a internet. Los SVE de este tipo son más convenientes que los DRES, pero conllevan más riesgos a nivel de seguridad.

Criptografía: "Criptografía es la práctica y estudio de técnicas para la comunicación segura en presencia de terceros" (The CryptoParty handbook, 2013)

Criptografía de Llave Pública: En este tipo de criptografía se utilizando dos llaves, una pública y otra privada. Con la llave pública se cifra y con la llave privada se descifra la información cifrada con la llave pública.

Criptomoneda: Es una moneda virtual, cuyo valor se sustenta en el tiempo y energía invertidos en generarla. Estas monedas no son reguladas por instituciones u organizaciones. Son muy difíciles de imitar, ya que se basan en criptografía para generarlas.

Cadena de Bloques: "Cadena de bloques es una estructura de datos que contiene bloques de transacciones. Cada bloque en la cadena está conectado al bloque anterior en la cadena" (Ayed, 2017)

Hash: Es un conjunto de caracteres alfanuméricos de longitud fija. Es la representación de alguna información o dato, sin importar su longitud.

Resiliencia: Se refiere a la capacidad de recuperación de su operación de un sistema informático después de un desastre.

1.7. Metodología de la investigación

1.7.1. Enfoque, tipo y diseño de la investigación

Este trabajo tiene un enfoque cualitativo, ya que consiste en el análisis y diseño de un sistema, no en la recopilación de datos numéricos, y, por lo tanto, se realizará una investigación aplicada. Se presentarán los requerimientos y la arquitectura del sistema propuesto, así como un costo aproximado del mismo.

Se utilizarán un método deductivo, ya que se examinarán los sistemas de votaciones electrónicos en general para obtener un análisis y diseño de un sistema votación que utilice Cadena de Bloques como principal medio de almacenamiento de los votos.

1.7.2. Técnicas e instrumentos de recolección de datos o información

Se consultarán y entrevistarán a expertos, documentos institucionales, especificaciones, estándares, entre otros.

CAPÍTULO II: MARCO REFERENCIAL

2.1. Sistemas de Votación Electrónicos (SVE)

El proceso de votación es sin duda uno de los procesos que ha tardado más en automatizar. Este proceso al ser sensible para la democracia y soberanía de un país se ha dudado en automatizar. (Gritzalis, 2002), destaca algunas barreras para la implementación de SVE, tales como: El tiempo y la dificultad de cambiar leyes existentes, El tiempo y costo de certificar un SVE, Falta de un estándar para los sistemas de votación entre las naciones, Riesgo político asociado con probar un nuevo sistema de votación, entre otros.

2.1.1. Tipos de SVE

El (Internet Policy Institude, 2001), reconoce 3 tipos de SVE:

1. **Poll Site:** En este sistema los votantes acuden a los centros de votación y allí en lugar de elegir sus candidatos en boletas, lo hacen a través de máquinas de votación. A estos también se les conoce como Sistema Electrónico de Captación Directa o DRES por sus siglas en inglés. (Ayed, 2017)
2. **Kiosko (Kiosk):** En este sistema se utilizan Kioskos que permiten realizar las votaciones. Estos están ubicados en sitios de acceso público, como: Centros comerciales, Escuelas, bibliotecas, etc.
3. **Remotos:** En estos sistemas el voto es realizado desde cualquier computador con acceso a internet. Estos proveen gran facilidad, pero son más vulnerables que los otros 2 tipos. A estos también se les conoce como i-Voting.

2.1.2. Aspectos de Seguridad

Las elecciones son eventos importantes para la democracia de una nación. No es de extrañar que existan organismos como la JCE, con leyes tan rigurosas y de tanta envergadura como la Ley Electoral 275-97. El país entra en un toque de queda por un día, para elegir a sus dirigentes.

Por tanto, es esencial contar con un alto nivel de seguridad en los SVE, ya que estos son los que soportaran los sufragios. Los SVE deben de proveer privacidad, seguridad y eficacia a la hora de realizar el conteo.

2.1.2.1. Requisitos básicos de un SVE

Según (Gritzalis, 2002) los requisitos básicos que debe tener un SVE son:

- **Autenticación:** Solo deben votar los votantes registrados o hábiles para votar.
- **Unicidad:** El votante solo puede votar una vez y solo una vez.
- **Eficacia:** El voto debe de ser registrado correctamente por el SVE.
- **Integridad:** Una vez realizado el voto, este no podrá ser modificado.
- **Verificabilidad:** Los votos deben de poder ser contables en el momento de conteo.
- **Auditabilidad:** Debe de guardarse registros de los votos en elecciones pasadas.
- **Confiabilidad:** Los SVE deben de ser robustos y tolerante a fallos.
- **Discreción:** Los SVE no deben de permitir relacionar un voto con el votante, es decir deben de asegurar el Secreto del Voto.

- **Conveniencia:** Los votantes deben de poder realizar el voto con la mayor facilidad posible.
- **Transparencia:** Los votantes deben poseer conocimiento general de todo el proceso de votación.
- **Costo-Efectivo:** Los SVE deben de ser asequible y eficientes.

2.1.2.2. Mecanismos de seguridad

(Gritzalis, 2002) también señala diversos mecanismos de seguridad que debe de tener un SVE para asegurar la autenticidad, verificabilidad e integridad de los votos:

- **Criptografía:** Los SVE utilizan varios tipos de encriptación y diversas técnicas de encriptación, tales como: Cifrado Homeomorfo, Firmas digitales, encriptación simétrica y asimétrica, certificados digitales, firmas ciegas, etc.
- **Antivirus:** Estos sistemas en su mayoría operan sobre un sistema operativo. Dependiendo de dicho sistema operativo, estos tal vez necesiten software de protección especializados contra ataques de software malintencionados.
- **Firewalls:** Algunos SVE utilizan internet para funcionar, así que es necesario equipos firewalls que bloqueen peticiones y paquetes de origen dudoso.
- **Datos biométricos:** La mejor forma de asegurar la Autenticidad y Unicidad es sin duda usando datos irreplicables de los votantes. Esto se hace mediante el uso de lectores biométricos.

- **Smart Cards:** Estas tienen el mismo propósito que los datos biométricos, pero existe el riesgo de que el votante pueda (accidental o incidentalmente) perder su identificación y que esta caiga en manos equivocadas. Así que es más conveniente utilizarlas en conjunto con los datos biométricos.

2.1.3. Implementaciones

Hemos mencionado que hay cierto escepticismo con la implementación de un SVE, pero aun así algunos países y estados han los implementado, siendo Estonia el primer país en hacerlo.

2.1.3.1. Estonia: Sistema de I-Voting

Como se ha mencionado anteriormente, Estonia fue el primer país en utilizar un SVE para sus elecciones nacionales. Este sistema fue desarrollado en la nación misma y el organismo encargado de correr o ejecutar dicho sistema fue el Internet Voting Committee (Comité de I-Voting de Estonia).

Este SVE es un sistema I-Voting, es decir, permite a los ciudadanos estonios hábiles votar desde un computador con conexión a internet. Claro, no solo se necesita un computador con conexión a internet, también se requiere de su documento de identidad nacional y un programa cliente para realizar la votación.

2.1.3.1.1. Documento de identidad estonio

El documento de identidad de los estonios es también una tarjeta de chip o SmartCard, el cual les permite utilizar varios servicios públicos y también les permite firmar digitalmente los documentos. Dicha tarjeta tiene dos pares de llaves RSA, un par para autenticación y el otro par para firmar digitalmente. Los certificados que conectan

las llaves públicas y la identidad de los ciudadanos están almacenados en una base de datos LDAP que públicamente accesible. La tarjeta no permite exportar llaves privadas, por tanto, todas las operaciones de cifrado son realizadas dentro de las tarjetas y para mayor protección cada llave tiene un PIN asociado, el cual es requerido para cualquier operación que se fuera realizar con la tarjeta. (Drew Springall, 2014)

Figura 1: Documento de Identidad estonio

Fuente: (AS Sertifitseerimiskeskus)

2.1.3.1.2. Infraestructura del SVE I-Voting de Estonia

El cliente de votación es un programa que es preinstalado en las máquinas de los votantes. Estos encriptan la información de la boleta y la mandan a un servidor, conocido como Vote Forwarding Server (VFS). (Drew Springall, 2014)

El Vote Forwarding Server (VFS) sirve como intermediario entre el programa cliente y el Vote Storage Server (VSS). Este verifica la autenticidad del votante y luego

envía los votos al VSS. Este es el único servidor que es accesible desde internet. (Drew Springall, 2014)

El Vote Storage Server (VSS) almacena los votos encriptados durante el periodo de votación, este también verifica la firma digital del votante contra un servidor OCSP externo. (Drew Springall, 2014)

El Log Server es un servidor que no puede ser accedido, excepto por el personal a cargo de la elección. Este servidor almacena logs, monitorea los votos, además de recolectar estadísticas. (Drew Springall, 2014)

El Vote Counting Server (VCS) es un servidor que no está conectado a ninguna red. Los votos son extraídos del VSS, grabados en un DVD y luego introducidos en el VCS. El VCS está conectado a un HSM el cual desencripta los votos con la llave primaria de la elección. Finalmente, el VCS cuenta los votos y muestra los resultados. (Drew Springall, 2014)

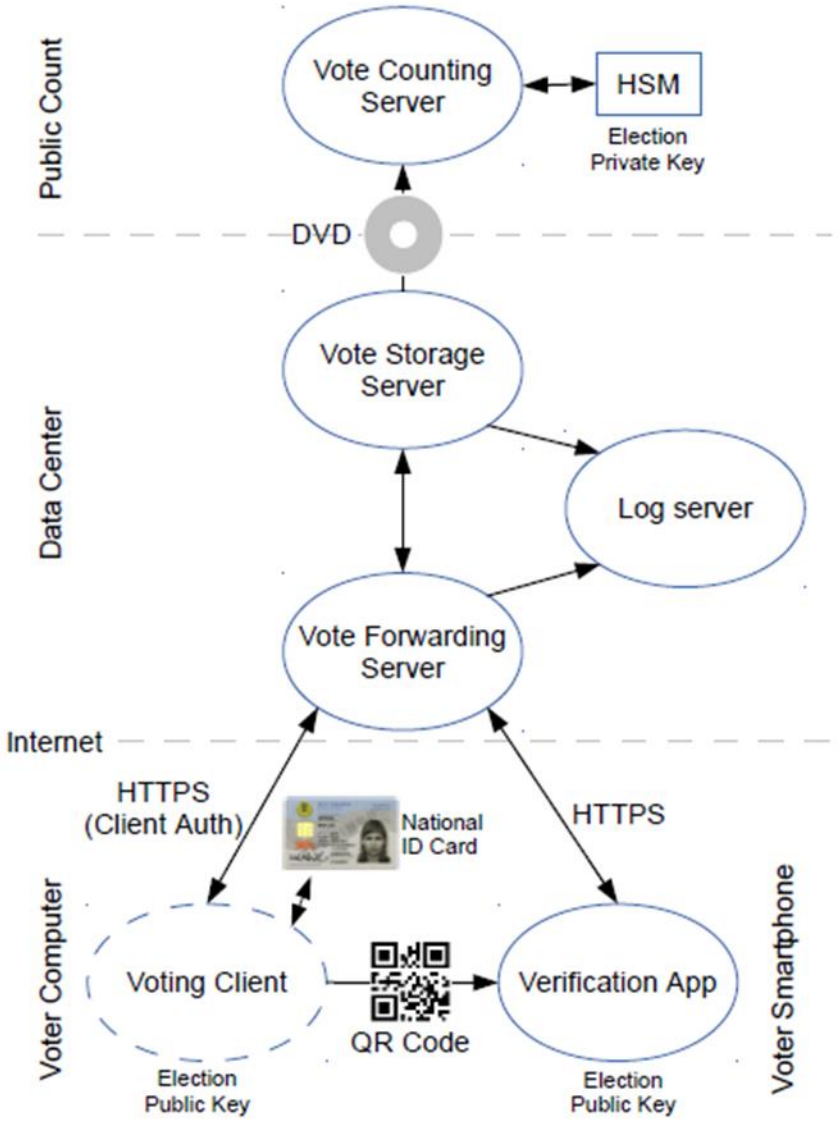


Figura 2: Infraestructura Estonia I-Voting

Fuente: (Drew Springall, 2014)

2.1.3.1.3. Proceso de Votación

El proceso de votación con el I-Voting es el siguiente:

1. El votante ejecuta el programa cliente, luego el votante inserta su documento de identidad y un PIN asociado con su llave de autenticación.

2. El programa cliente estable una conexión con el VFS y utiliza un certificado codificado en el mismo, para autenticar el servidor VFS.
3. El VFS verifica la elegibilidad del votante basado en la llave pública del votante y luego retorna una lista de candidatos.
4. El votante elige su candidato *c* e introduce su PIN utilizado para firmar digitalmente.
5. El programa cliente rellena *c* usando RSA-OAEP con un número aleatorio *r* luego encripta el voto con la llave publica de la elección, y también firma el voto con la llave privada del votante y lo envía al VFS.
6. El VFS recibe el voto, lo asocia con un token *x*, el cual es enviado al cliente junto al número aleatorio *r*.
7. El cliente luego muestra en pantalla a *x* y a *r* codificados como código QR.
8. El votante puede verificar que su voto no ha sido alterado utilizando una aplicación móvil de la elección. La aplicación lee el código QR y verifica que los datos son válidos.

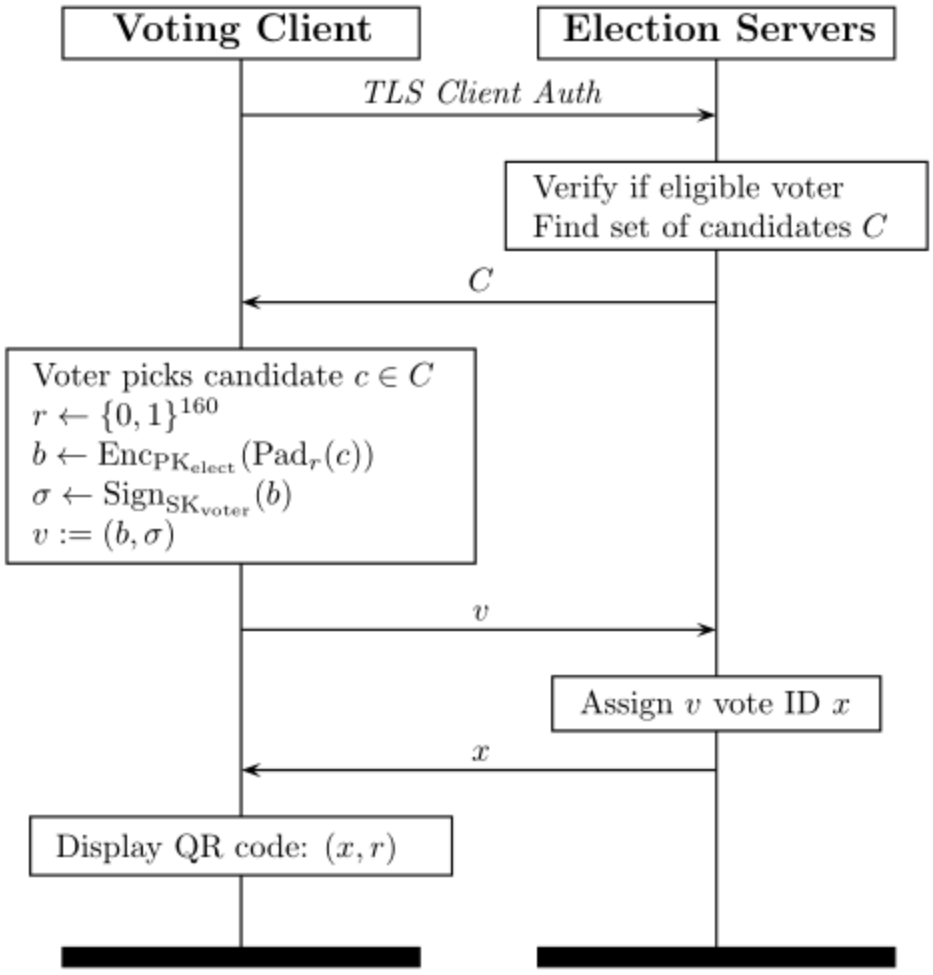


Figura 3: Proceso de Votación Estonia I-Voting: Votación

Fuente: (Drew Springall, 2014)

2.1.3.1.4. Proceso de Verificación

Después de procesar un voto con el programa cliente, el votante puede utilizar la aplicación de verificación, para certificar que su voto no fue alterado.

El proceso de verificación que la aplicación realiza es el siguiente:

1. La aplicación escanea el código QR para obtener a *r* y a *x*. La aplicación envía *x* al servidor, para obtener un voto *b*, junto a una lista de candidatos posibles.

2. La aplicación usa a *r* para encriptar un voto simulado para cada uno de los candidatos posibles.
3. La aplicación compara los resultados con *b*, si algún candidato concuerda, la aplicación muestra dicho candidato en pantalla.

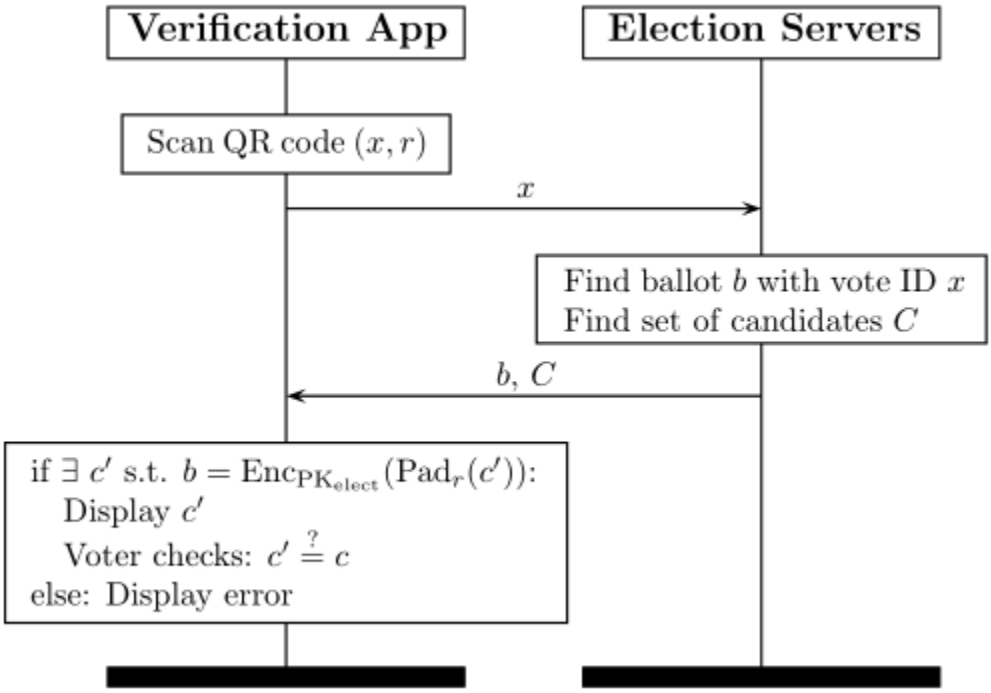


Figura 4: Proceso de Votación Estonia I-Voting: Verificación

Fuente: (Drew Springall, 2014)

2.1.3.1.5. Proceso de tabulación o conteo de votos

Al final de las elecciones, se procede a la etapa de Tabulación. En esta etapa se obtienen los resultados de la elección.

El proceso de Tabulación es el siguiente:

1. El VSS procesa los votos encriptados para eliminar los votos revocados o inválidos.

2. Los oficiales extraen los votos encriptados sin las firmas, y almacenan los votos anónimos encriptados en un DVD.
3. El VCS desencripta los votos usando un HSM que contiene la llave privada de la elección. Estos votos desencriptados son tabulados y los resultados son combinados con los resultados de los colegios de votación, después son publicados.

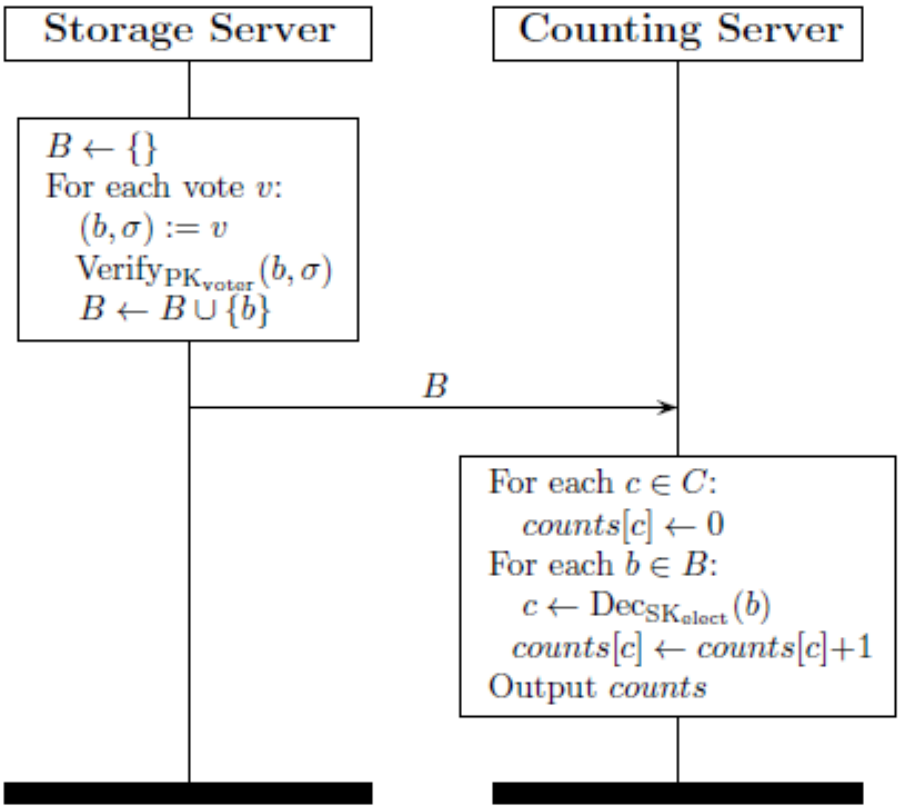


Figura 5: Proceso de Votación Estonia I-Voting: Tabulación

Fuente: (Drew Springall, 2014)

2.1.3.2. Noruega: Sistema de I-Voting

En las elecciones municipales de Noruega, llevadas a cabo el 12 de septiembre del 2011, se puso en funcionamiento un SVE tipo I-Voting que permitiera captar votos en conjunto con el sistema tradicional.

Dicho SVE cumplió con su objetivo con algunos inconvenientes. Aun así, estos inconvenientes fueron causados por mala coordinación, procesos ineficientes y factores externos fuera del control de los organismos noruegos.

2.1.3.2.1. Infraestructura del SVE I-Voting de Noruega

El SVE de Noruega consta de varios componentes, tales como:

Aplicación de Votación: Es un applet de java, con el cual el votante pude interactuar. Este acepta el voto del votante, lo encripta y lo envía al Vote Collector Server (VCS). (OSCE/ODIHR Election Expert Team, 2012)

Vote Collector Server (VCS): Es un servidor contiene un programa que sirve como una urna, donde los votos son almacenados. (OSCE/ODIHR Election Expert Team, 2012)

ID-Portal: Este componente es utilizado para autenticar a los votantes. Los votantes deben de registrarse en este portal, antes de realizar el voto electrónicamente. Esto solo se realiza una vez. (OSCE/ODIHR Election Expert Team, 2012)

Return Code Generator (RCG): Este componente es un servidor que se encarga de calcular y transmitir los códigos de retorno, a través de SMS. (OSCE/ODIHR Election Expert Team, 2012)

Servidores del Ministerio de Justicia: Son un conjunto de componentes, cuyo propósito es el de depurar, mezclar y contar los votos. El servidor de depuración

elimina las boletas repetidas del mismo votante, boletas de votantes que también votaron usando una boleta física y boletas de votantes que no están en la lista de votantes. (OSCE/ODIHR Election Expert Team, 2012)

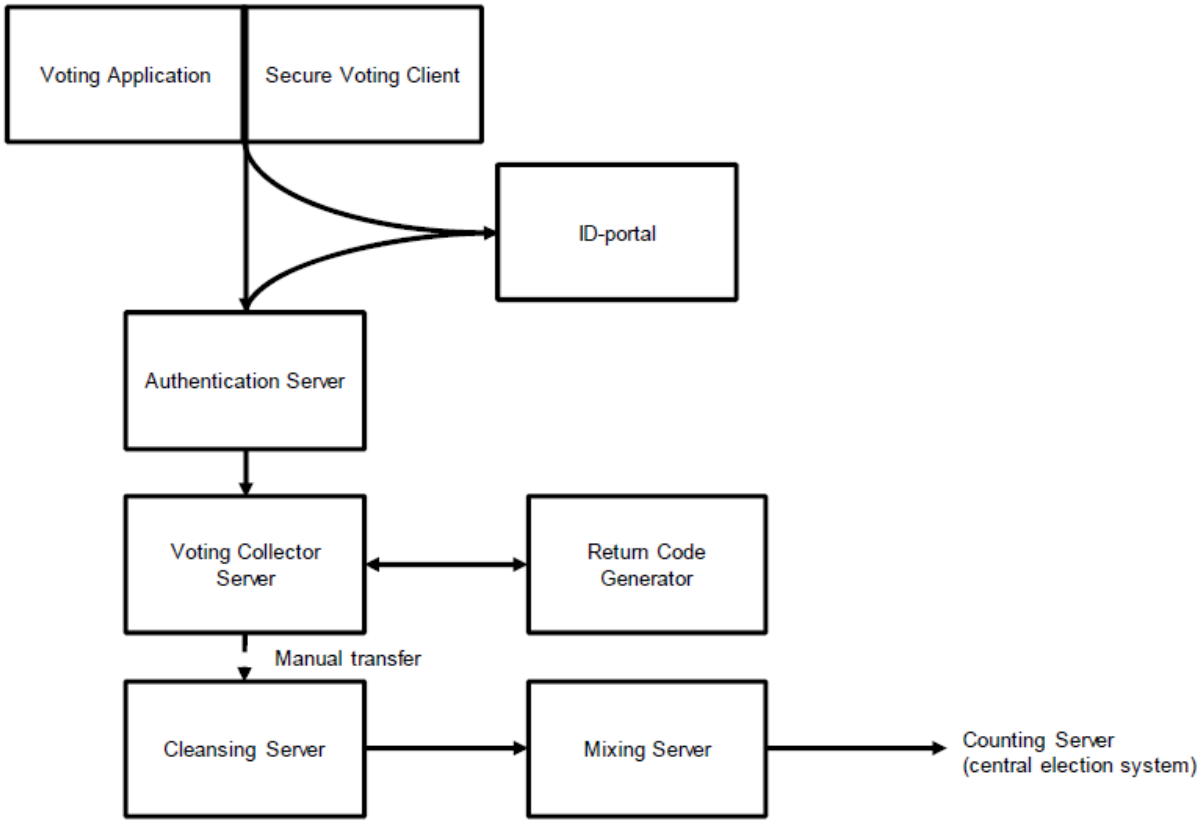


Figura 6: Infraestructura Noruega I-Voting

Fuente (OSCE/ODIHR Election Expert Team, 2012)

2.1.3.2.2. Proceso de Votación

Este SVE fue diseñado para representar la votación basada en papel. Por esto algunos términos son iguales que los usados en el sistema convencional basados en boletas de papel.

Para que un ciudadano noruego pueda realizar un voto utilizando el SVE, este debe de estar registrado en el ID-Portal, de lo contrario, su boleta será eliminada en el proceso de limpieza y depuración.

1. El proceso para registrarse en el ID-Portal es el siguiente:
2. En el portal, el votante debe seleccionar su ubicación.
3. El votante inicia sesión con sus credenciales.
4. El SVE dirige la transacción al proveedor común de identidad.
5. Este proveedor autentica al votante y luego regresa automáticamente al SVE.
6. El SVE recibe la confirmación de la autenticación del votante.
7. El SVE, luego revisa los permisos de usuario y muestra los roles para los cuales el votante tiene privilegios.
8. El votante, entonces elige el rol con cual quiere continuar.

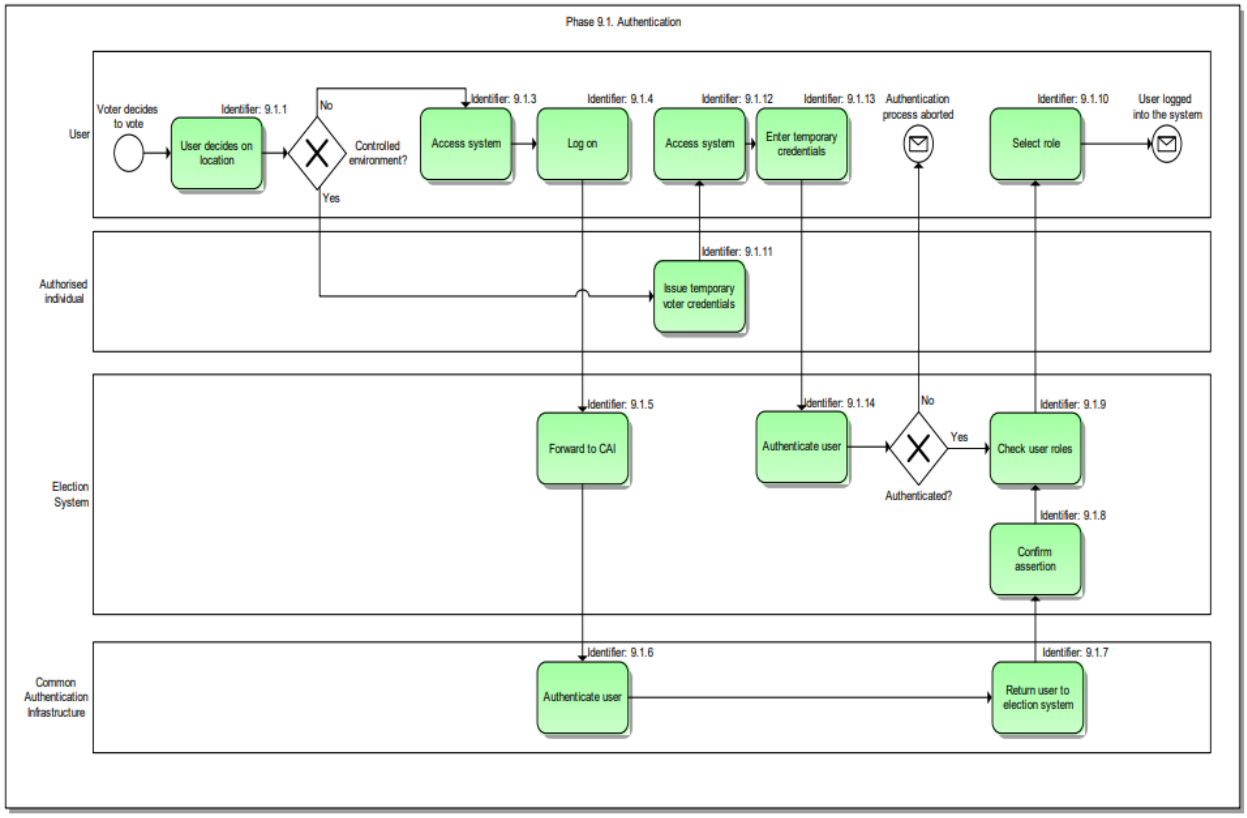


Figura 7: Proceso de Votación Noruega I-Voting: Autenticación

Fuente: (Norwegian Minitry of Local Goverment And Regional Development, 2011)

Una vez el votante es autenticado, el mismo puede proceder a realizar su voto utilizando la aplicación de votación.

El proceso de votación es el siguiente:

1. El SVE verifica al votante contra el padrón electoral.
2. El SVE muestra los candidatos.
3. El votante elige un candidato o modifica su elección, y luego procesa su voto.
4. El SVE marca al votante en el padrón electoral. Cuando el votante es marcado, aunque procese otro voto de manera presencial por el sistema

tradicional, su boleta electrónica será descartada en el SVE y solo se contara la boleta física.

5. La boleta es almacenada en el VCS.
6. Al mismo tiempo el votante recibe un código de retorno que indica si su boleta fue alterada o no. Esto puede usarse como verificación.

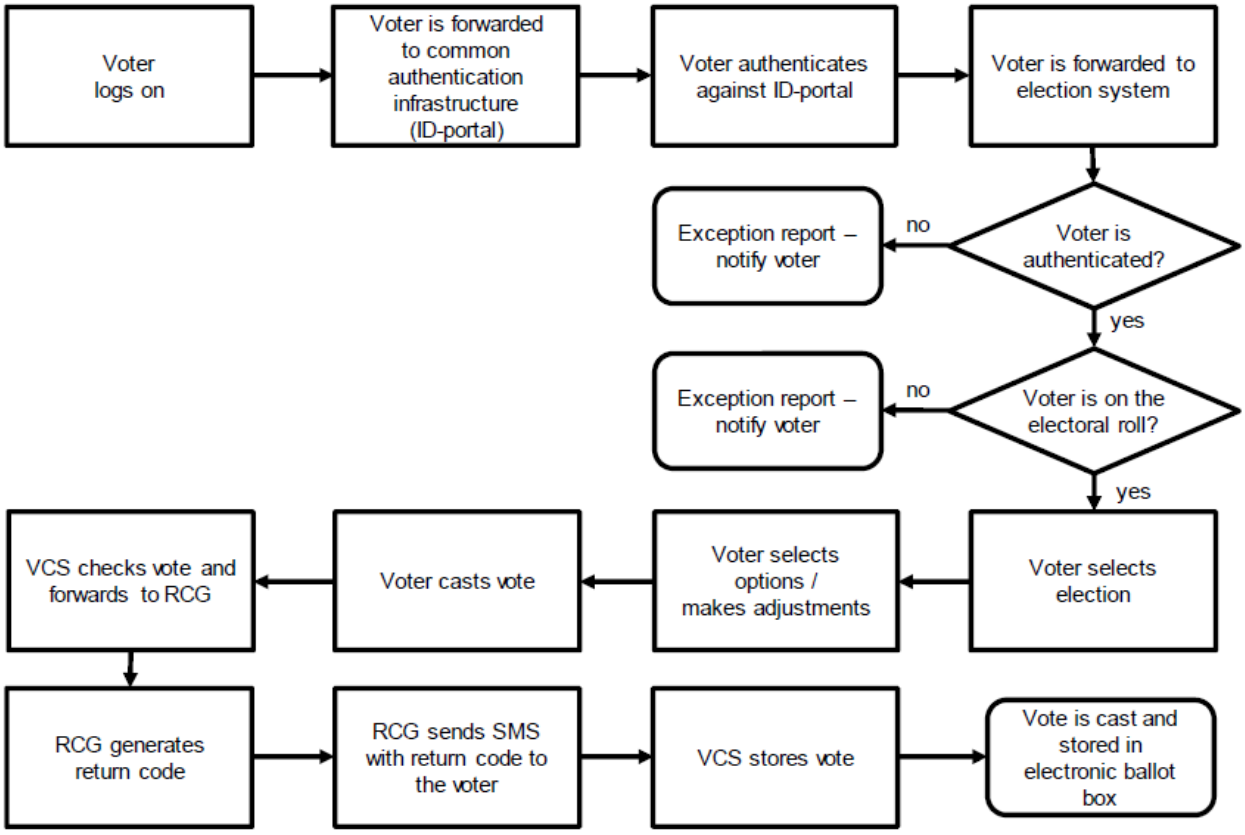


Figura 8: Proceso de Votación Noruega I-Voting: Votación

Fuente: (OSCE/ODIHR Election Expert Team, 2012)

2.1.3.2.3. Proceso de Depuración de Votos y Conteo

En este proceso los servidores del ministerio de depuran las boletas y realizan un conteo, junto con las boletas físicas.

El proceso de depuración y conteo es el siguiente:

1. Las boletas electrónicas son extraídas e introducidas en el sistema de conteo.
2. El servidor de depuración elimina las boletas duplicadas, las boletas que tiene una correspondiente física para un mismo votante y las boletas, cuyos votantes no se encontraron en el padrón electoral.

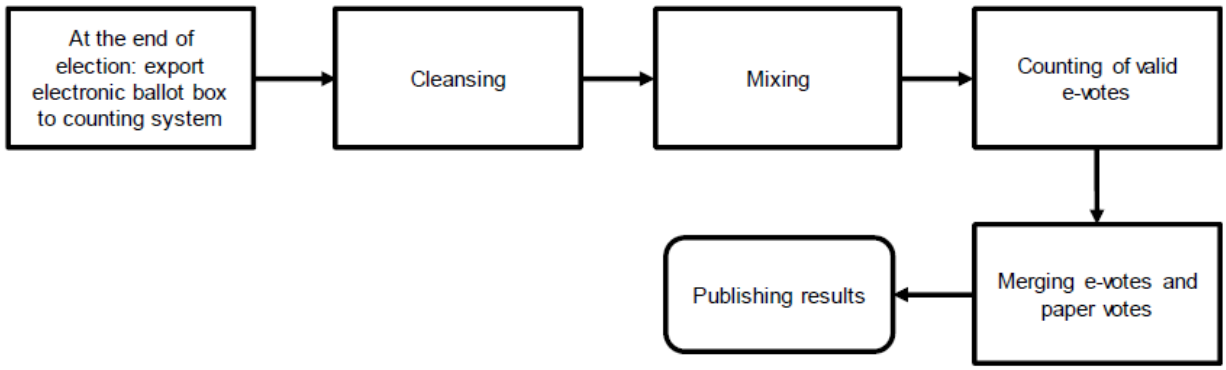


Figura 9: Proceso de Votación Noruega I-Voting: Depuración de boletas y Conteo

Fuente: (OSCE/ODIHR Election Expert Team, 2012)

2.1.3.3. South Wale iVote: Sistema de I-Voting

El SVE iVote fue desarrollado por un proveedor de SVE llamado Scytl, en cooperación con la Comisión Electoral de New South Wales en Australia. Este sistema como todo i-Voting permite votar a través del internet. iVote se ha estado utilizando en Australia desde 2011 hasta la fecha.

El proceso de votación usando iVote consta de tres etapas:

- **Aplicación:** Donde el votante se registra para realizar su voto utilizando el portal web de iVote. En esta etapa, se verifica el padrón electoral si el votante tiene derecho al voto.

- **Votación:** En esta etapa el votante puede realizar su voto.
- **Verificación:** El votante puede verificar si su voto se ha realizado con éxito.

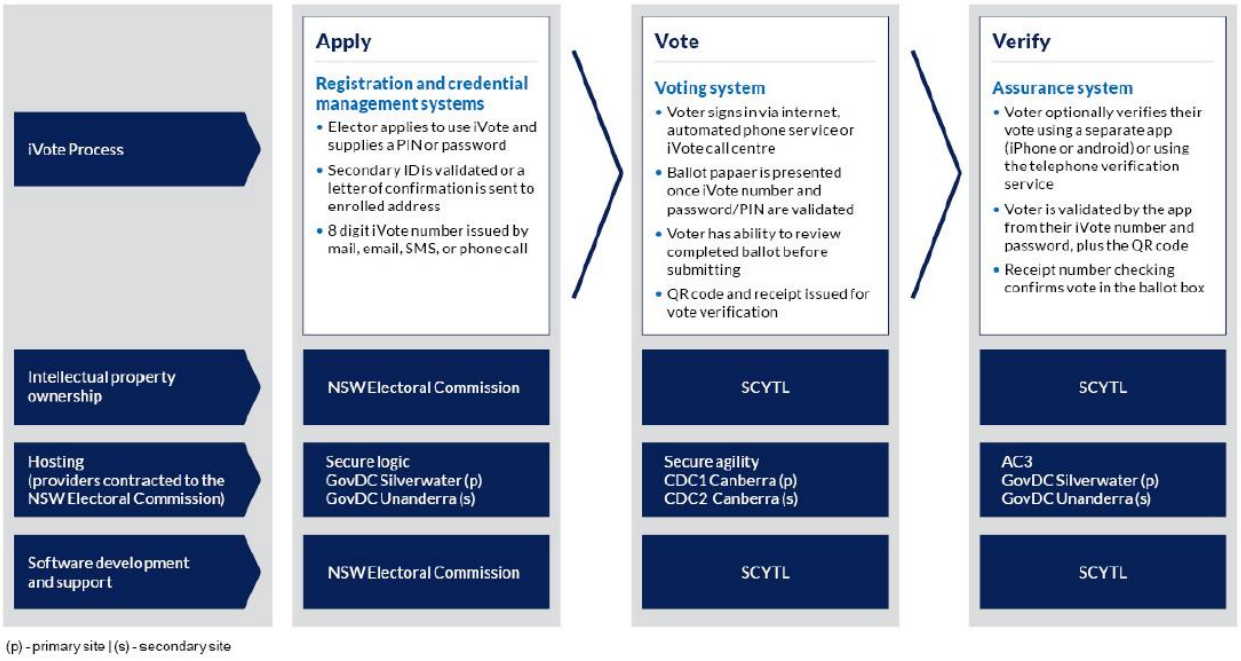


Figura 10: Proceso completo de votación iVote

Fuente: (NSW Electoral Commission, 2019)

2.1.3.3.1. Infraestructura de iVote

- **Sistema de registro y Gestor de Credenciales:** Son sistemas utilizados para autorizar a los votantes para que estos puedan realizar su voto a través del iVote.
- **Sistema iVote:** Este permite a los votantes realizar su voto vía internet o mediante una llamada telefónica, la cual es procesada por un IVR. Una vez realizado el voto el votante puede verificar si su voto fue almacenado sin problemas.

- **Proportional Representation Computer Count (PRCC):** Es una computadora, donde los votos son depurados, mezclados con votos de otros canales, desencriptados y finalmente contados.
- **Servidor de Verificación:** Este servidor almacena copias de los recibos generados cuando se realiza un voto a través de iVote.

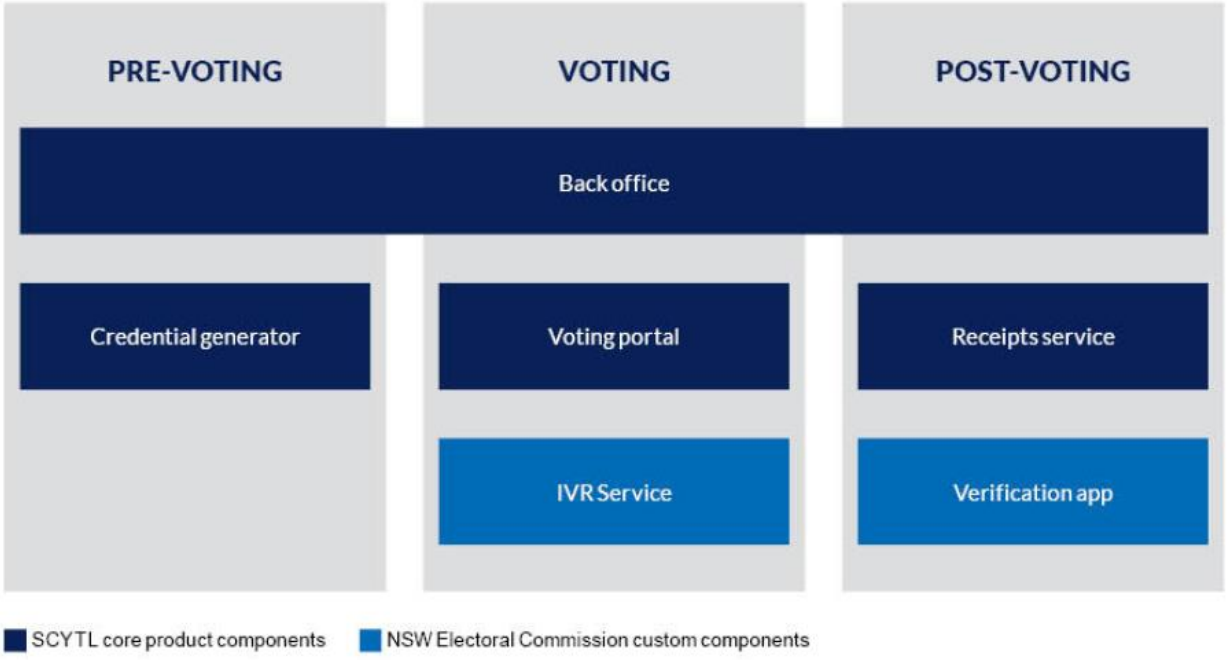


Figura 11: Arquitectura conceptual de iVote

Fuente: (NSW Electoral Commission, 2019)

2.1.3.3.2. Proceso de Votación

Para realizar un voto a través del iVote, el votante debe registrarse en el Sistema de Registro. El Sistema de Registro, verifica la información del votante en el padrón. Una vez registrado el votante, el Gestor de Credenciales genera un número de iVote y lo pasa al sistema de votación iVote. iVote genera un identificador único a partir de la contraseña, PIN y el número de iVote, también este genera una boleta en vacía, que se llenara con la información del voto.

Los votantes pueden realizar su voto a través del website de iVote. Estos deben de iniciar sesión con su número de iVote y contraseña. Luego el votante elige sus candidatos, después de que el votante somete su voto, este es encriptado y digitalmente firmado en el navegador, una prueba de integridad es generada por el mismo y es enviado a una urna electrónica de boletas. Una vez recibido, el iVote genera un recibo de entrega basado en la información de la boleta. Junto con el recibo, se genera un código QR, con el cual se puede verificar que el voto ha sido procesado correctamente.

2.1.3.3.3. Proceso de Verificación

Para verificar el voto electrónico procesado a través de iVote, los votantes deben de instalar una aplicación de verificación de iVote en sus teléfonos inteligentes. Luego de sometido el voto, iVote muestra un código QR a los votantes. Los votantes pueden escanear el código QR con la aplicación móvil de iVote. Al inicio la aplicación requerirá el numero iVote y la contraseña del votante. Luego de escanear el código e introducir los datos solicitados, la aplicación mostrará la elección del votante.

2.1.3.3.4. Proceso de Conteo

Después de que el proceso de votación terminal, las boletas almacenadas en el iVote son desencriptadas e importadas en el PRCC, junto con las boletas captadas a través de otro canal de votación.

Este proceso consta de 4 etapas:

1. El proceso de depuración elimina boletas con inconsistencias, sin la necesidad de desencriptarlas. En este proceso se eliminan las boletas

duplicadas de un mismo votante y las boletas captadas por canales diferentes que correspondan a un mismo votante.

2. El servicio de “mezclado” romper con la relación entre los votos recolectados en la urna y los votos que serán desencriptados al eliminar la conexión entre el voto y el hash de la credencial del votante. Eso se realiza al barajar los votos y Re-encriptándolos y además generando prueba matemática de mezcla correcta y una desencriptación verificable.
3. Una vez que las boletas esta mezcladas, estas están listas para ser desencriptadas. En el proceso de desencriptación, los miembros que tienen las partes de la llave privada de desencriptación deben de reunirse para ensamblarla. Este proceso también produce prueba matemática de que el contenido obtenido luego de la desencriptación es exactamente el mismo que está en la boleta encriptada.
4. Una vez que las boletas son desencriptadas, estas son introducidas en el PRCC, para que sean incluidas en el conteo.

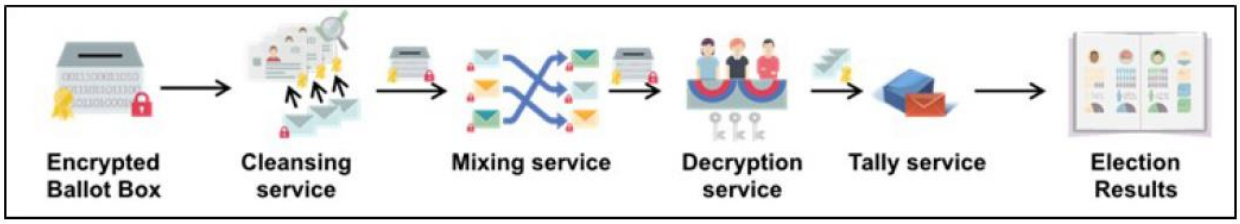


Figura 12: Sistema de Votación Electrónico iVote: Apertura de Urna

Fuente: (NSW Electoral Commission, 2019)

2.2 Cadena de Bloques

2.2.1. ¿Qué es una Cadena de Bloques?

Una cadena de bloques se visualiza como una base de datos compartida que almacena sus datos de manera descentraliza, lo que denota que la información que comprende es pública. Por la peculiar manera de guardar la información, es prácticamente imposible de corromper el sistema de información, haciendo la misma segura. Al respecto (Dolader Retamal, Bel Roig, & Muñoz Tapia) , afirma que:

"La blockchain permite implementar una base de datos distribuida, pública e inmutable basada en una secuencia creciente de bloques. Esta base de datos proporciona de forma intrínseca tolerancia a fallos en nodos, robustez frente a manipulación y al ser pública, transparencia. Los usos de esta tecnología son potencialmente inmensos y por ello se considera como una de las tecnologías con más potencial disruptivo de los últimos años".

De igual manera, otra opinión es la expuesta por (ASOBAMCARIA, 2017), señala que: "El Blockchain o cadena de bloques es un registro público de transacciones que se mantiene mediante una red distribuida de computadores, que no requiere respaldo de ninguna autoridad central o una tercera parte y que ofrece un esquema transaccional libre de intermediarios, gracias al uso de algoritmos criptográficos. Esta tecnología, que va más allá de las criptomonedas, promete transformar la forma en que se intercambia valor. La agilidad y seguridad al administrar la identidad de los actores en la red, rastrear los activos intercambiados y la facilidad con la que se puede llevar a cabo el control y verificación de los contratos, plantea una disminución fundamental de costos y una reducción sustancial de la incertidumbre en las transacciones."

2.2.2. Bloque Inicial

El bloque principal de la cadena es llamado "*Bloque Génesis*", el cual es la base. El Bloque Genesis es la raíz de toda la cadena de bloque, a partir de esta se construye toda la arquitectura. Cada bloque tiene un hash del anterior, en el caso del bloque génesis contiene el hash 0, debido a que no existe algún otro bloque que lo antecede. Posteriormente del bloque inicial, los de más hash irán creciendo a medida que se vaya agregando nuevos bloques.

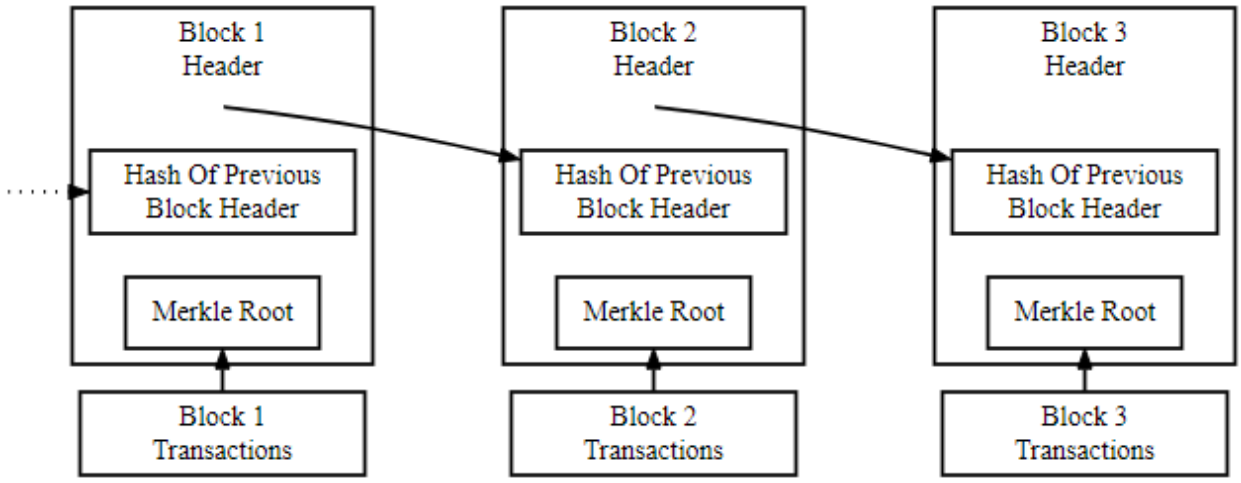


Figura 13: Esquema de la cadena de bloques

Fuente: (Bitcoin Organization, 2019)

2.2.3. Nodos

Un nodo es una computadora conectada a la red que tiene como objetivo salvaguardar y repartir una copia actualizada en tiempo real de la cadena de bloques y esto se hace a través de un software especializado. Además de salvaguardar y repartir su propósito es verificar la validez de la data (Comprobar que no existe la modificación de un hash dentro de un bloque). Para que la data que contiene un nodo sea

confirmada, pasa por un procedimiento criptográfico con el propósito de validar que no existe problema alguno con el mismo.

Luego que el nodo pase por el proceso criptográfico y sea correcto, este se incrusta a la cadena y replica la información en cada uno de los nodos conectados a la red. Los nodos guardan una copia de seguridad de cada información que distribuyen, lo cual hace que nunca se pierda la información, siempre se mantienen los datos sincronizados en la red incluso si uno o más de los nodos dejase de funcionar.

Según (Basantes, 2018) “El sistema descentralizado en la red P2P involucra algunos criterios:

- Cada nodo es el encargado de verificar independientemente cada transacción, teniendo en cuenta su correcta sintaxis y estructura de los datos; el tamaño de la transacción en bytes, número de operaciones y revisar el hash apropiado para la transacción.
- El rol de los nodos mineros es añadir las transacciones a los nuevos bloques por medio del algoritmo de consenso llamado prueba de trabajo.
- Cada nodo es delegado de comprobar los nuevos bloques creados y colocar estos dentro de la cadena de bloques.

Una transacción en Blockchain se propaga en broadcast a toda la red P2P, donde cada nodo de la red escucha las transacciones y las intercambia con sus nodos vecinos. Este proceso de broadcast permite que todos los nodos de la red sepan la información que está siendo validada y posteriormente sea añadida en el ledger.

Los nodos son iguales, pero de acuerdo a la función que cumplen pueden ser nodos simples, encargados de validar, propagar las transacciones y actualizar la copia

de la cadena entre sus vecinos sin requerir permisos externos; y nodos especiales, mineros, encargados de crear nuevas transacciones o bloques, en base al algoritmo de prueba de trabajo y su posterior propagación al resto de la red, mantienen también una copia completa de la cadena."

2.2.4. Estructura del Bloque

Cada bloque en la cadena está constituido por una cabecera y almacena una lista de transacciones. Está conformado por un conjunto de campos que se ilustra en la tabla número 1. Además, dentro de la cabecera contiene unas series de campo como se muestra en el cuadro número 2.

Campo	**Descripción**
Magic No.	Valor establecido siempre a 0xD9B4BEF9
Blocksize	Numero de bytes que siguen, hasta el final del bloque
Transaction counter	Cabecera con metainformación sobre el bloque y la cadena
Transaction	Número de transacciones contenidas en el bloque

Tabla 1: Campos de un bloque

Fuente: (INTECO, 2014)

Campo	Descripción
Version	Versión de bloque
hashPrevBlock	Hash del bloque anterior
hashMerkleRoot	Hash de la raíz del árbol Merkle
Time	Marca de tiempo de creación del bloque
Bits	Especificación de la complejidad del bloque
Nonce	Nonce que resuelve la prueba de trabajo

Tabla 2: Cabecera de un bloque de Bitcoin

Fuente: (INTECO, 2014)

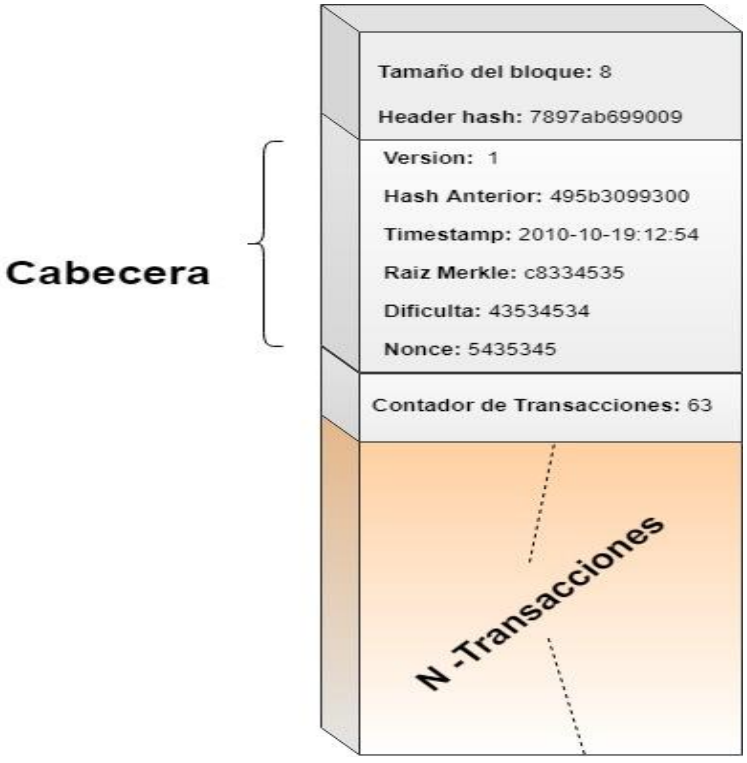


Figura 13: Estructura de un bloque

Fuente: Elaboración propia

2.2.5. Consenso

En los sistemas basados en cadena de bloques, se presenta un escenario llamado: problemas de consenso. Estos problemas de consenso se producen cuando varios nodos producen un bloque casi al mismo tiempo y como resultado se produce una bifurcación en la cadena de bloques.

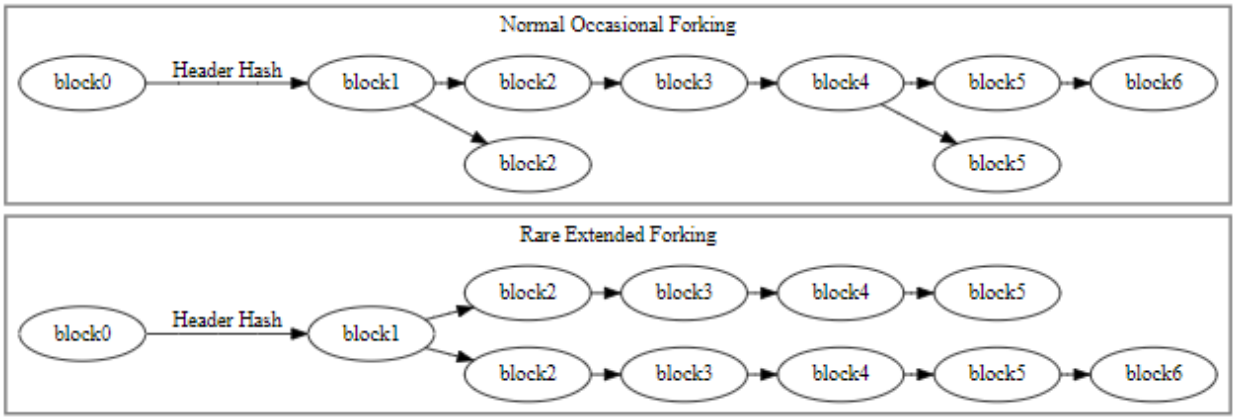


Figura 14: Bifurcación o Fork de cadena de bloques

Fuente: (Bitcoin Organization, 2019)

Cuando la cadena de bloques se bifurca, algunos bloques tienen la misma "altura". Altura en este contexto significa; el número de bloques entre el bloque inicial o bloque génesis y el mismo.

Cuando un software para minar o "miner" produce bloques simultáneamente y los agrega a la cadena de bloques, cada nodo decide cuál de los bloques acepta. Usualmente los nodos eligen el primer bloque que reciban.

Eventualmente un miner produce otro bloque el cual es agregado a una de las bifurcaciones que tienen los nodos y dependiendo de su poder de procesamiento una rama de la cadena de bloques obtiene más bloques agregados a su cola. Cuando esto sucede los nodos descartan la rama más corta.

2.2.6. Billeteras

Las billeteras, también conocidos como monederos o Wallets en inglés, son las referencias a las cuales se les transfiere fondos. Cada usuario de las cripto-moneda debe de tener una billetera donde recibir pagos. (INTECO, 2014)

Técnicamente, las billeteras son una dirección que se compone de un par de llaves ECDSA, una pública y otra privada. Esta dirección se genera a partir del hash de la llave pública a la cual se le concatena una suma de verificación y su resultado es codificado en base 58. (INTECO, 2014)

Las aplicaciones billeteras son programas que generan llaves públicas donde recibir los pagos y usan las llaves privadas para gastar o utilizar los fondos. (Bitcoin Organization, 2019)

Las aplicaciones billeteras se encargan de:

1. Generan llaves privadas y derivan llaves públicas a partir de esta.
2. Distribuye llaves públicas, monitorea los pagos realizados a esas llaves, crea y firma las transacciones para utilizar los fondos obtenidos en esas llaves.
3. Distribuye las transacciones ya firmadas a través de la red de nodos.

Existen billeteras que realizan todas estas tareas, sin embargo, a pesar de que sea conveniente que una aplicación de billetera realice todas estas tareas, también se crean brechas de seguridad. Por esto existen billeteras que solo realizan algunas de estas tareas.

Estas billeteras se clasifican en:

Billeteras de solo firma (Signing-Only Wallets): Para incrementar la seguridad, las llaves privadas son generadas y almacenadas en un programa aislado en un ambiente más seguro. Estas billeteras de solo firma funcionan en conjunto con billeteras conectadas a internet que interactúan con la red de nodos. (Bitcoin Organization, 2019)

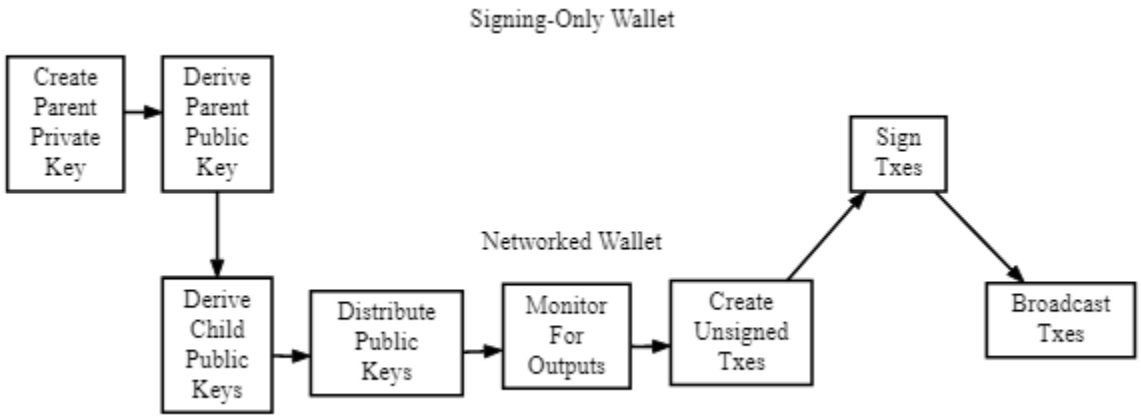


Figura 15: Operación de una billetera de solo firma

Fuente: (Bitcoin Organization, 2019)

Billeteras Físicas: Son dispositivos cuyo único propósito es el de ejecutar una billetera de solo firma. Al solo ejecutar este programa, les permite prescindir de un sistema operativo, lo cual también elimina muchas fallas de seguridad que normalmente los sistemas operativos conllevan. Estas tienen puertos que permiten conectarse con otros dispositivos y transferir los datos necesarios para realizar una transacción, evitando que los usuarios tengan que transferir esos datos manualmente. (Bitcoin Organization, 2019)

Figura 16: Ledger Nano S, La primera billetera física

Fuente: (Ledger, 2019)

Billeteras de solo distribución: Estas aplicaciones billetera se ejecutan en ambientes difíciles de asegurar, tales como servidores web. Estas son diseñadas para distribuir llaves públicas y nada más.

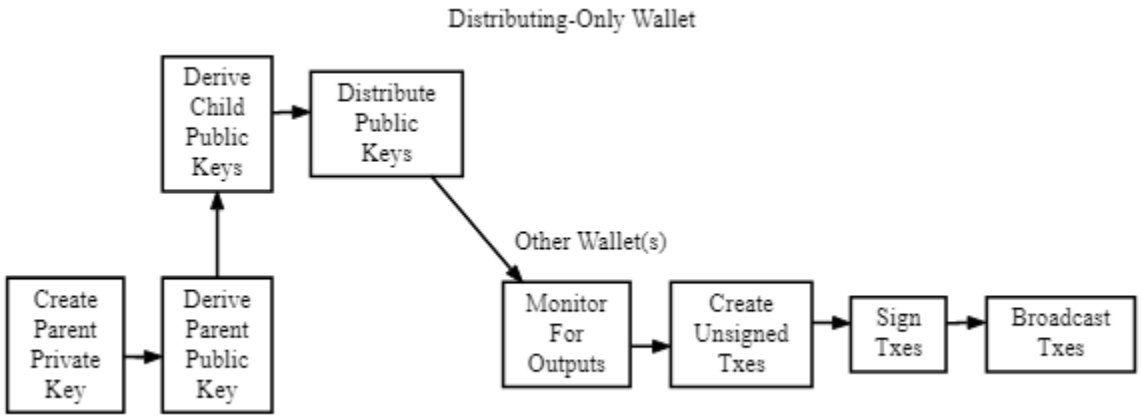


Figura 17: Operación de una billetera de sólo distribución

Fuente: (Bitcoin Organization, 2019)

2.3 Análisis y Diseño de Sistemas

A la hora de construir o desarrollar un sistema de información o software, es necesario contar con etapas claras, ya que el desarrollo del software es un proceso complejo y a medida que este va creciendo, la implementación de los posteriores cambios se va complicando también.

Por esto es necesario analizar bien el problema que el sistema pretende solucionar, las necesidades del cliente y las expectativas que tiene el cliente del software. Además, es necesario indicar como se desarrollará el software, es decir, indicar que técnicas, patrones de diseño, arquitectura y estándares se utilizaran para desarrollar el software.

En resumen, el análisis y diseño indican “que” se debe desarrollar y “como” debe desarrollarse, respectivamente.

2.3.1. Requisitos

Luego de la etapa de elicitación de requisitos, donde se obtienen las necesidades del cliente y que espera el cliente del sistema, se procede a documentar los requisitos.

Los requisitos son descripciones de lo que el sistema debe (y algunas veces no debe) hacer. Estos mayormente se dividen en funcionales y no funcionales. (Sommerville, 2011)

2.3.1.1. Funcionales

Los requisitos funcionales son enunciados sobre los servicios que el software debe de proveer, como debe reaccionar ante cierto tipo de entradas y de cómo debe comportarse en situaciones específicas. (Sommerville, 2011)

2.3.1.2. No Funcionales

Los requisitos no funcionales son restricciones y limitaciones sobre los servicios que ofrece el sistema. Estos afectan al sistema completo, en lugar de características puntuales del sistema. Estas limitaciones se suelen aplicar a los aspectos de seguridad e interfaz gráfica, pero también a los aspectos del desarrollo del proyecto, como, por ejemplo: el lenguaje de programación a utilizar, la tecnología de la base de datos, etc.. (Sommerville, 2011)

2.3.2. Casos de Uso

Los casos de uso identifican a los actores implicados en una interacción, y nombre el tipo de interacción. Describe también las acciones que dichos actores

pueden realizar y las responsabilidades de estos. Los casos de uso se suelen documentar en forma gráfica mediante los diagramas de casos de uso de UML, pero también existen las especificaciones de casos de uso.

2.3.2.1. Diagrama de Caso de Uso

Es un diagrama de alto nivel, que muestra las interacciones de los actores de un sistema y las funciones del sistema. Es un diagrama que permite a los usuarios y clientes que no poseen conocimiento técnico, entender que hará el sistema.

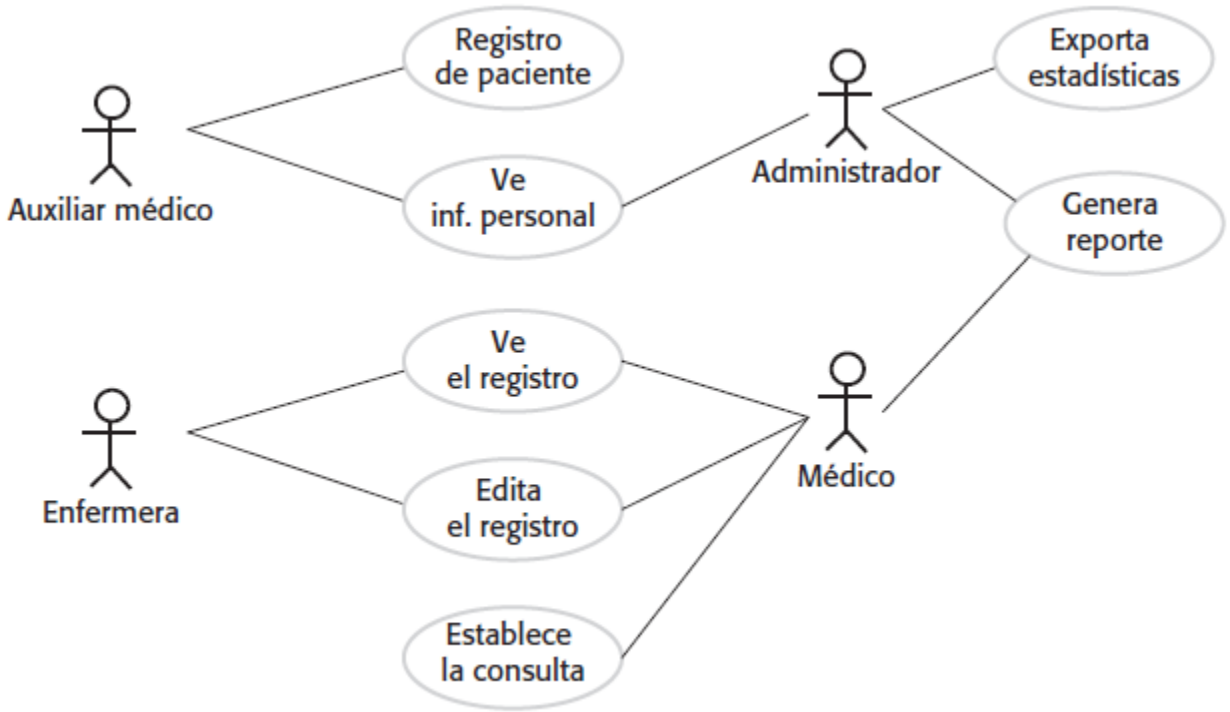


Figura 18: Ejemplo de diagrama de Caso de Uso

Fuente: (Sommerville, 2011)

2.3.2.2. Especificación de Caso de Uso

Si bien los diagramas de caso de uso son diagramas de alto nivel, estos carecen de detalles importantes para los usuarios con conocimiento más técnico. Esto hace necesario que se describan los casos de uso de una forma más estructurada y detallada. Para esto último se introdujo las especificaciones de casos de uso o escenarios de casos de uso.

Las especificaciones de casos de uso no solo describen los actores, relaciones y funcionalidades del sistema, sino, también, las condiciones, los flujos, tanto estándar, alternativos o de error.

Use Case Name	The name of the use case. It usually starts with a verb.	
Brief Description	Summarizes the use case in a short paragraph.	
Precondition	What should be true before the use case is executed.	
Primary Actor	The actor which initiates the use case.	
Secondary Actors	Other actors the system relies on to accomplish the services of the use case.	
Dependency	Include and extend relationships to other use cases.	
Generalization	Generalization relationships to other use cases.	
Basic Flow	Specifies the main successful path, also called "happy path".	
	Steps (numbered)	Flow of events.
	Postcondition	What should be true after the basic flow executes.
Specific Alternative Flows	Applies to one specific step of the basic flow.	
	RFS	A reference flow step number where flow branches from.
	Steps (numbered)	Flow of events.
	Postcondition	What should be true after the alternative flow executes.
Global Alternative Flows	Applies to all the steps of the basic flow.	
	Steps (numbered)	Flow of events.
	Postcondition	What should be true after the alternative flow executes.
Bounded Alternative Flows	Applies to more than one step of the basic flow, but not all of them.	
	RFS	A list of reference flow steps where flow branches from.
	Steps (numbered)	Flow of events.
	Postcondition	What should be true after the alternative flow executes.

Figura 19: Ejemplo de especificación de caso de uso

Fuente: (Tools: zen-tools.com, n.d.)

2.3.3. Diagramas de Modelado de Sistemas

Los diagramas de modelados de sistemas permiten visualizar la arquitectura, diseño y comportamiento de un sistema. Estos son expresados usualmente utilizando UML, pero también se puede expresar con matemáticamente con un lenguaje formal.

2.3.3.1. Diagrama de Actividad

Los diagramas de actividad muestran una visión simplificada de durante una operación o proceso. Los diagramas de actividad tienen cierta similitud con los diagramas de flujo, pero estos son más abstractos y simples que los últimos. (Schmuller)

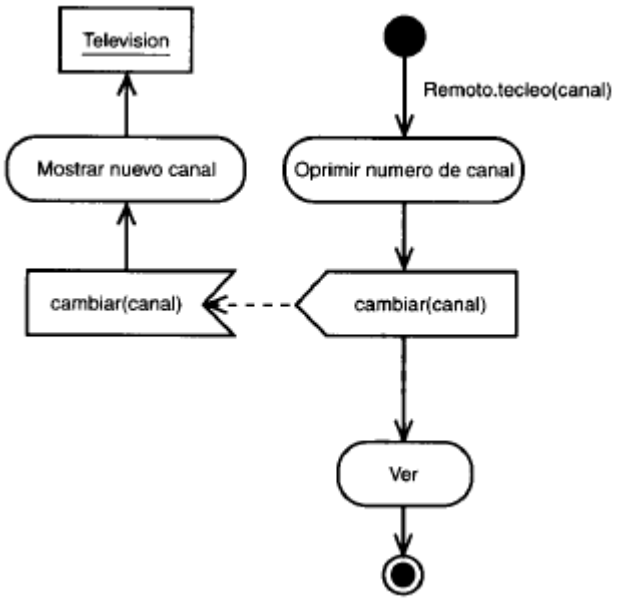


Figura 20: Ejemplo de un Diagrama de Actividad

Fuente: (Schmuller)

2.3.3.2. Diagramas de Secuencias

Los diagramas de secuencia describen las interacciones de los objetos, pero con la dimensión del tiempo. Estos diagramas muestran el comportamiento de los objetos a

través del tiempo, el orden de las llamadas de los métodos

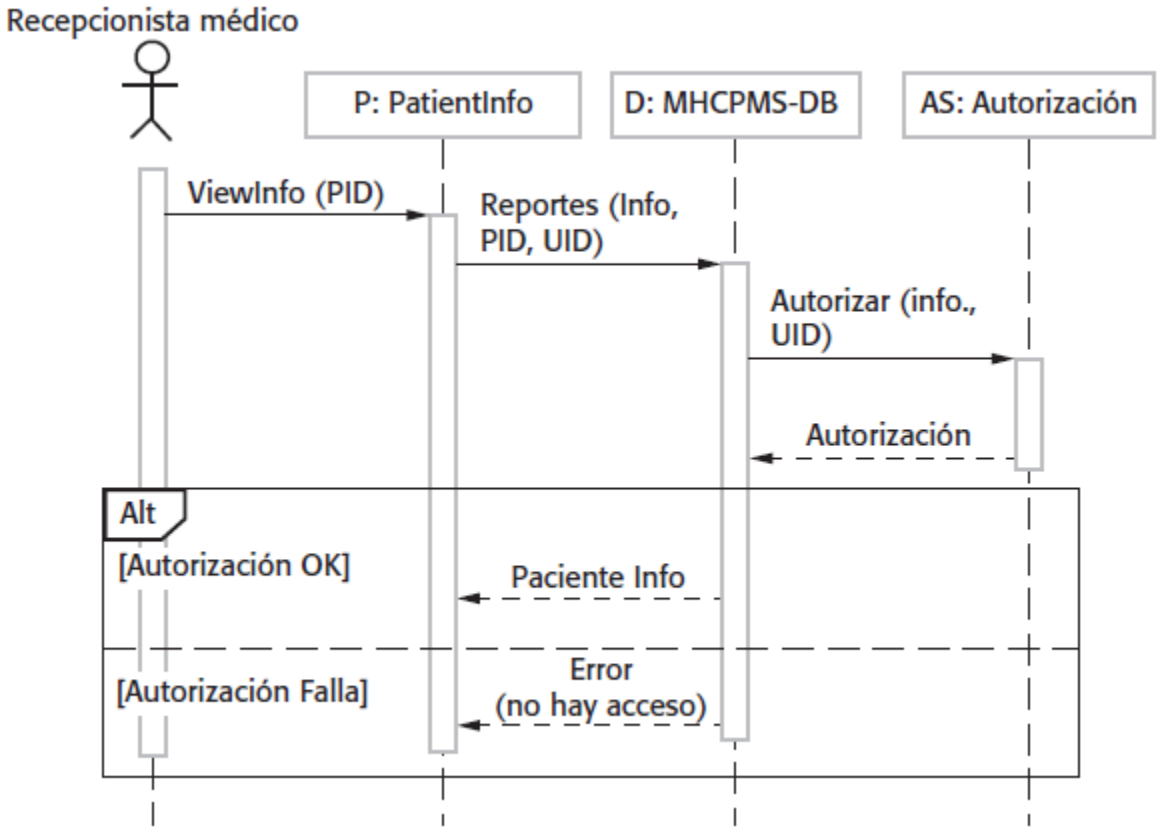


Figura 21: Ejemplo de un Diagrama de Secuencia

Fuente: (Sommerville, 2011)

2.3.3.3. Diagrama de Estados

Los diagramas de estado muestran cómo cambia el estado de los objetos a través del tiempo. Estos muestran los posibles estados que puede tomar un sistema, así como los eventos que producen dicho cambio. Los cambios pueden ser producidos por eventos externos al sistema o por el transcurrir del tiempo.

.

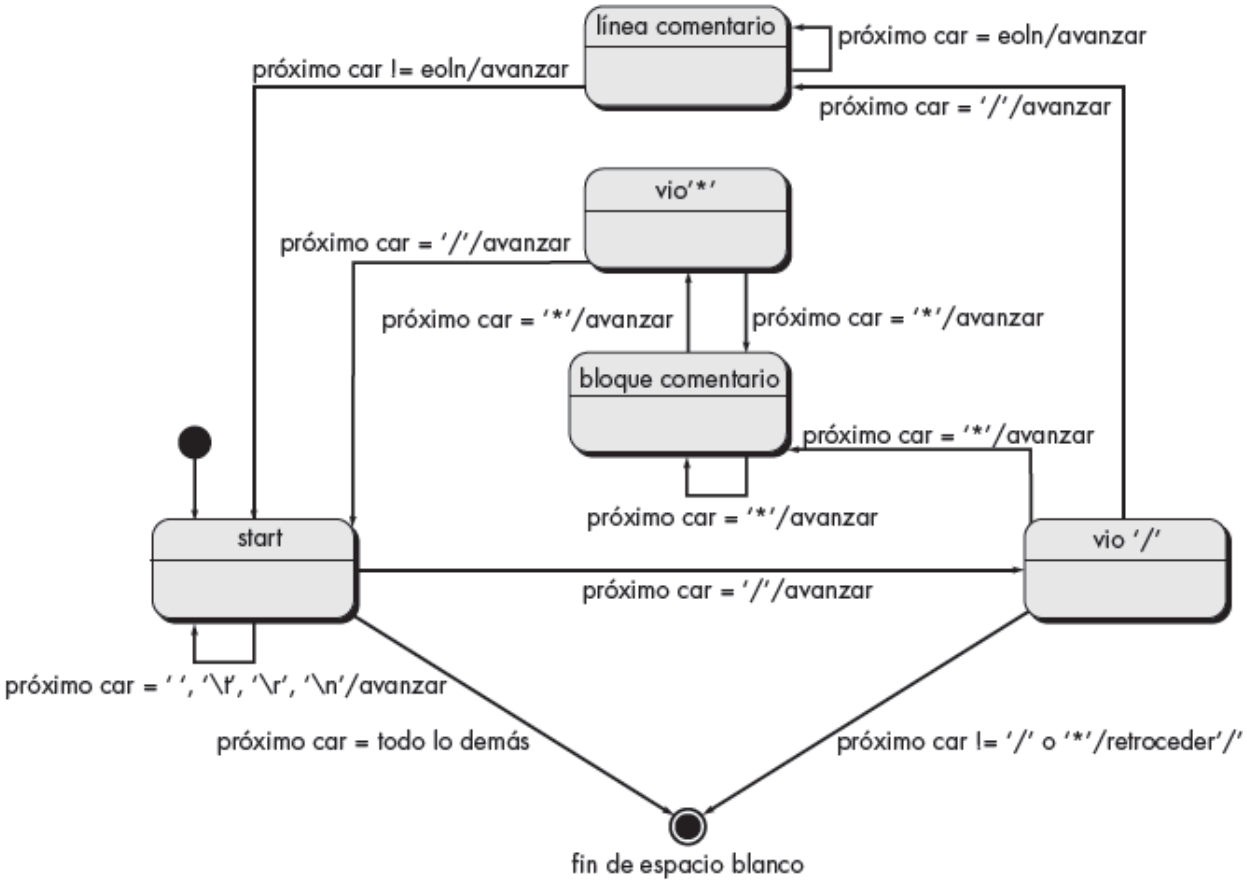


Figura 22: Ejemplo de diagrama de estado

Fuente: (Pressman, 2010)

Los estados se pueden subdividir en secciones tal y como las clases en un diagrama de clases. Estos se pueden subdividir en tres secciones: Nombre, Variables, Actividades.

En los diagramas de estado, los estados pueden estar compuestos de subastados. Esto permite agregar más detalles a los diagramas de estado. Es posible también representar operaciones concurrentes en los subestados. (Schmuller)

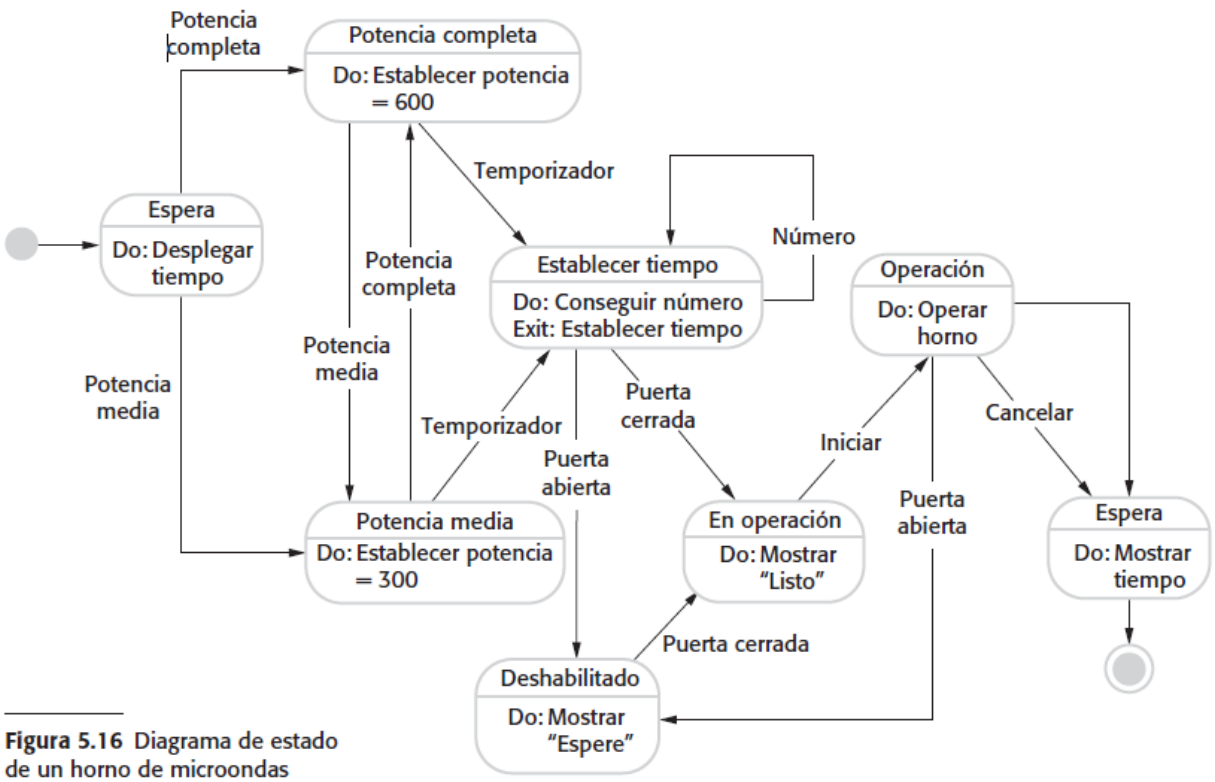


Figura 5.16 Diagrama de estado de un horno de microondas

Figura 23: Diagrama de estado con subdivisiones de Nombre y Actividades

Fuente: (Sommerville, 2011)

2.3.3.4. Diagrama de Clases

Los diagramas de clases se pueden utilizar para representar las clases y sus asociaciones con otras clases en un sistema orientado a objetos. En UML las clases se representan con un rectángulo que tiene tres secciones: Nombre de la clase, atributos y métodos u operaciones.

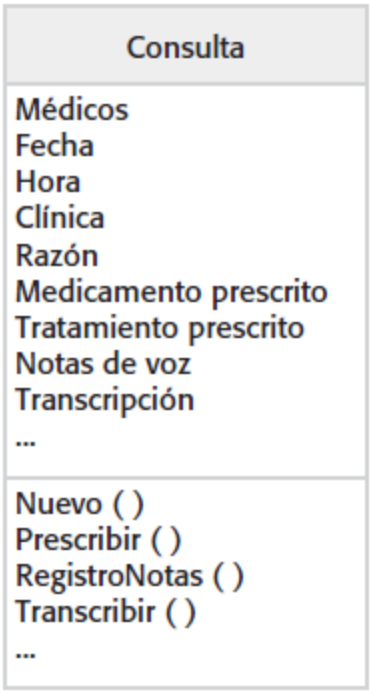


Figura 24: Representación de una Clase en UML

Fuente: (Sommerville, 2011)

Las asociaciones son líneas con algunas características especiales. Estas indican que tipo de relación tienen las clases entre sí.

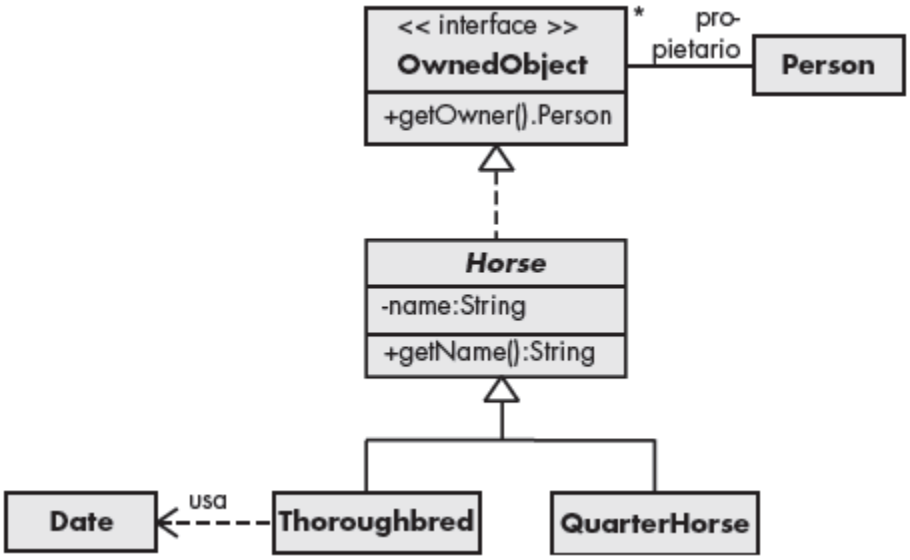


Figura 25: Diagrama de clases con implementación de interfaz y herencia

Fuente: (Sommerville, 2011)

En la Figura 20 se muestra un ejemplo de un diagrama con relaciones de diferentes tipos

2.3.3.5. Diagrama de Base de Datos Relacional

Los diagramas de modelos de bases de datos relacionales expresan el diseño de la base de datos. Estos indican expresan las reglas del negocio de manera gráfica.

Los diagramas de base de datos relacional expresan entidades y relaciones. Las entidades son cualquier objeto o evento sobre el que se pueda captar información. Estas entidades se obtienen de estudiar y comprender las reglas de negocio.

Las relaciones son los equivalentes a las asociaciones en un diagrama de clases. Las relaciones tienen una multiplicidad que indica el número de entidades que se pueden relacionar. Según la multiplicidad hay tres tipos de relaciones:

1. Uno a no (1:1)
2. Uno a muchos (1:N)
3. Muchos a muchos (M:N)

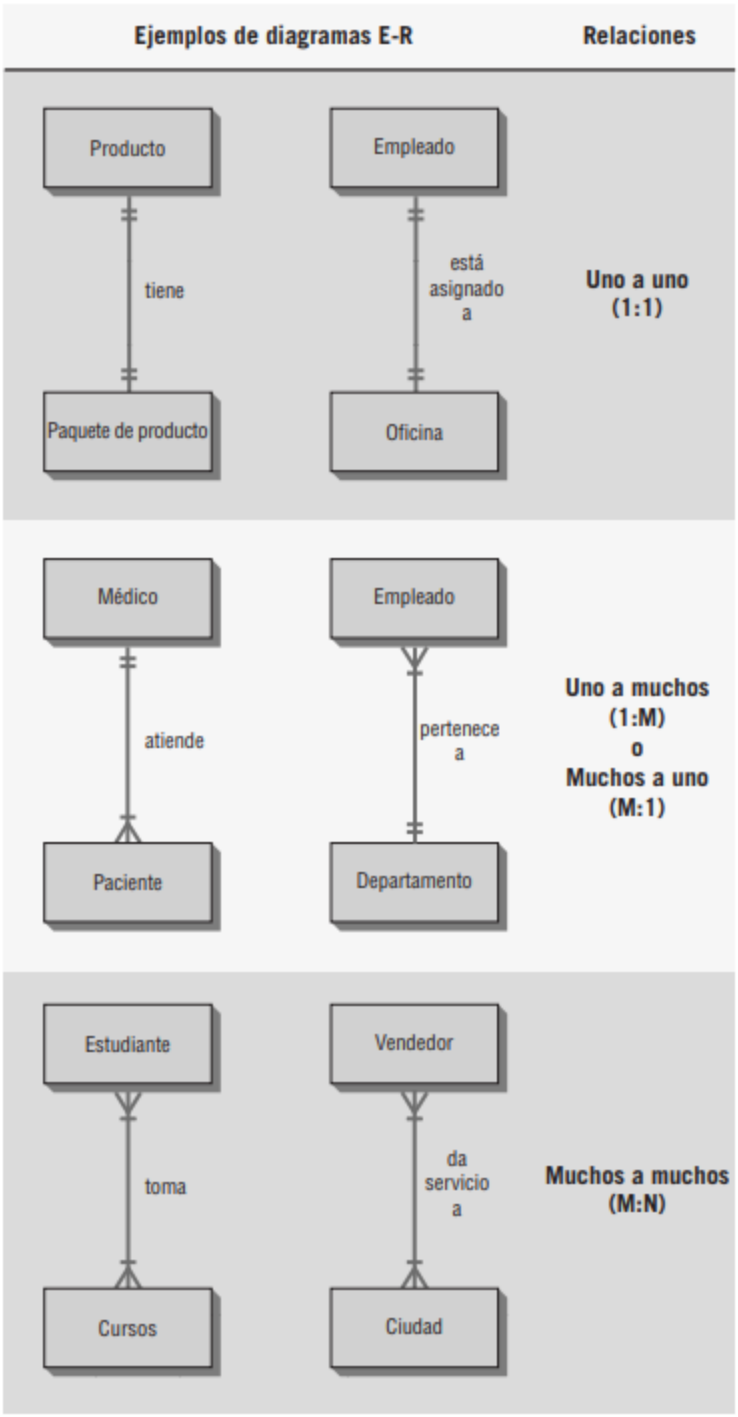


Figura 26: Tipos de relaciones entre entidades

Fuentes: (Kenneth E Kendall, 2011)

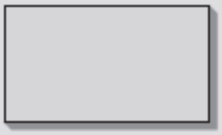
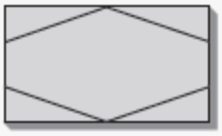
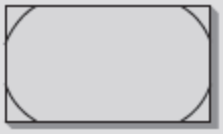
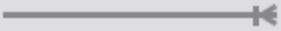
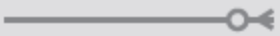
Símbolo	Explicación oficial	Lo que realmente significa
	Entidad	Una clase de personas, lugares o cosas
	Entidad asociativa	Se utiliza para unir dos entidades
	Entidad atributiva	Se usa para repetir grupos
	Relación a 1	Exactamente uno
	Relación a muchos	Uno o más
	Relación a 0 o 1	Sólo cero o uno
	Relación a 0 o más	Puede ser cero, uno o más
	Relación a más de 1	Mayor de uno

Figura 27: Simbología de diagrama de Entidad-Relación

Fuente: (Kenneth E Kendall, 2011)

Las reglas de Normalización permiten eliminar la redundancia de datos y reducir la complejidad de las tablas al crear tablas más pequeñas y simples y establecer relaciones entre estas.

En la normalización existen las formas normales de una tabla. Son cinco formas normales (1NF,2NF,3NF, BCNF,4NF), de estas las más utilizadas son las primeras tres.

Para alcanzar la 3NF se deben agotar tres pasos:

1. Eliminación de grupos repetidos
2. Eliminación de dependencias parciales
3. Eliminación de dependencias transitivas

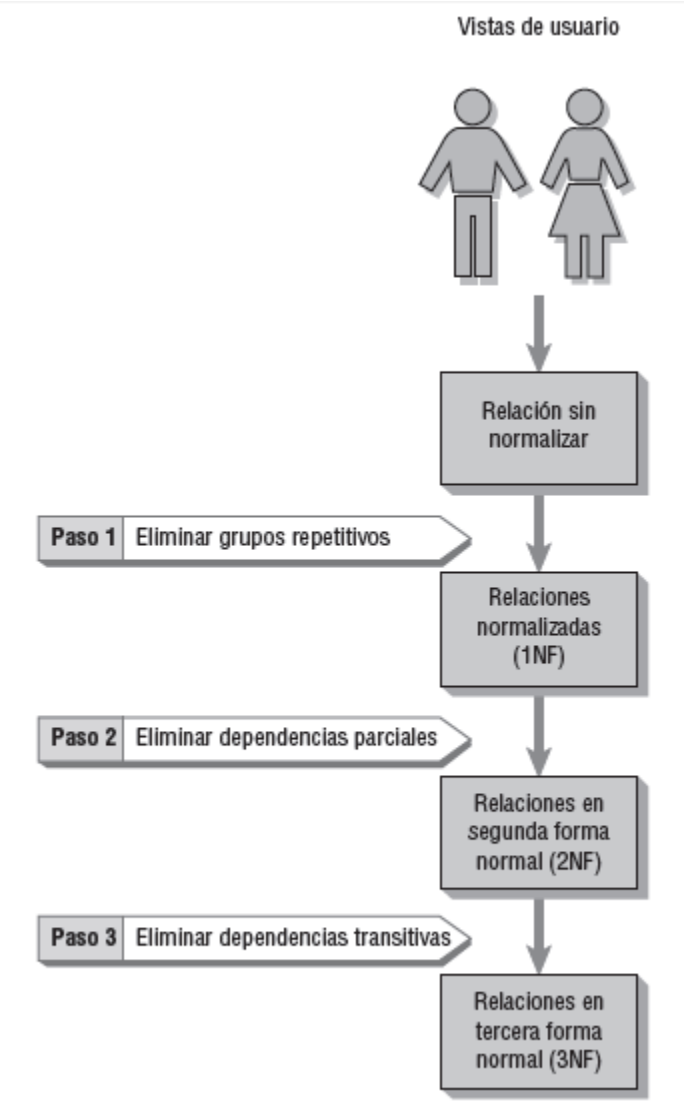


Figura 28: Reglas de normalización

Fuente: (Kenneth E Kendall, 2011)

2.3.4. Patrones de Diseño y Arquitectónico.

El Diseño arquitectónico trata sobre cómo debe organizarse un sistema y sobre cómo tiene que diseñarse la estructura global de un sistema. En esta etapa se identifican los principales componentes estructurales y como estos se relacionan entre sí. (Sommerville, 2011)

Los patrones arquitectónicos son descripciones abstractas estilizadas de buenas prácticas, que se han probado y utilizado con éxito en diferentes sistemas. Estos deben incluir información de cuándo debe o no debe utilizarse, así como sus debilidades y fortalezas. (Sommerville, 2011)

Algunos de los patrones arquitectónicos más utilizados son:

Arquitectura en Capas: provee desacoplamiento al apilar capas de abstracción de funcionalidades que solo son accesibles a través de interfaces. Las capas pueden cambiar su implementación sin afectar las capas inferiores o superiores, siempre y cuando su interfaz no cambie. Sin embargo, para una aplicación de tres capas A, B y C, la capa A no puede acceder directamente a la capa C, sino es a través de la capa B.

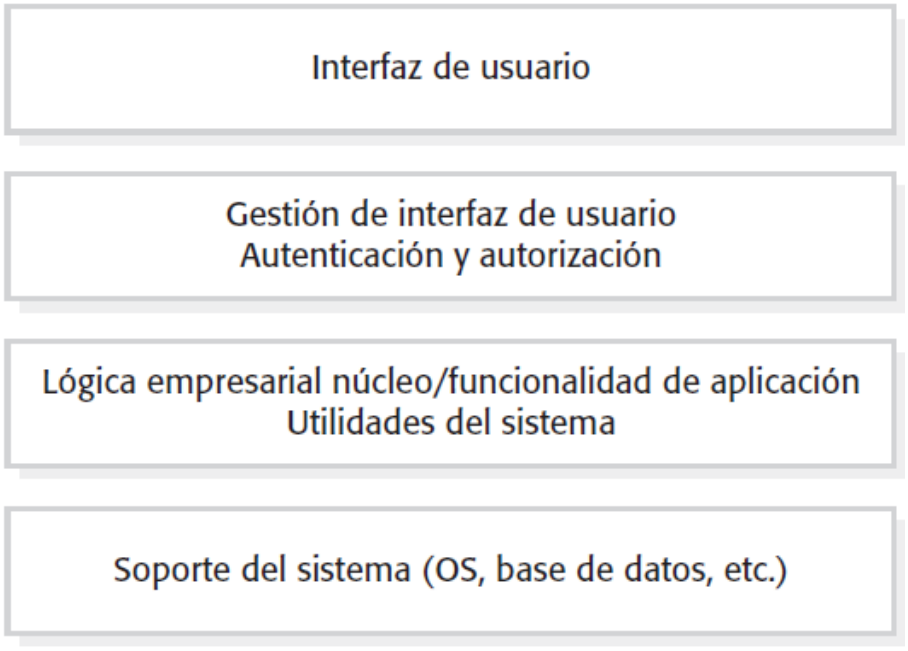


Figura 29: Arquitectura en capa genérica

Fuente: (Sommerville, 2011)

Arquitectura de Repositorio: establece que todas las interacciones entre los componentes se deben realizar a través de un repositorio compartido entre los mismos.

Este tipo de arquitectura es ideal para sistemas en que la inclusión de los datos activa una acción o herramienta o cuando se genera una gran cantidad de datos que deban ser guardados por largo tiempo.

En este tipo de sistemas el repositorio es el corazón del sistema, si este presenta problemas el sistema se detiene, además resulta difícil distribuir el repositorio en varias computadoras.

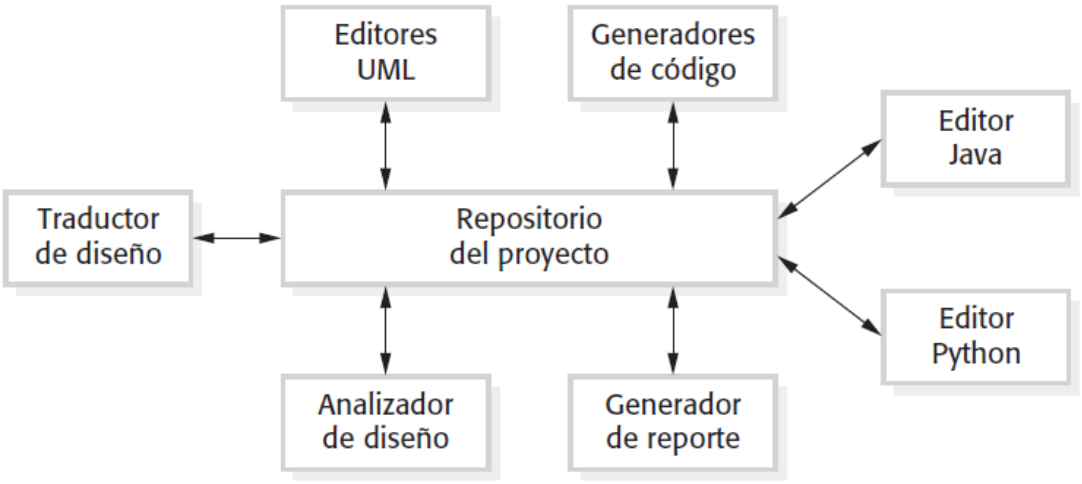


Figura 30: Arquitectura de repositorio para un IDE

Fuente: (Sommerville, 2011)

Arquitectura cliente-servidor: La funcionalidad del sistema es provista por servicios y estos son entregados por servidores. Los clientes hacen uso de los servicios.

Mayormente utilizado cuando se necesita acceder a una funcionalidad desde varias ubicaciones. También cuando la carga del sistema es variable.

El cambio o actualización a los servicios no afecta a los clientes o servidores, sin embargo, los servidores son un punto central de falla, si el servicio es interrumpido, el sistema detiene su ejecución. Por la centralización, los servidores son susceptibles a ataques de negación de servicio distribuidos (DDoS). (Sommerville, 2011)

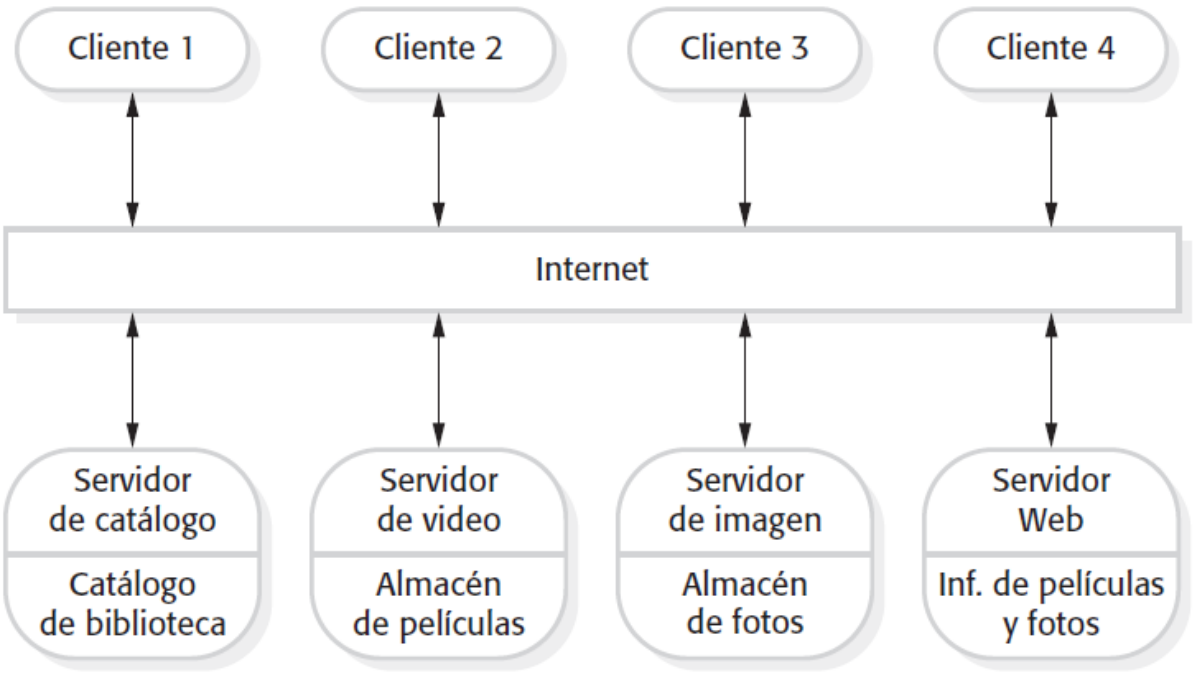


Figura 31: Arquitectura cliente-servidor

Fuente: (Sommerville, 2011)

Arquitectura de tubería y filtro: Consiste en enviar los datos a través de canales conocidos como tuberías a componentes que realizan alguna transformación en los datos y luego producen una salida diferente, estos últimos son conocidos como filtros.

Este patrón arquitectónico es de fácil comprensión y soporta reutilización de transformación. Se puede implementar en forma secuencial o concurrente.

Una desventaja de este patrón es que, si el formato de entrada no es compatible con la salida de un filtro anterior, el funcionamiento se puede detener o peor aún puede provocar salidas inconsistentes (GIGO).

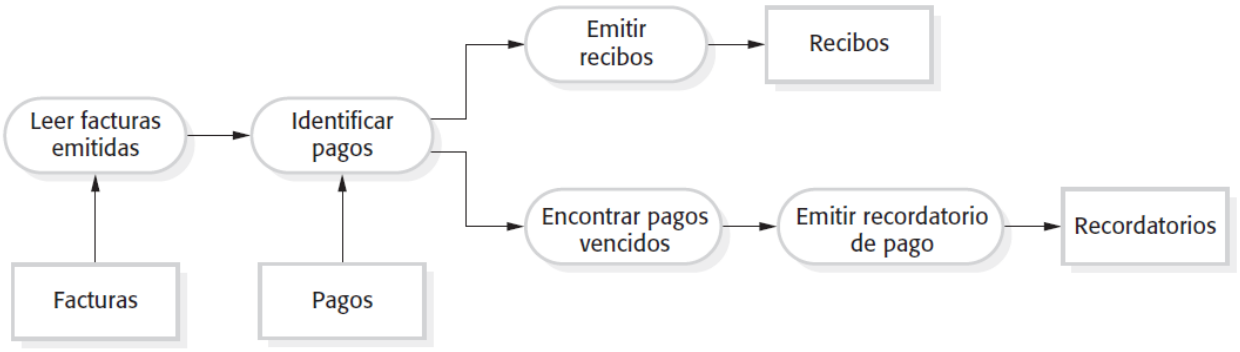


Figura 32: Arquitectura de tubería y filtro

Fuente: (Sommerville, 2011)

Los patrones de diseño fueron introducidos por el Arquitecto Christopher Alexander, quien sugirió que existían ciertos patrones comunes de diseño de edificaciones. Esta idea fue extrapolada al ámbito de la ingeniería de software, para describir soluciones comunes, probadas y que funcionaban con éxito.

Los patrones de diseño resuelven un problema que se repite a la hora de implementar un sistema, el utilizarlos resuelve dicho problema sin tener que “reinventar la rueda”, al reutilizar los conocimientos de los expertos.

Un patrón es una descripción del problema y la solución que este emplea al mismo. No es una especificación exhaustiva.

La mayoría de los patrones de diseño solo son aplicables a los sistemas desarrollados utilizando el paradigma de orientación a objetos (OO). Los patrones explotan cada uno de los cuatro pilares de la orientación a objetos: Herencia, Encapsulación, Abstracción y Polimorfismo.

Erich Gamma y sus colaboradores en (Erich Gamma, 1998), describen 23 patrones de diseño, muchos de los cuales ellos mismos tuvieron que bautizar.

El catálogo de patrones de diseño que Gamma muestra, son:

1. **Abstract Factory:** Provee una interfaz para la creación de familias de objetos relacionados o independientes, sin especificar sus clases concretas.
2. **Builder:** Separa la creación de objetos complejos de su representación de forma que con el mismo proceso de construcción se puedan crear diferentes representaciones.
3. **Factory Method:** Define una interfaz para la creación de un objeto, pero deja que las subclases decidir cual clase instanciar. El Factory Method deja que la clase delegue la instanciación a las subclases.
4. **Prototype:** Especifica el tipo de objeto a crear utilizando un prototipo de instancia, y crea nuevos objetos al copiar este prototipo.
5. **Singleton:** Se asegura de que solo existe una instancia, y provee un punto de acceso global a la instancia.
6. **Adapter:** Convierte la interfaz de una clase en una interfaz que el cliente espera. Adapter permite que clases que no pueden funcionar juntas porque sus interfaces son diferentes, funcionen en conjunto.
7. **Bridge:** Desacopla una abstracción de su implementación de modo que estas puedan cambiar independientemente.
8. **Composite:** Permite tratar un conjunto de objetos como uno. Composite permite representar objetos como una estructura de árbol de jerarquía.
9. **Decorator:** Agrega responsabilidades adicionales a un objeto de forma dinámica. Decorator provee una alternativa flexible a la herencia para extender funcionalidad.

10. **Facade:** Provee una única interfaz para acceder a un conjunto de interfaces en un subsistema. Facade define a una interfaz de alto nivel que permite el uso de un subsistema más fácil.
11. **Flyweight:** Soporta un gran número de objetos bien definidos eficientemente, mediante el compatir.
12. **Proxy:** Proporciona un sustituto para otro objeto para controlar el acceso a él.
13. **Change of Responsability:** Evita el acoplamiento del remitente de una petición a un receptor al permitir que otros objetos manipulen la petición. Encola los objetos receptores en cadena y pasa la petición a través de la cadena hasta que un objeto lo manipule.
14. **Command:** Encapsula una petición como un objeto, permitiendo parametrizar clientes con diferentes peticiones, colas o peticiones de logueo, y soporte para operaciones reversibles.
15. **Interperter:** Dado un lenguaje, define una representación de su gramática junto con un intérprete que usa la representación para interpretar sentencias en ese lenguaje.
16. **Iterator:** Provee una forma de acceder elementos de un objeto agregado secuencialmente sin exponer su representación interna.
17. **Mediator:** Define un objeto que encapsula como un conjunto de objetos interactúan. Mediator promueve desacoplamiento al evitar que los objetos se referencien explícitamente, y permite que su interacción varíe independientemente

18. **Memento:** Sin violar la encapsulación, captura y externaliza el estado interno de un objeto para que el objeto pueda ser restaurado a este estado más adelanto.
19. **Observer:** Define una relación de uno a muchos entre objetos para que cuando un objeto cambia su estado, todos sus dependientes son notificados y actualizados automáticamente.
20. **State:** Permite a un objeto alterar su comportamiento cuando su estado interno cambia. Parecerá que el objeto cambio su clase.
21. **Strategy:** Define una familia de algoritmos, encapsula cada uno, y los hace intercambiable. Strategy permite que el algoritmo varíe independientemente de los clientes que los usan.
22. **Template Method:** Define la estructura de un algoritmo en una operación, delegando algunos pasos a las subclases. Template Method permite que las subclases redefinan ciertos pasos de un algoritmo sin cambiar la estructura del algoritmo.
23. **Visitor:** Representa una operación a realizar sobre los elementos de un objeto. Visitor permite definir una nueva operación sin cambiar las clases de los elementos sobre los cuales opera.

CAPÍTULO III: SITUACION ACTUAL DEL SISTEMA DE VOTACIÓN EN REPÚBLICA DOMINICANA Y SISTEMAS DE VOTACIÓN ELECTRÓNICOS UTILIZADOS

3.1. Junta Central Electoral

Constituida en el año 1923, con el mandato de establecer las elecciones en República Dominicana. Sus primeras décadas estuvieron marcadas por un sistema dominante que sofoco al país por más de 30 años. A partir del 1962 comienza un robustecimiento institucional constante que reflecta sus grandes aportes a la democracia, a la identidad dominicana y a los derechos civiles y políticos. Posteriormente del desmoronamiento del absolutismo con 21 elecciones realizadas, la JCE ha desarrollado sus capacidades de gestión de procedimientos electorales logrando realizar una preferencia en la región con significativos objetivos de avances específicamente en los últimos 25 años.

Desde un padrón de 140,000 en el año 1924, 95 años después la JCE cuenta con un total de más de 6,700,00 electores y 16,224 colegios electorales. Y por primera vez este padrón podría obtener una cifra de 7,000,000 de electores en el año 2020 respaldando el voto y la intención política de la población dominicana. El tras paso de la cédula y el registro civil a la Junta Central Electoral (JCE) a partir de la década de los 90 esta institución tiene su identidad, el más valioso activo de cada ciudadano; de esta manera la JCE gestiona la custodia y protección de los miles de libros que comprenden en sus folios los diferentes eventos de la vida civil de muchas generaciones de dominicano; Además de constituir un área de servicio primordial para los ciudadanos.

En los últimos 5 años la JCE ha registrado el nacimiento de más de 1 millón 200 mil dominicanos y ha emitido más de 17 millones de actas que revelan: nacimientos, matrimonios, divorcios y defunciones. Estos servicios se han podido lograr gracias a los métodos de digitalización y automatización que la institución ha venido desarrollando

por casi 15 años, esos eventos se completan con lo más básico de la identidad ciudadana la cédula; la cual ha crecido para convertirse en la actualidad en un documento seguro que certifica el accionar de los ciudadanos y su derecho al voto.

Desde el 1994 la JCE ha emitido más de 8 millones de cédulas, solo desde 2014 más de 7 millones tienen la cédula nueva y más de 900 mil ciudadanos adoptaron cédula por primera vez. Luego de 95 años la JCE es una institución soberana y traslúcida con una infraestructura que va evolucionando con el tiempo encaminada a estar más próxima a los pobladores.

En la actualidad, por añadidura a su única cede central cuenta con la oficina central del estado civil en el centro de los héroes del distrito nacional, 158 Juntas Electorales esparcidas en todos los municipios del país, 165 oficialías del estado civil en todo territorio nacional, 63 delegaciones de oficialías civiles en hospitales,7 centros de regionales de servicios y legalizaciones,14 oficinas en el exterior para servicios a los dominicanos incluyendo a: Nueva York, Boston, Orlando, San Juan, Nueva Jersey, Miami, Philadelphia, Panama, Madrid, Zurich, Barcelona y Milan . Asimismo, cuenta con 180 Centros de cedulación fijos en toda el país y 3 centros móviles y 10 unidades móviles de declaraciones tardías; además de un centro fijo con un nuevo marco constitucional y bajo nueva gestión encabezada por su presidente El magistrado Julio Cesar Castaño Guzmán la JCE muestra un sostenido creciendo y fortaleciéndose en su obligación de preservar la identidad de los dominicanos y asegurar la democracia del país.

3.1.1. Estructura Organizacional

Figura 33: Organigrama de la Junta Central Electoral

Fuente: Junta Central Electoral

Las realización, organización y observancia de los procesos electorales, es llevado a cabo por los siguientes órganos electorales:

- La Junta Central Electoral (JCE).
- Las Juntas Electorales.
- Los Colegios Electorales.

La JCE es la máxima autoridad en materia electoral y los demás órganos responden a esta. La JCE está compuesta por dos Cámaras: Administrativa y Contenciosa Electoral.

Entre las atribuciones otorgadas a la JCE, están:

- Adoptar medidas que puedan resolver cualquier dificultad para la realización de los procesos electorales, Ofrecer mejores condiciones para que los ciudadanos aptos para ejercer el voto.
- Disponer de todos los materiales, útiles y equipos necesarios para la adecuada realización de las actividades ejecutadas en las juntas y colegios.

Las Juntas Electorales son órganos dependientes de la Junta Central Electoral. Estas se encargan de los procesos electorales realizados en los municipios que les corresponda. Estos distribuyen los materiales, útiles y equipos a los diferentes colegios de ese municipio, además es en estos donde se computan los resultados de los colegios del municipio.

Por otro lado, están los colegios electorales, las cuales sirven de asiento para las urnas donde los ciudadanos ejercen su derecho al voto. La JCE se encarga de crear dichos colegios, que en su mayoría utilizan los centros educativos para ejercer el sufragio.

3.2. Sistema Electoral de la Republica Dominicana

3.2.1. Ley Electoral

La ley fundamental que crea la JCE y sus dependencias es la Ley Electoral 275-97. En esta se establece las responsabilidades de la JCE, de las juntas electorales y de las responsabilidades de los colegios. Además, establece las condiciones bajo las cuales se pueden crear los partidos, así como las circunstancias de su eliminación.

Esta ley también establece los tiempos para realizar las elecciones, las disposiciones para asegurar el libre ejercicio del derecho a elegir, trata sobre el escrutinio en los colegios electorales, sobre el cómputo de los resultados, las relaciones de los municipios, sobre las anulaciones de las elecciones y también sobre las infracciones realizadas durante las elecciones.

3.2.2. Proceso de votación antes de los SVE

La apertura del proceso de votación inicia a las 6:00 a.m. después que la instalación del Colegio Electoral ha sido concluida. La ley Electoral 275-97 indica que no se podrá iniciar la votación antes de la hora establecida.

Antes de que los electores empiecen a votar se debe dejar que los miembros del colegio, los delegados, políticos y sus suplentes sean las primeras personas en depositar las boletas electorales en la urna correspondiente. Sebe tener encuentra que ciertas personas tienen privilegios para votar ya sea por el cargo que ocupa, por la condición física en que se encuentra o alguna situación especial.

Cuando es el turno de los electores, el segundo vocal tiene el deber de facilitar el paso y pausar las personas que van entrando como considere apropiado. La

cantidad de electores dentro del Colegio Electoral está relacionada con el espacio del establecimiento donde se encuentren.

En el instante que entre el elector debe de entregar la cedula al primer(a) vocal que lo estará esperando en la mesa para verificar que sea la entidad que dice ser y validar que no esté inhabilitado o alguna otra razón. En caso de que al elector se le imposibilite votar por algún inconveniente, los miembros tendrán la obligación de explicar porque se le impide votar.

Luego de verificar y validar al elector él presidente le entrega las boletas con un marcador para señalar a la entidad. Las boletas son entregadas con su correspondiente firma y selladas por el mismo. Enseguida el elector se dirige a la caseta para seleccionar el candidato preferencial. Luego el mismo va a las urnas que estarán en el centro del Colegio Electoral para indicar transparencia.

Después de marcar las boletas electorales los electores se dirigen al primer vocal para estampar sus huellas dactilares en el Padrón Electoral acoplado a su nombre. Inmediatamente el primer vocal tiñe el dedo del elector como muestrario de la votación y recibe su identificación marchándose del local.

3.3. SVE utilizados por la JCE

3.3.1. Dispositivo de Escaneo y Transmisión (EyT)

A partir del 2008 la JCE integro en un solo dispositivo, una pantalla táctil, un escáner, una impresora térmica, un lector de huellas y un lector de código de barras. Este dispositivo fue nombrado “EyT” por las siglas Escaneo y Transmisión.

Estos dispositivos fueron utilizados en las elecciones del 2010, en los diferentes recintos, en todo el territorio nacional.

Figura 20: Componentes de las Unidades EyT.

Fuente: (Junta Central Electoral, 2010)

Las unidades EyT facilitan la digitalización y transporte de las boletas para su tabuladas y contadas. Esto es logrado al escanear las boletas y luego la misma unidad transmite las imágenes de las boletas a través de una red móvil 3G. (Junta Central Electoral, 2019)

Las boletas luego de ser firmadas, selladas y plastificada durante el escrutinio manual, se procede a escanearlas para digitalizarlas. Una vez digitalizadas, las unidades EyT realizan los procesos de reconocimiento óptico de caracteres (OCR), reconocimiento inteligente de caracteres (ICR) y el reconocimiento óptico de marcas (OMR), para luego realizar una digitación ciega de dichas boletas.

3.3.1.1 Beneficios e Inconvenientes

Las unidades EyT reducían considerablemente los tiempos necesarios para el procesamiento y divulgación de los resultados. Utilizando las unidades EyT se elimina las largas filas para entregar las valijas a las Juntas Electorales.

Otros beneficios son:

1. Escaneo y digitalización de las actas desde los colegios.
2. Validación del acta escaneada.
3. Encriptación de imágenes a la hora de transmitirlas
4. Respaldo de las imágenes en dispositivos de almacenamiento USB.
5. Entrega inmediata de las imágenes de las actas a los centros de cómputos de los partidos.

Entre las posibles desventajas de las unidades EyT, están:

- Baterías de baja capacidad, solo tiene energía para 4 horas en autonomía.
- Si se averiaba el escáner, no sería posible procesar las actas.
- Los componentes de las unidades EyT están todos integrados en la placa base, por lo tanto, se dificulta la actualización de hardware (CPU, RAM, Módulos de comunicación, etc.)

3.3.2. Escáneres INDRA

En busca de alcanzar mayor automatización, eficiencia y rapidez a la hora de realizar los sufragios, la JCE realizó una licitación pública para elegir la solución más viable y barata. Dicha licitación la gano INDRA Sistemas, S.A., la cual proveería el software y hardware necesario para realizar elecciones automatizadas en el 2016.

Los Escáneres de INDRA son dispositivos que pretendían superar algunas limitaciones que tenían las unidades EyT. Estos producirían los resultados de forma inmediata desde los colegios y sin intervención humana, alcanzando así un mayor nivel de automatización.

Figura 34: Escáner INDRA original

Fuente: (Junta Central Electoral, 2017)

3.3.2.1 Beneficios e Inconvenientes

El sistema de INDRA es fácil de comprender. Centraliza los datos electorales reduciendo el riesgo de ser manipulada aun precio asequible.

Por otra parte “Una evaluación realizada por la Dirección de Informática de la JCE determinó que los equipos usados en las pasadas elecciones no están aptos para ser utilizados en procesos futuros.

Estableció que el desempeño de la tecnología fue muy pobre y que desde la primera prueba se detectaron fallos en los equipos; y que en ninguno de los demás intentos se pudo conseguir una transmisión de datos mayor al 74% de los colegios electorales.

“Luego de revisar el diagnóstico realizado a las unidades de registro y escrutinio, y habiendo ponderado los problemas técnicos de los equipos junto con los fallos de software, salvo su mejor parecer, sugerimos no hacer uso de estos en procesos electorales futuros”, recomendó el informe técnico.”

Niza Campos. (2018). La empresa Indra Sistema es propietaria de los escáneres hasta que la JCE pague. 21/05/2019, de Diario Libre Sitio web: https://www.diariolibre.com/actualidad/politica/la-empresa-indra-sistema-es-propietaria-de-los-escaneres-hasta-que-la-jce-pague-HN9861559

3.4. Encuesta orientada a la opinión del votante respeto a un nuevo sistema de votación

3.4.1. Análisis e interpretación de los resultados

Luego de haber adherido herramientas de recolección de datos, se comenzó a componer las formas adecuadas para el análisis de los resultados obtenidos. La información será utilizada para vislumbrar la aceptación del pueblo dominicano respecto a un nuevo sistema de votación digital integrado con la tecnología blockchain y la opinión de los ciudadanos dominicanos acerca del sistema de votación actual de la Junta Central Electoral. Se encuesto a un total de 34 personas de forma global para captar una idea próxima a un resultado realista que demuestre el nivel de aceptación de la propuesta “Sistema de votación electrónico basado en cadena de bloques para la Junta Central Electoral**”.**

A partir de la información que brinda la encuesta realizada se puede discernir que en su totalidad los votantes están dispuestos a transformar el sistema de votación actual en la República Dominicana por uno que funcione digital con el propósito de brindar mayor confiabilidad y agilizar el procedimiento de votación. Además, podría sumar un público que nunca se ha interesado en las elecciones por múltiples razones que se visualizan en la figura 37.

3.4.1.1. Interrogantes y respuestas

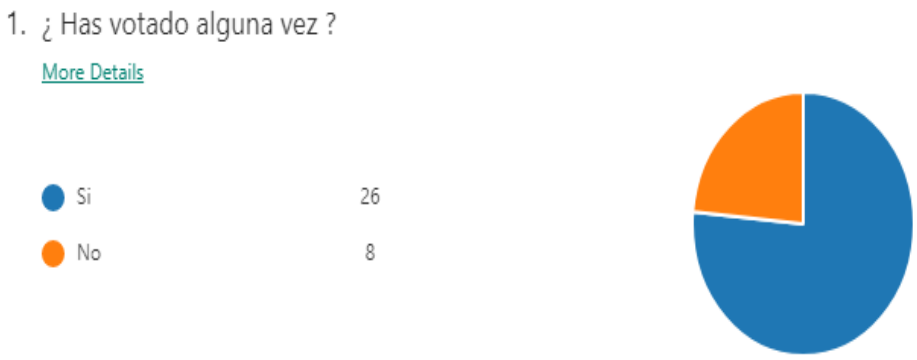


Figura 35: Ilustración que muestra si el individuo no ha votado

Fuente: Elaboración propia

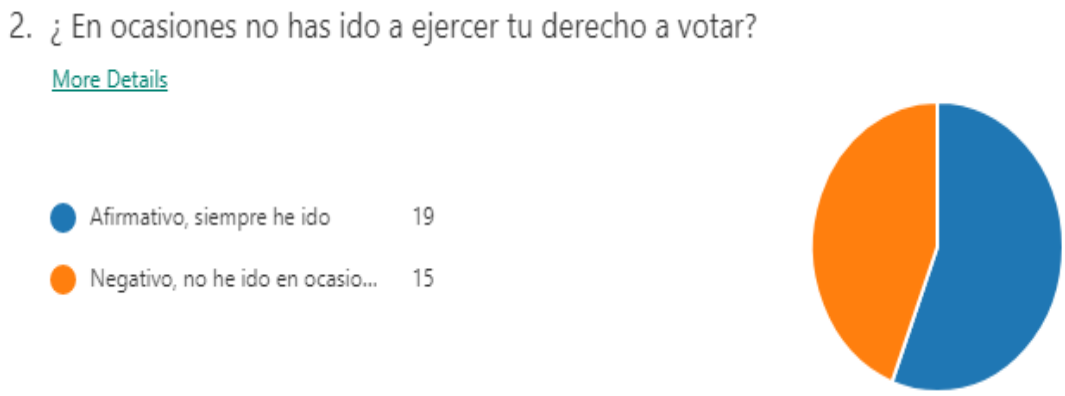


Figura 36: Muestra si las personas no han ido a votar

Fuente: Elaboración propia

Ilustra el porcentaje que no han ido a votar en ocasiones, este diagrama de pastel lo muestra con un 44%.

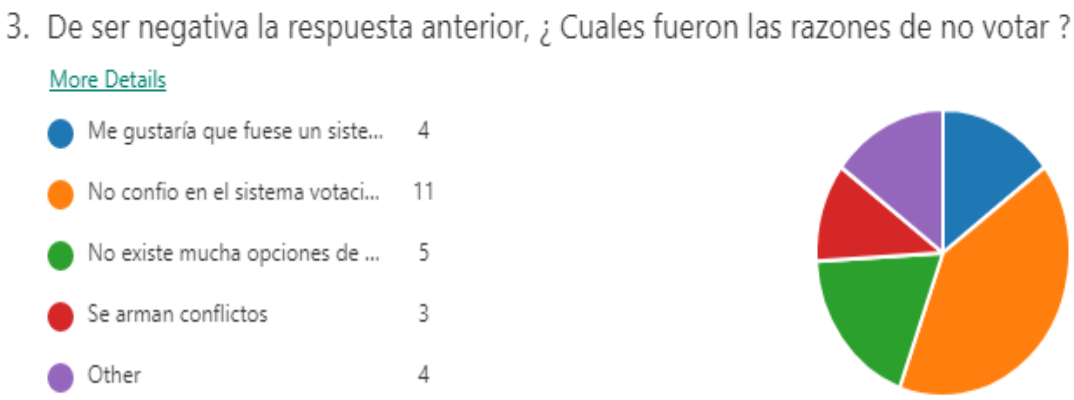


Figura 37: Ilustración que da a conocer la razón de que las personas no han votado

Fuente: Elaboración propia

Reflecta las razones de no ir a votar en ciertas ocasiones. Según la encuesta la razón principal por la que no han ido es porque consideran que el sistema de votación actual no es confiable; el diagrama lo representa con el color naranja que muestra el 32% de los que eligieron esa respuesta.

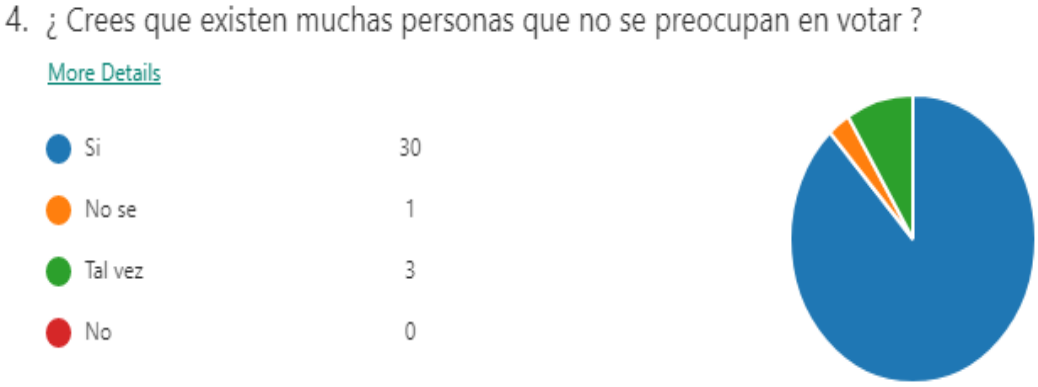


Figura 38: Cantidad de personas que consideran que existen personas sin preocupación por votar

Fuente: Elaboración propia

Un 88% cree que aún existen muchas personas que no se preocupa en dirigirse a su respectivo colegio electoral para ejercer su derecho a votar.

Figura 39: Ilustración que da a conocer según la encuesta el rango de edad de las personas sin preocupación por votar

Fuente: Elaboración propia

La figura 39 refleja el rango de personas con menor preocupación para ir a votar. Según el porcentaje mayor con el valor de 73%, el rango de edad va desde los 18 años hasta los 29 años.

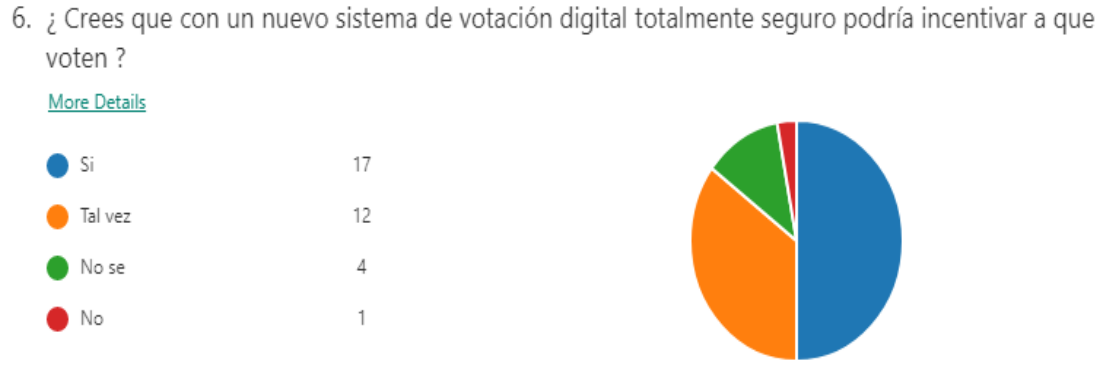


Figura 40: Manifiesta la suma de persona que cree que un nuevo sistema digital pudiera incentivar a un público

Fuente: Elaboración propia

En esta pregunta se obtuvo un 50% que representa la respuesta afirmativa “Si” que revela que un nuevo sistema de votación digital fiable podría incentivar a los

electores con menor preocupación por votar. Por otro lado, el 35% considera que talvez pudiera crear cierta motivación.

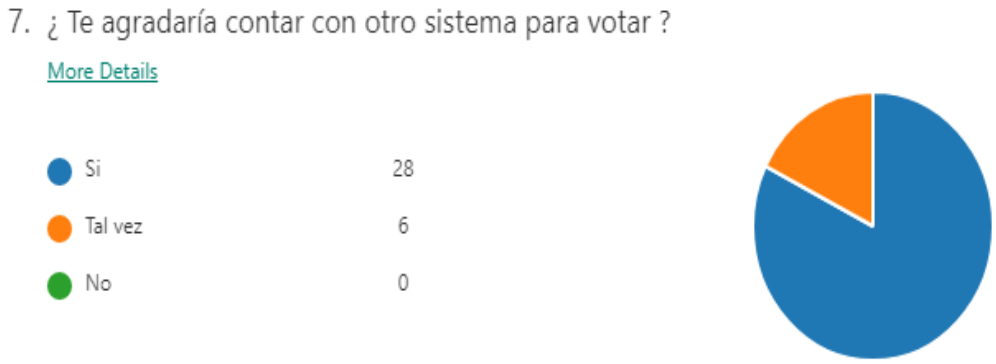


Figura 41: Expone la cantidad de individuos que le gustaría contar con otro sistema para votar

Fuente: Elaboración propia

Esta figura proyecta que existe un total de 82% que representa la cantidad dispuesta a contar con otro sistema diferente para votar. Sin embargo, el 18% respondieron la pregunta con “Tal vez” y un 0% respondieron con “No” indicando en lo absoluto que los electores esperan un sistema distinto que el actual.

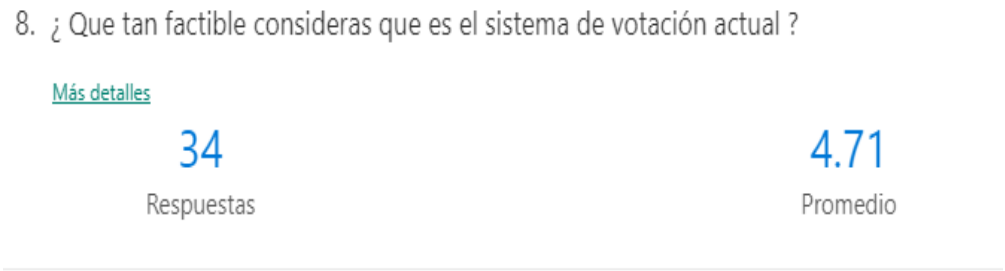


Figura 42: Evidencia el promedio de un rango de 1 a 10 de la factibilidad del sistema de votación actual

Fuente: Elaboración propia

La figura 42 ilustra un promedio de 4.71 en un rango que va desde 1 a 10 para evidenciar que tan factible se considera el sistema actual.

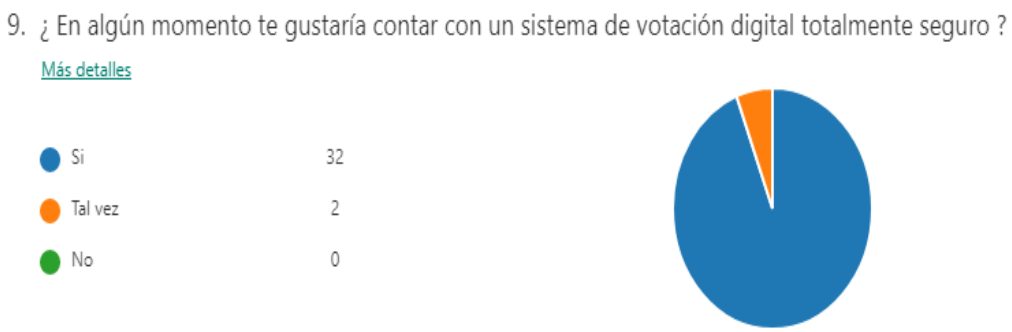


Figura 43: Revela la aceptación de un sistema digital seguro

Fuente: Elaboración propia

Hubo un porcentaje de 94% que marcaron “Si” y otro de 6% que indicaron “Tal vez”. Representando que un sistema de votación digital seguro es aceptado en la República Dominicana.

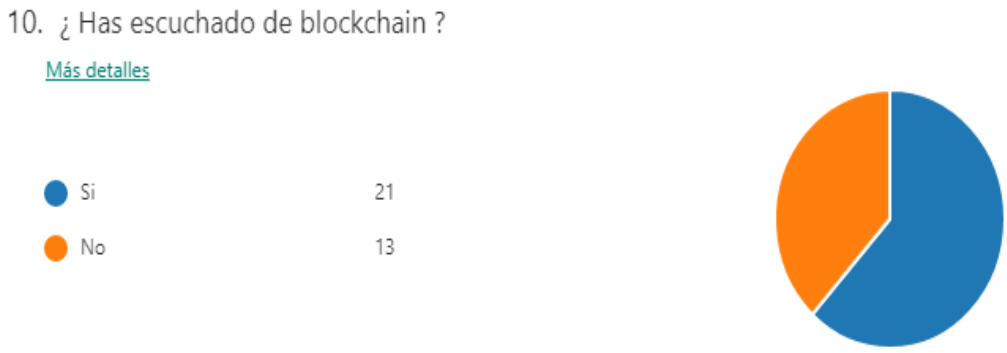


Figura 44: Indica la porción de personas que ha escuchado de blockchain

Fuente: Elaboración propia

Esta imagen muestra que el 62% de los encuestados habían escuchado de blockchain y un 38% nunca lo escucho.

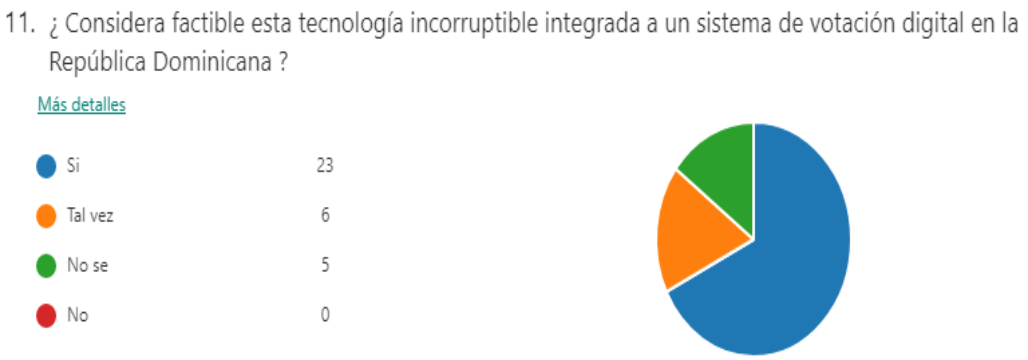


Figura 45: Enseña el nivel de aceptación de la propuesta del sistema de votación electrónico basado en la tecnología blockchain

Fuente: Elaboración propia

Este diagrama de pastel simboliza un 67% de aceptación del “Sistema de votación electrónico basado en la tecnología blockchain”. Por otro lado, el 18% respondieron con “Tal vez” considerando el cambio, mientras que un 15% de mostro que no sabe.

3.4.2. SVE basado en blockchain frente Sistema de votación actual

SVE BASADO EN BLOCKCHAIN		SISTEMA DE VOTACIÓN ACTUAL	
VENTAJAS	**DESVENTAJAS**	**VENTAJAS**	**DESVENTAJAS**
▪ Seguridad ▪ Rapidez ▪ Eficaz ▪ Confiable ▪ Ahorro de dinero con el tiempo ▪ Intuitivo ▪ Transparencia	▪ Alto costo		▪ Exposición al Fraude ▪ Ineficaz ▪ Procedimiento Lento ▪ No claro

▪ Anónimato ▪ Inalterabilidad			

Tabla 3: SVE basado en blockchain frente al sistema de votación actual

Fuente: Elaboración propia

CAPITULO IV: PROPUESTA DE ANALISIS Y DISEÑO DE UN SVE BASADO EN CADENA DE BLOQUES

4.1. Fundamentación de la propuesta

La democracia es vital para mantener una república, y la forma de alcanzar dicha democracia es contar con procesos que permitan a los ciudadanos elegir quienes serán sus dirigentes. Estos procesos son las elecciones de los diferentes niveles, realizados de forma local o nacional. Las elecciones permiten que los ciudadanos puedan ejercer su derecho al voto sin complicaciones y es la Junta Central Electoral quien debe de orquestar las elecciones en sus diferentes niveles.

La forma en que son realizadas las elecciones es basada en papel, de hecho, en muchos países todavía son realizadas así. Esto se debe a varios motivos: La arquitectura de un sistema de votación electrónica (SVE) es compleja, la seguridad de los SVE existentes es cuestionable, los SVE puede llegar a ser muy costosos, entre otros.

La JCE está intentando moverse de votación basado en papel al voto digital. Algunos de sus proyectos fueron las unidades EyT y los escáneres de INDRA. Sin embargo, todavía estos requieren de boletas físicas para captar el voto. En la actualidad, al tiempo que se está escribiendo esta propuesta, la JCE junto con la empresa DIGIWORLD S.R.L han desarrollado un SVE, el cual se planea usar en las elecciones del 2020.

4.2. Presentación de la propuesta

Esta propuesta consiste en el desarrollo de un sistema de votación electrónico, que, si bien agilice los sufragios, este también provea de mayor seguridad, a través del uso de una tecnología sobre la cual se fundamentan las criptomonedas, tales como bitcoin: Cadena de bloques o “Blockchain”.

4.3. Documento de Visión

4.3.1. Propósito

El propósito de esta propuesta es el sistematizar el análisis general del problema, las necesidades y las características del proceso de votación desde una perspectiva de alto nivel. Esta propuesta describe un SVE basado en Cadena de Bloques, el cual provee un esquema más seguro que los SVE convencionales. También se describen las necesidades y perfiles de los involucrados.

4.3.2. Alcance

El ámbito de este proyecto es el de analizar y diseñar un SVE basado en cadena de bloques.

4.3.3. Oportunidad de negocio

La JCE es un organismo autónomo, encargada de orquestar y coordinar el proceso de las elecciones en sus diferentes niveles.

La JCE ha estado usando el método convencional de votación, basado en papel, pero con algún elemento de SVE. Es decir, JCE usa un sistema de votación híbrida. Esta votación hibrida abre muchas brechas de seguridad, que pueden ser explotadas para desviar los resultados de las elecciones.

4.3.4. Definición del problema

El problema / Necesidad u oportunidad de negocio	Realizar votos totalmente electrónicos, a través de un SVE basado en Cadena de Bloques. Evita la alteración de los votos una vez registrados en la Cadena de Bloques.
Afecta a	Votantes
El impacto asociado es	• Alteración de los resultados del conteo de votos • Votos anulados por errores humanos.
Una solución adecuada sería	Almacenar la información de los votos en los bloques de una cadena de bloques. Esto evita que esta información sea modificada accidental o incidentalmente.

Tabla 4: Definición del Problema

Fuente: Elaboración propia

4.3.5. Posición de la Solución

Para	Junta Central Electoral (JCE)
Quienes	Gestionan el proceso de votación
El Nombre del Producto	SVE BlockVote
Cualidades del sistema propuesto	Permite que los votantes realicen su voto, sin la necesidad de boletas físicas. Todo es procesado electrónicamente. Su voto es almacenado en los bloques de la cadena de bloques.
A diferencia de	El sistema clásico, que utiliza boletas físicas, la cual son limitadas y que para generarlas se utilizan materia prima. Existe también de anular el voto por un error humano. Los SVE convencionales, como los de Estonia, Noruega y iVote de Sout Wale. Son susceptibles a los ataques de negación de servicios, por su naturaleza descentralizada.

Tabla 5: Posición de la Solución

Fuente: Elaboración propia

4.4. Especificación de Requisitos del Sistema

A continuación, se listarán los requisitos tanto funcionales como no funcionales. El nivel de prioridad va desde 1 (menos prioritario) a 5 (máxima prioridad).

4.4.1 Requisitos Funcionales

ID	Requisito	Prioridad
RF-BV-01	El sistema verificará si el ciudadano está en la Lista de Electores (Padrón Electoral).	3
RF-BV-02	El sistema permitirá que el votante pueda elegir solo un candidato por lista.	4
RF-BV-03	El sistema permitirá votar sólo una vez. Después de haber votado, el votante será marcado en la cadena de bloques como inhabilitado para votar por ese periodo de elección.	5
RF-BV-04	El sistema permitirá realizar un voto de protesta. El voto de protesta indica que el votante no está conforme con ninguno de los candidatos en la lista.	1
RF-BV-05	El sistema permitirá el registro de candidatos.	5
RF-BV-06	El sistema solo permitirá la edición de candidatos ya registrados, antes del periodo de votación.	4
RF-BV-07	El sistema permitirá obtener la cantidad de votos por candidatos durante y después del periodo de elección.	3
RF-BV-08	El sistema permitirá eliminar todos los votos (bloques) de las cadenas de bloques de los candidatos.	4

Tabla 6: Tabla de requerimientos funcionales

Fuente: Elaboración propia

4.4.2. Requisitos No Funcionales

ID	Requisito	Prioridad
RNF-BV-01	El sistema no debe vincular el voto con el votante. Utilizar el algoritmo NZKP	3
RNF-BV-02	El sistema requerirá la cédula y la huella dactilar	5
RNF-BV-03	El sistema requerirá un nodo por cada junta electoral a través del país.	
RNF-BV-04	Los organismos superiores autónomos, tales como: Junta Central Electoral, Banco Central y la Cámara Cuentas serán validadores de las transacciones de votación.	5
RNF-BV-05	Cada entrada de la lista de candidatos deberá tener una foto del logo del partido	4
RNF-BV-06	El tamaño de la tipografía de la interfaz gráfica de la máquina de votación deberá ser de por lo menos 24pt.	2
RNF-BV-07	El sistema debe ser capaz ejecutarse en Linux o Unix	4

Tabla 7: Tabla de requerimientos funcionales

Fuente: Elaboración propia

4.5. Diagramas y Especificación de caso de usos

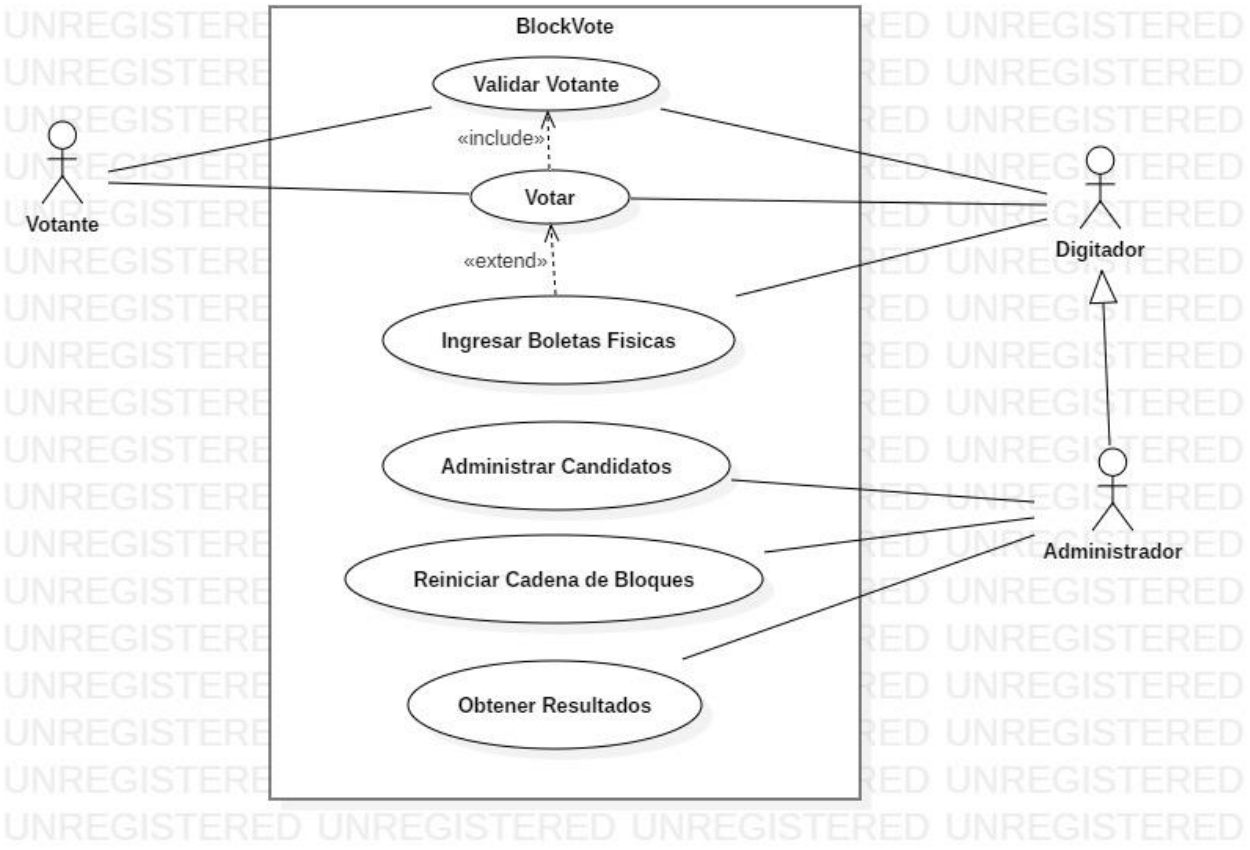


Figura 46: Caso de Uso General

Fuente: Elaboración propia

4.5.1. Caso de Uso Validar Votante

Caso de Uso	**Validar Votante**	**CU-01**
Escenario	Valida si el votante está en el padrón	
Fuente	RF-BV-01	
Autor	Votante	
Descripción	Permite que el ciudadano pueda validarse contra el padrón.	
Propósito	Validar al votante contra el padrón y verifica si esta hábil	

	para votar.	
Precondiciones	El Votante tiene su cedula de identidad electoral.	
Flujo Normal de Eventos		
Paso	**Acción del Actor**	**Respuesta del Sistema**
FN-01	El Votante ingresa su Numero de identidad electoral (Número de Cédula)	
FN-02		El sistema activa el lector de huellas y muestra en la pantalla un mensaje indicando que debe poner su pulgar derecho en el lector.
FN-03	El votante pone su pulgar derecho en el lector.	
FN-04		El sistema utiliza el número de identidad electoral y los datos biométricos captados por el lector de huellas contra la base de datos del padrón

FN-05		El sistema procede al siguiente paso
Flujo de Error 1		
Paso	**Acción del Autor**	**Respuesta del Sistema**
FE1-01	El Votante ingresa su Número de identidad electoral (Número de Cédula)	
FE1-02		El sistema activa el lector de huellas y muestra en la pantalla un mensaje indicando que debe poner su pulgar derecho en el lector.
FE1-03	El votante pone su pulgar derecho en el lector.	
FE1-04		El sistema Utiliza el número de identidad electoral y los datos biométricos captados por el lector de huellas contra la base de datos del padrón

FE1-05		El sistema muestra un mensaje indicando que no pudo encontrar al votante en la base de datos del padrón
Flujo de Error 2		
Paso	**Acción del Autor**	**Respuesta del Sistema**
FE2-1	El Votante ingresa su Numero de identidad electoral (Número de Cédula)	
FE3-2		El sistema responde que la cédula no es auténtica.
Post Condiciones	El sistema permite al votante realizar su voto	
Comentarios	El Votante debe tener su cédula de identidad personal	

Tabla 8: Especificación de Caso de uso CU-01

Fuente: Elaboración propia

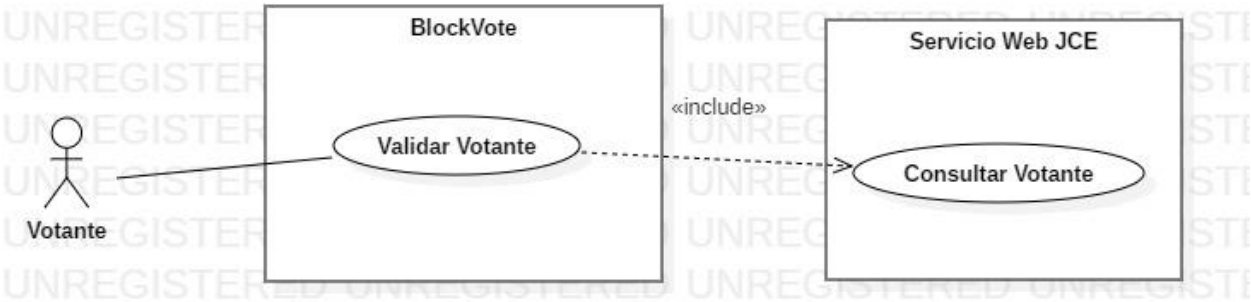


Figura 47: Caso de Uso Específico para Validar Votante

Fuente: Elaboración propia

4.5.2. Caso de Uso Votar

Caso de Uso	**Votar**	**CU-02**
Escenario	Realización del voto	
Fuente	RF-BV-02	
Autor	Votante	
Descripción	Permite elegir a los candidatos de los diferentes niveles	
Propósito	Seleccionar a los candidatos de los diferentes niveles	
Precondiciones	El Votante fue validado contra el padrón electoral.	
Flujo Normal de Eventos		
Paso	**Acción del Actor**	**Respuesta del Sistema**
FN-1		El sistema muestra una o varias listas de candidatos
FN-2	El Votante elige su candidato al tocar sobre su imagen.	
FN-3		El sistema muestra una confirmación de que el voto fue realizado satisfactoriamente
FN-4		El sistema imprime un voucher con un número de confirmación.
Flujo Alterno 1		

Paso	Acción del Actor	Respuesta del Sistema
FA1-1		El Sistema muestra una lista vacía sin candidatos a excepción del voto nulo y muestra un mensaje: “No hay candidatos en esta lista”.
Flujo Alterno 2		
Paso	**Acción del Actor**	**Respuesta del Sistema**
FA2-1		El sistema muestra una o varias listas de candidatos
FA2-2	El Votante toca sobre la imagen del candidato nulo, para realizar un voto nulo.	
FA2-3		El sistema muestra un mensaje indicando: “Estas seguro(a) que quieres realizar un voto nulo”
FA2-4	El Votante selecciona la Opción “Si”	
FA2-5		El sistema muestra una confirmación de que el voto fue realizado

		satisfactoriamente
FA2-6		El sistema imprime un voucher con un número de confirmación.
Flujo Alterno 3		
Paso	**Acción del Actor**	**Respuesta del Sistema**
FA3-1		El sistema muestra una o varias listas de candidatos
FA3-2	El Votante toca sobre la imagen del candidato nulo, para realizar un voto nulo.	
FA3-3		El sistema muestra un mensaje indicando: “Estas seguro(a) que quieres realizar un voto nulo”
FA4-4	El Votante selecciona la Opción “No”	
FA5-5		El sistema muestra una o varias listas de candidatos
Post Condiciones	El sistema habrá ingresado el bloque del voto a la cadena de bloques.	
Comentarios		

Tabla 9: Especificación de Caso de Uso CU-02

Fuente: Elaboración propia

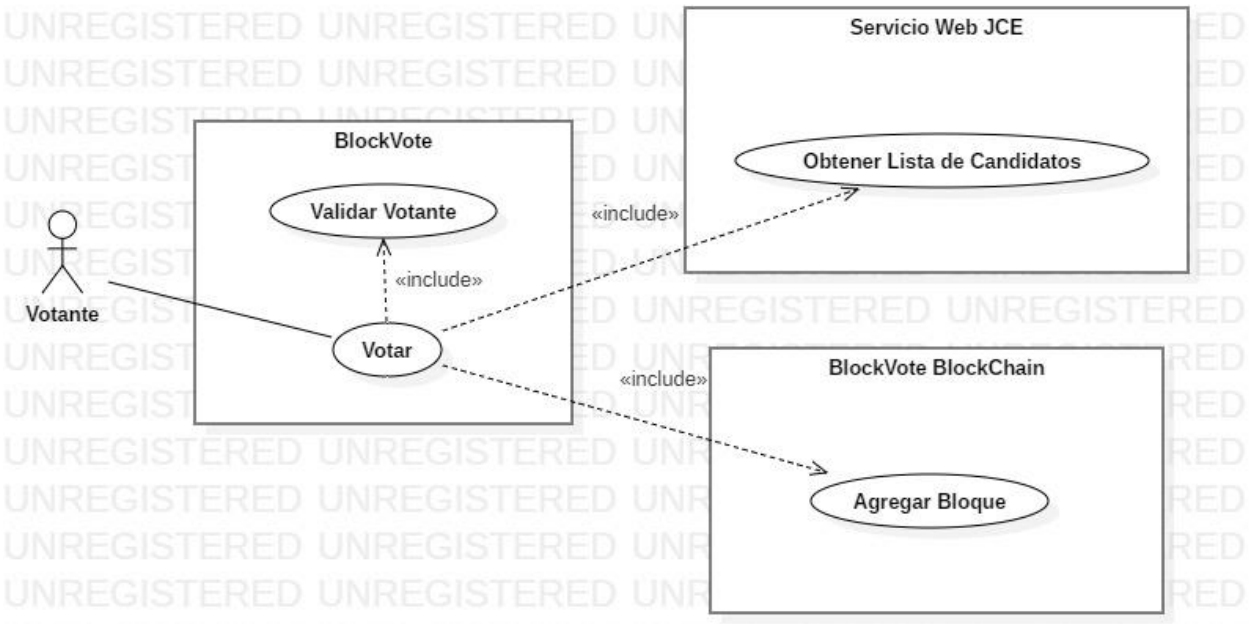


Figura 48: Caso de Uso Específico para Votar

Fuente: Elaboración propia

4.5.3. Caso de Uso Administrar Candidatos

Caso de Uso	**Administrar Candidatos**	**CU-03**
Escenario	Gestión de los Candidatos	
Fuente	RF-BV-05	
Autor	Administrador	
Descripción	Permite agregar y editar candidatos al sistema	
Propósito	Registrar candidatos al sistema	
Precondiciones	El periodo de votación no ha comenzado y el Candidato fue validado contra el padrón electoral	

Flujo Normal de Eventos		
Paso	**Acción del Actor**	**Respuesta del Sistema**
FN-1	El Administrador toma los datos de los candidatos y los ingresa al sistema. Los datos son: Nombre completo, cedula, Foto 2x2, nivel (Presidencial, municipal, etc.)	
FN-2		El sistema agrega el candidato a la cadena de bloques.
FN-3		El sistema genera un numero único y luego lo imprime, junto con el mismo número, codificado como un código QR.
FN-4		
Flujo Alterno 1		
Paso	**Acción del Actor**	**Respuesta del Sistema**
FA1-1	El Administrador pide el numero único, en caso de que el candidato ya este	

	creado en la cadena de bloques	
FA1-2		El sistema muestra una pantalla para editar la información existente del candidato
FA1-3	El Administrador introduce los datos nuevos	
FA1-4		El sistema muestra que la información del candidato fue cambiada satisfactoriamente.
Flujo Alterno 2		
Paso	**Acción del Actor**	**Respuesta del Sistema**
FA1-1	El Administrador procede a eliminar	
FA1-2		El sistema muestra los detalles del candidato a eliminar y muestra un mensaje: “Esta seguro que desea eliminar el este candidato”.
FA1-3	El Administrador elige “Si”	

FA1-4		El sistema muestra que la información del candidato fue eliminada satisfactoriamente.
Post Condiciones	El candidato estará disponible en el sistema, en la lista correspondiente al nivel que eligió	
Comentarios	El candidato puede enviar sus datos mediante correo. Es importante que el candidato conserve el numero único.	

Tabla 10: Especificación de Caso de Uso CU-03

Fuente: Elaboración propia

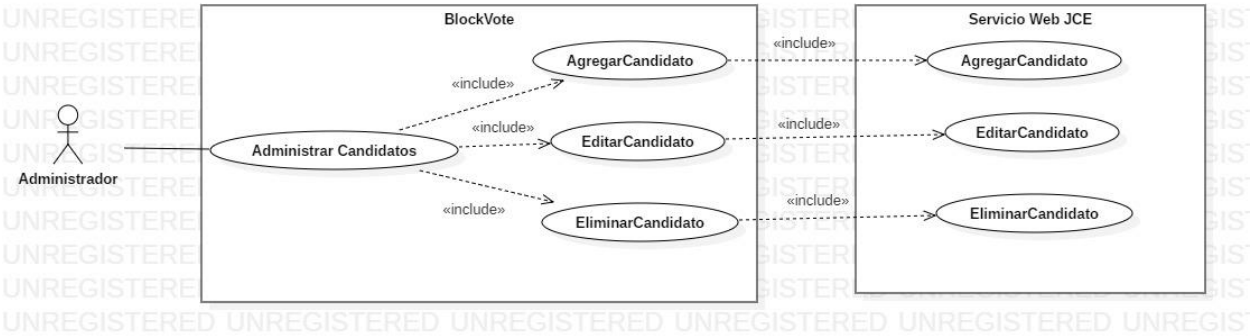


Figura 49: Caso de Uso Específico para Administrar Candidato

Fuente: Elaboración propia

4.5.4. Caso de Uso Ingresar Boletas Físicas

Caso de Uso	**Ingresar Boletas Físicas**	**CU-04**
Escenario	Realización del voto	
Fuente	RF-BV-02	
Autor	Digitador, Administrador	

Descripción	Permite ingresar boletas físicas al sistema para que estas sean contadas	
Propósito	Ingresar boletas físicas, para proveer compatibilidad con votación convencional	
Precondiciones	El periodo de votación ha finalizado	
Flujo Normal de Eventos		
Paso	**Acción del Actor**	**Respuesta del Sistema**
FN-1	El Administrador abre la cuenta de Digitador, la cual permite ingresar boletas sin verificar en el padrón	
FN-2		El sistema muestra una lista de candidatos
FN-3	El Digitador selecciona el candidato que esta seleccionado en la boleta	
FN-4		El sistema muestra un mensaje, indicando que voto fue realizado satisfactoriamente
Post Condiciones	Se habrán registrado todas las boletas tanto físicas como virtuales en el sistema. Luego se procede a	

	realizar el conteo y obtener los resultados.
Comentarios	

Tabla 11: Especificación de Caso de Uso CU-04

Fuente: Elaboración propia

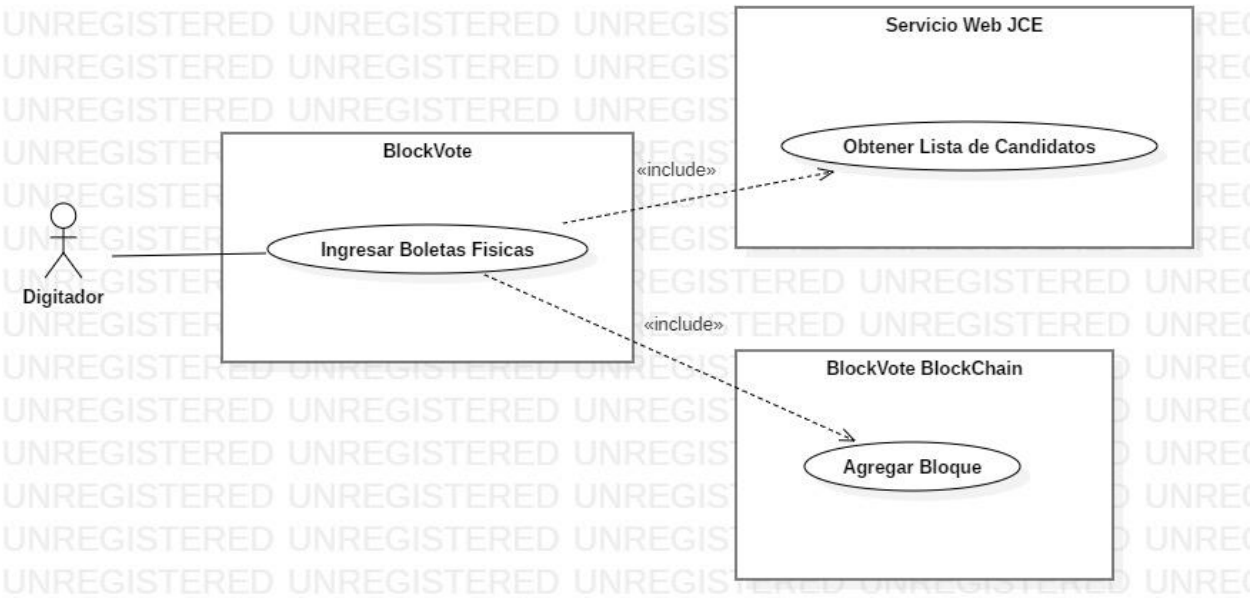


Figura 50: Caso de Uso Específico para Ingresar Boletas Físicas

Fuente: Elaboración propia

4.5.5. Caso de Uso Obtener Resultados

Caso de Uso	**Obtener Resultados**	**CU-05**
Escenario	Conteo	
Fuente	RF-BV-07	
Autor	Administrador	
Descripción	Permite obtener la cantidad de votos	
Propósito	Obtener los resultados de las elecciones durante y después del periodo de votación.	

Precondiciones	El Periodo de votación debe haber comenzado.	
Flujo Normal de Eventos		
Paso	**Acción del Actor**	**Respuesta del Sistema**
FN-1	El Administrador selecciona la opción “Resultados”	
FN-2		El Sistema muestra un panel de estadísticas de los resultados por niveles y por candidatos.
Post Condiciones	Se muestra estadísticas de votos.	
Comentarios	Estos resultados se pueden imprimir.	

Tabla 12: Especificación de Caso de Uso CU-05

Fuente: Elaboración propia

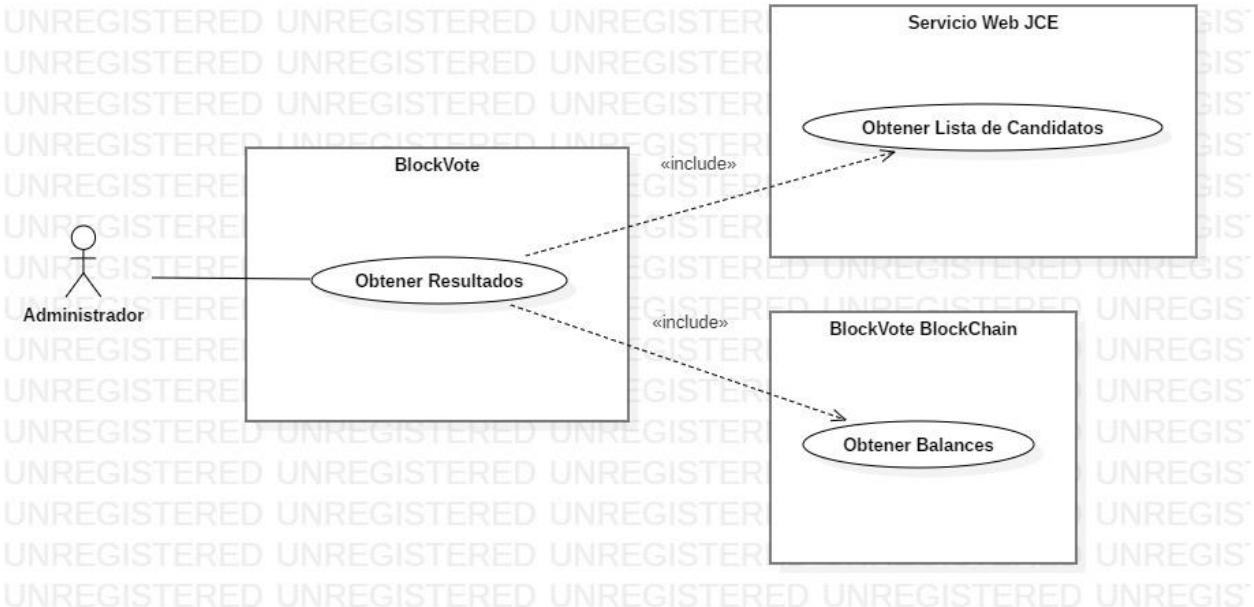


Figura 51: Caso de Uso Específico para Obtener Resultados

Fuente: Elaboración propia

4.5.6. Caso de Uso Reiniciar Cadena de Bloques

Caso de Uso	**Reiniciar Cadena de Bloques**	**CU-06**
Escenario	Cierre de proceso de votación	
Fuente	RF-BV-08	
Autor	Administrador	
Descripción	Permite eliminar todos los bloques de la cadena de bloques	
Propósito	Reiniciar la cadena de bloques del sistema	
Precondiciones	El periodo de votación debe haber finalizado y haber obtenido los resultados	
Flujo Normal de Eventos		
Paso	**Acción del Actor**	**Respuesta del Sistema**
FN-1	El Administrador elige “Reiniciar Cadena de bloques”	
FN-2		El Sistema pide confirmación con un mensaje: “Esta seguro que desea reiniciar la cadena de bloques”
FN-3	El Administrador elige que	

	“Si”	
FN-4		El sistema elimina todos los bloques de la cadena de bloques.
FN-5		El sistema obtiene la lista de candidatos
FN-6		El sistema desvincula los candidatos de la cadena de bloques al eliminar su relación con el número único.
Flujo Alterno de Eventos		
Paso	**Acción del Actor**	**Respuesta del Sistema**
FA-1	El Administrador elige “Reiniciar Cadena de bloques”	
FA-2		El Sistema pide confirmación con un mensaje: “Esta seguro que desea reiniciar la cadena de bloques”
FA-3	El Administrador elige que “No”	

FA-4		El Sistema vuelve a su estado normal
Post Condiciones	La cadena de bloques estará vacía y se le tendrán que generar un nuevo número único a los candidatos existentes.	
Comentarios		

Tabla 13: Especificación de Caso de Uso CU-06

Fuente: Elaboración propia

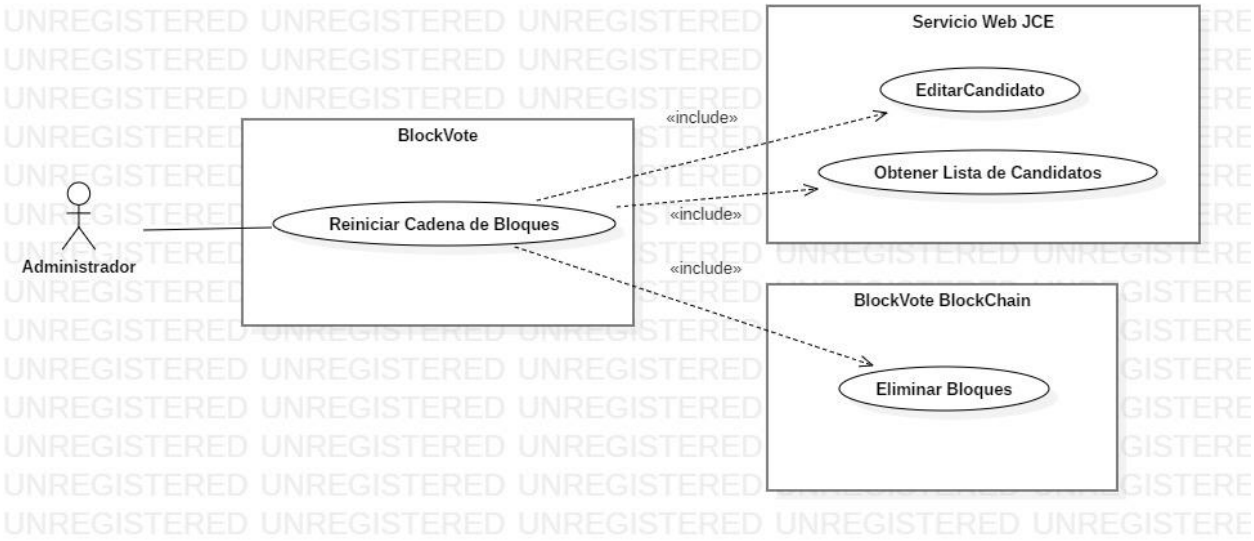


Figura 52: Caso de Uso Específico para Reiniciar Cadena de Bloques

Fuente: Elaboración propia

4.6. Diagramas de modelado del sistema

4.6.1 Diagramas de actividades

4.6.1.1. Diagrama de Actividad de Validar Votante

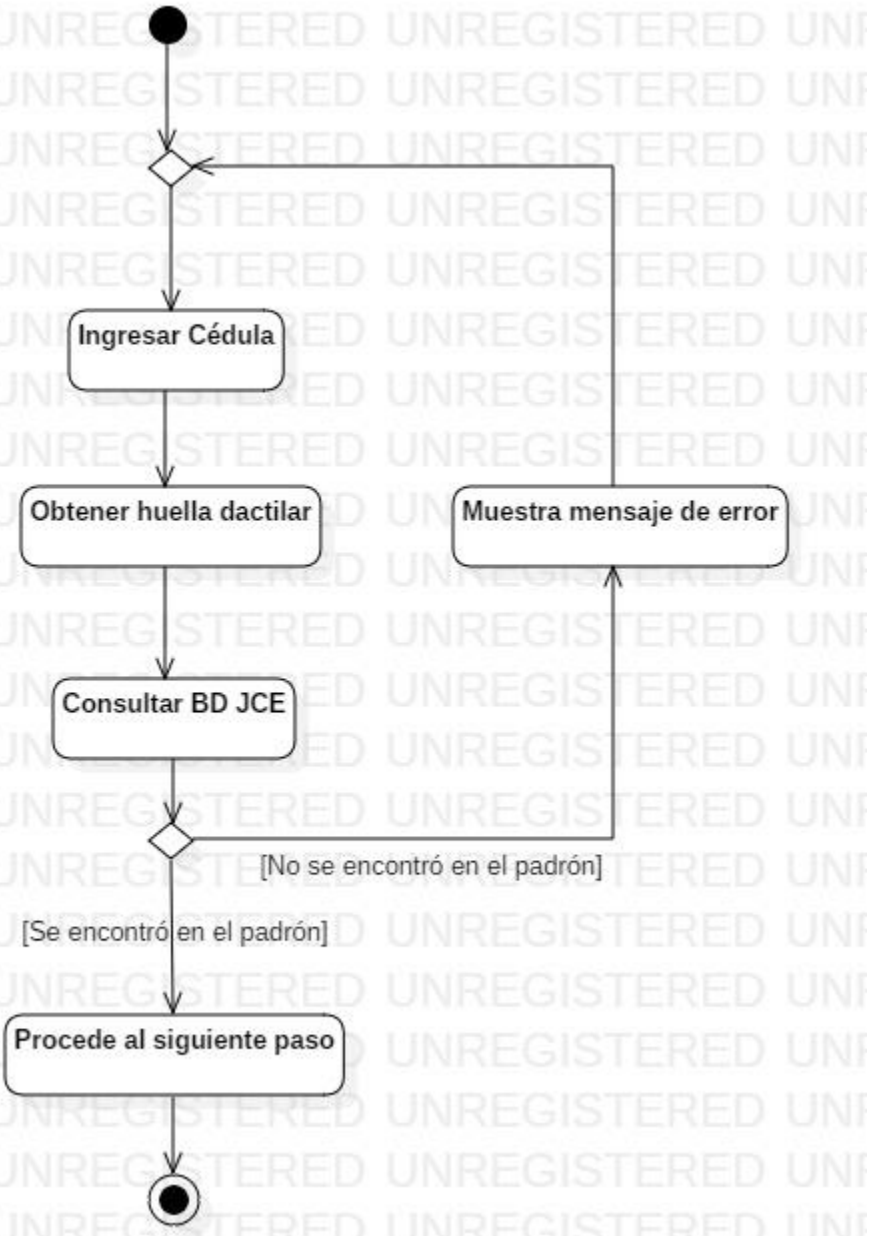


Figura 53: Diagrama de Actividad de Validar Votante

Fuente: Elaboración propia

4.6.1.2. Diagrama de Actividad de Votar

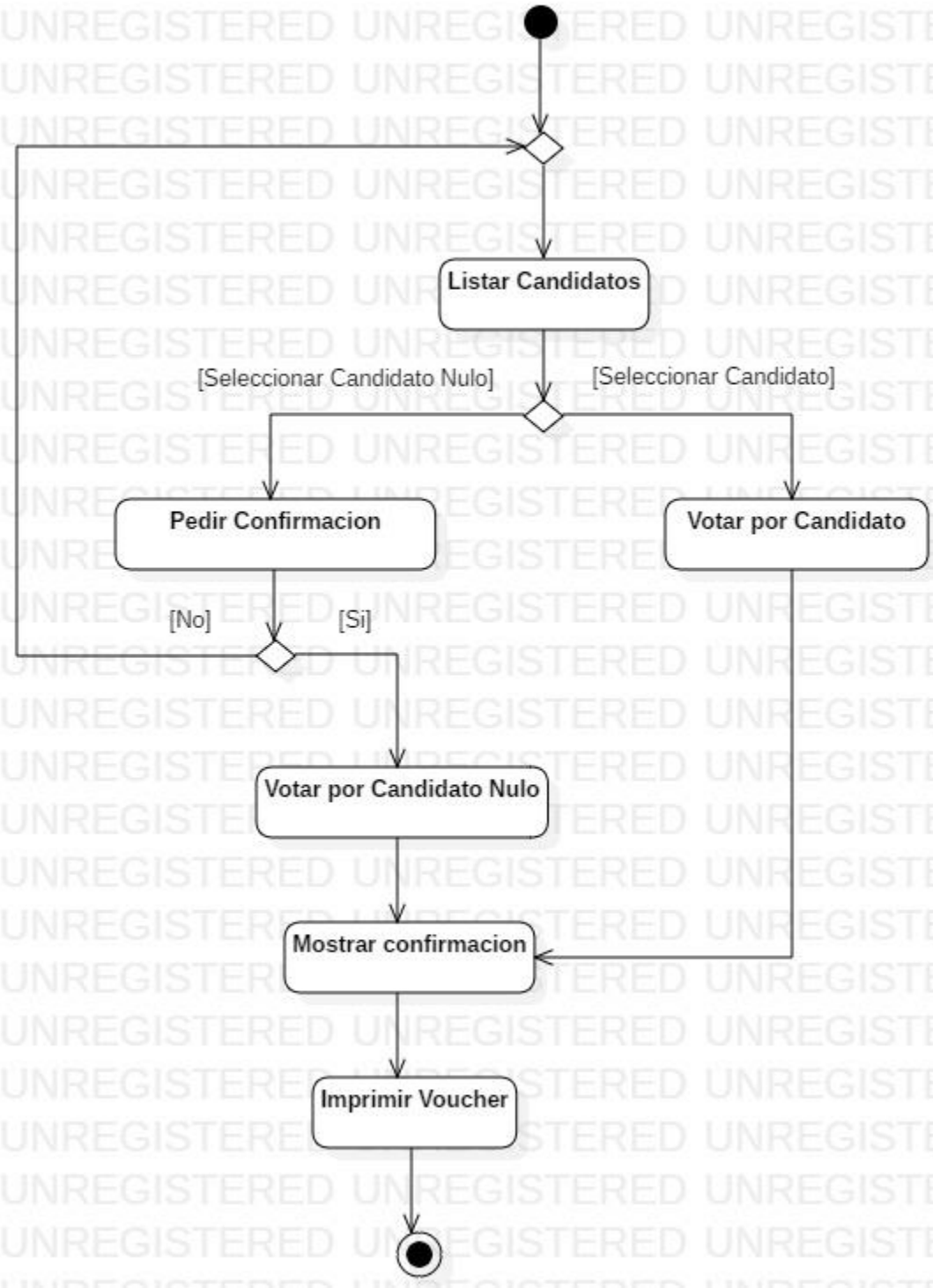


Figura 54: Diagrama de Actividad de Votar

Fuente: Elaboración propia

4.6.1.3. Diagrama de Actividad de Administrar Candidatos

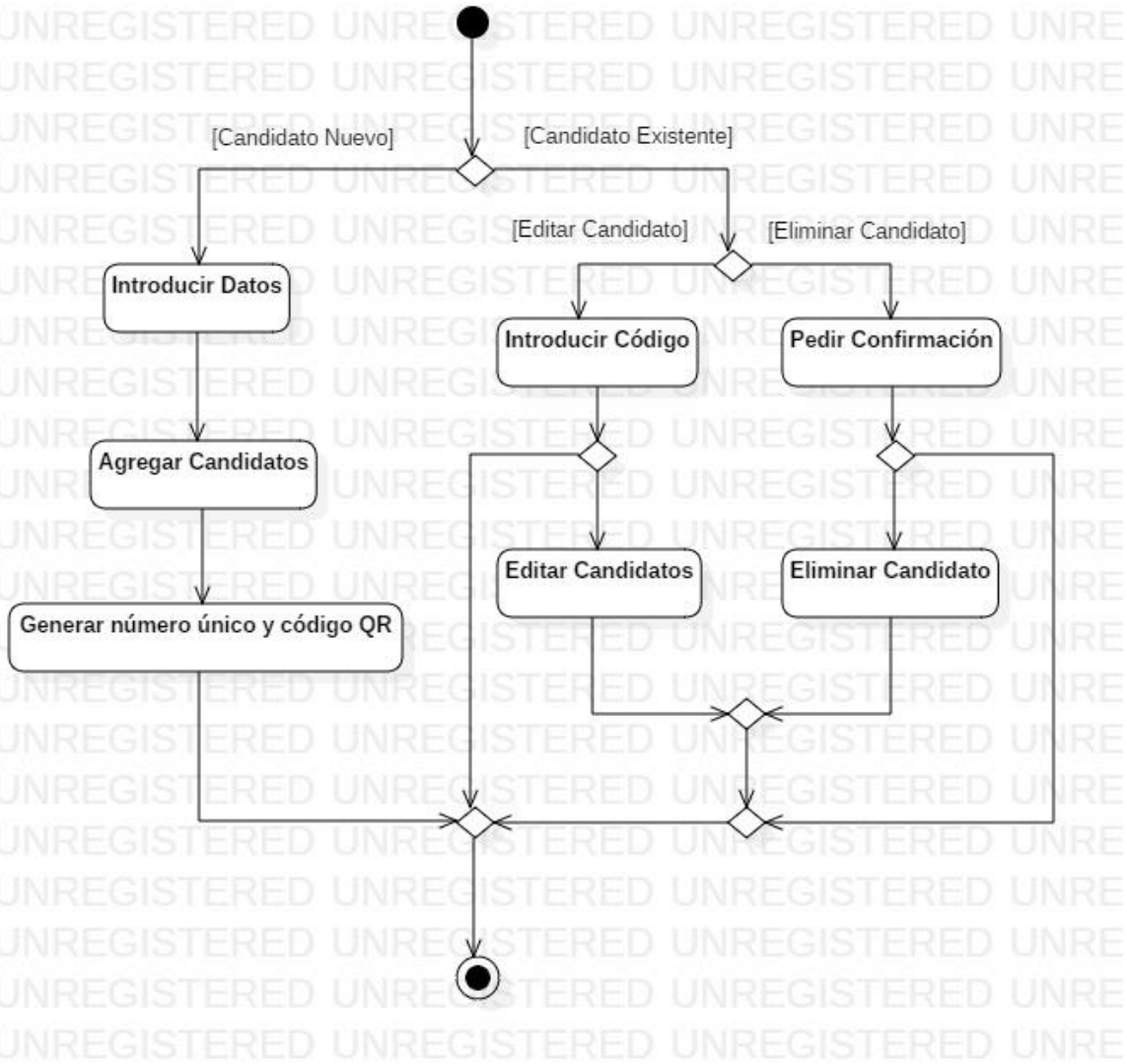


Figura 55: Diagrama de Actividad de Administrar Candidatos

Fuente: Elaboración propia

4.6.1.4. Diagrama de Actividad de Ingresar Boletas Físicas

Figura 56: Diagrama de Actividad de Ingresar Boletas Físicas

Fuente: Elaboración propia

4.6.1.5. Diagrama de Actividad de Obtener Resultados

Figura 57: Diagrama de Actividad de Obtener Resultados

Fuente: Elaboración propia

4.6.1.6. Diagrama de Actividad de Reiniciar Cadena de Bloques

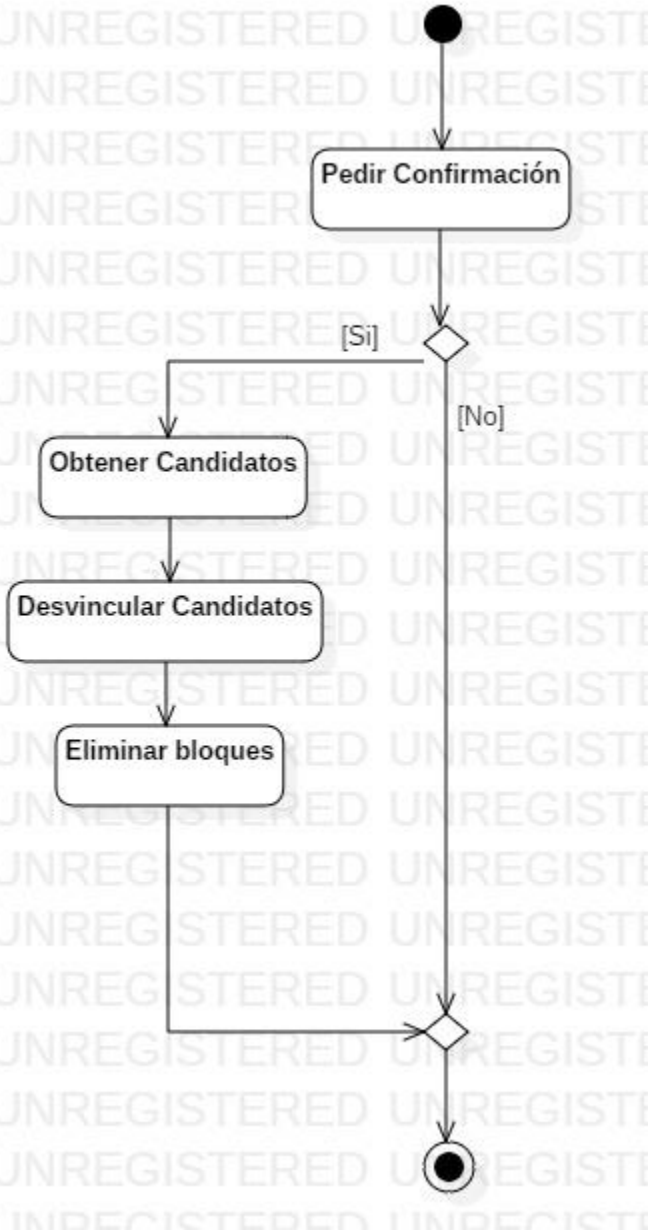


Figura 58: Diagrama de Actividad de Reiniciar Cadena de bloques

Fuente: Elaboración propia

4.6.2. Diagramas de secuencias

4.6.2.1 Validar Votante

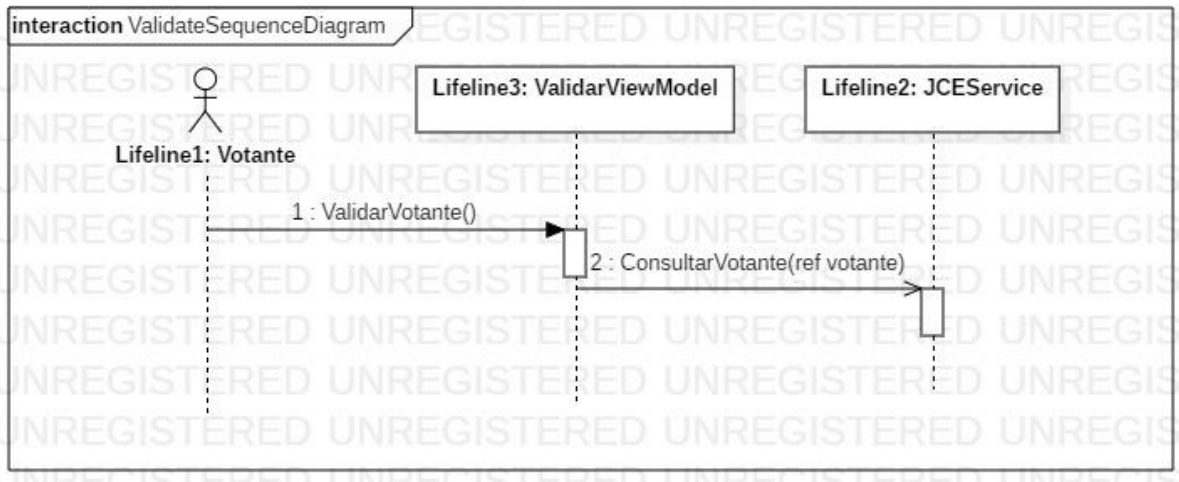


Figura 59: Diagrama de Secuencia de Validar Votante

Fuente: Elaboración propia

4.6.2.2 Votar

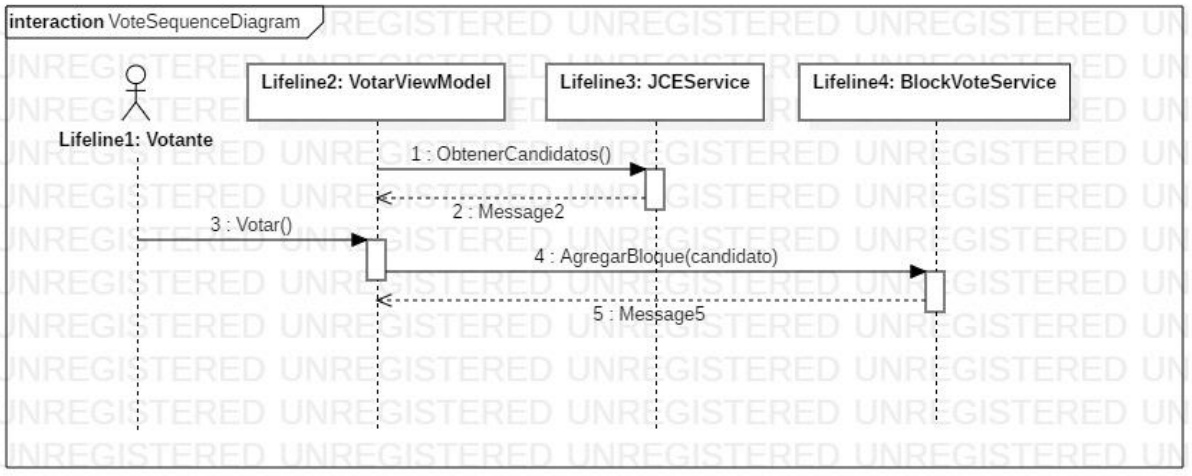


Figura 60: Diagrama de Secuencia de Votar

Fuente: Elaboración propia

4.6.2.3 Administrar Candidatos

4.6.2.3.1. Agregar

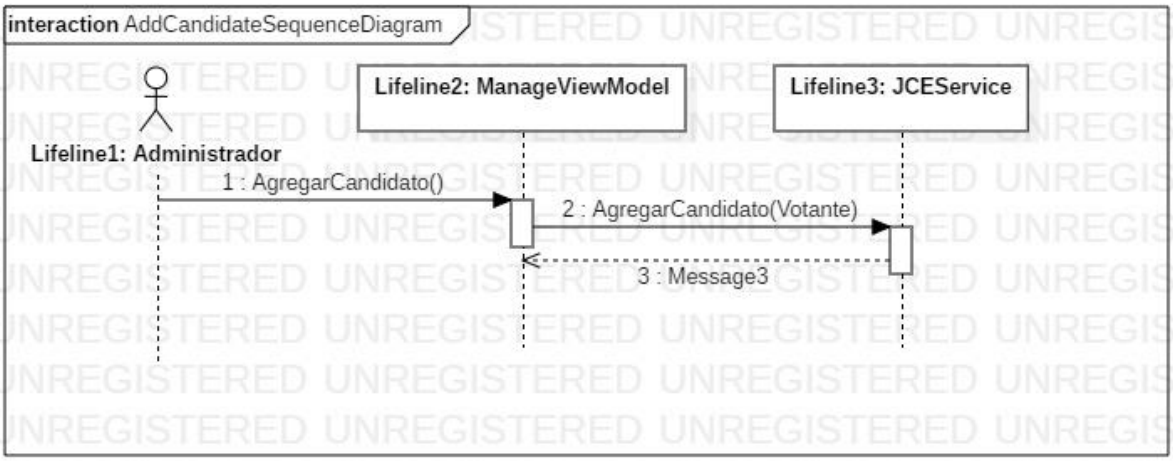


Figura 61: Diagrama de Secuencias Administrar Candidatos: Agregar

Fuente: Elaboración propia

4.6.2.3.1. Editar

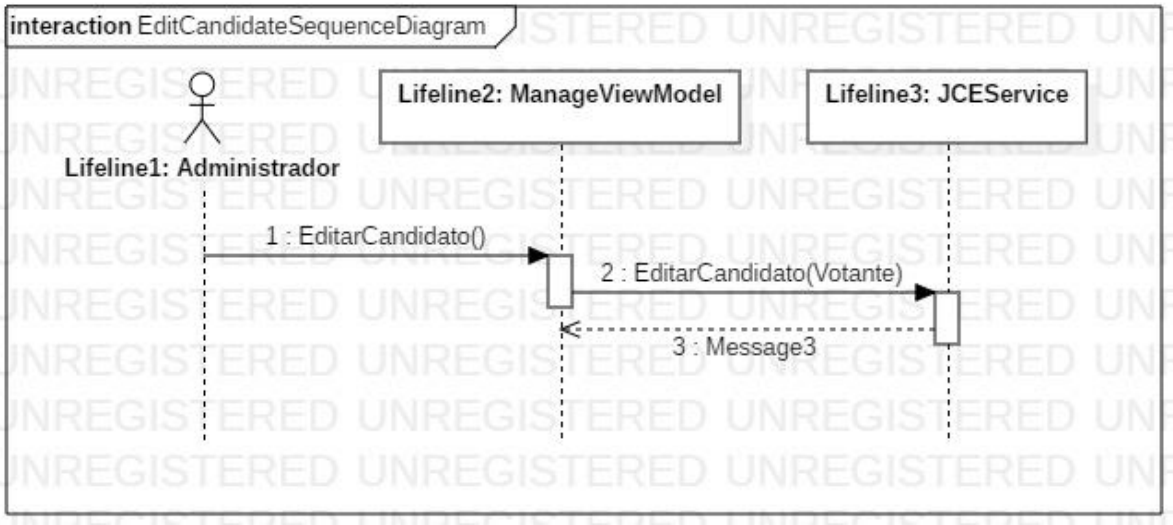


Figura 62: Diagrama de Secuencias Administrar Candidatos: Editar

Fuente: Elaboración propia

4.6.2.3.1. Eliminar

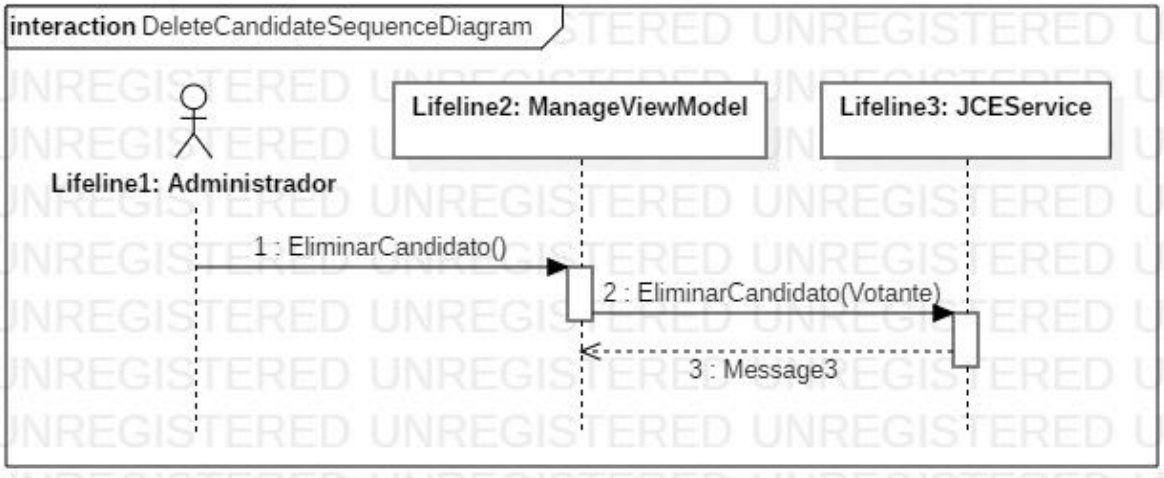


Figura 63: Diagrama de Secuencias Administrar Candidatos: Eliminar

Fuente: Elaboración propia

4.6.2.4 Reiniciar Cadena

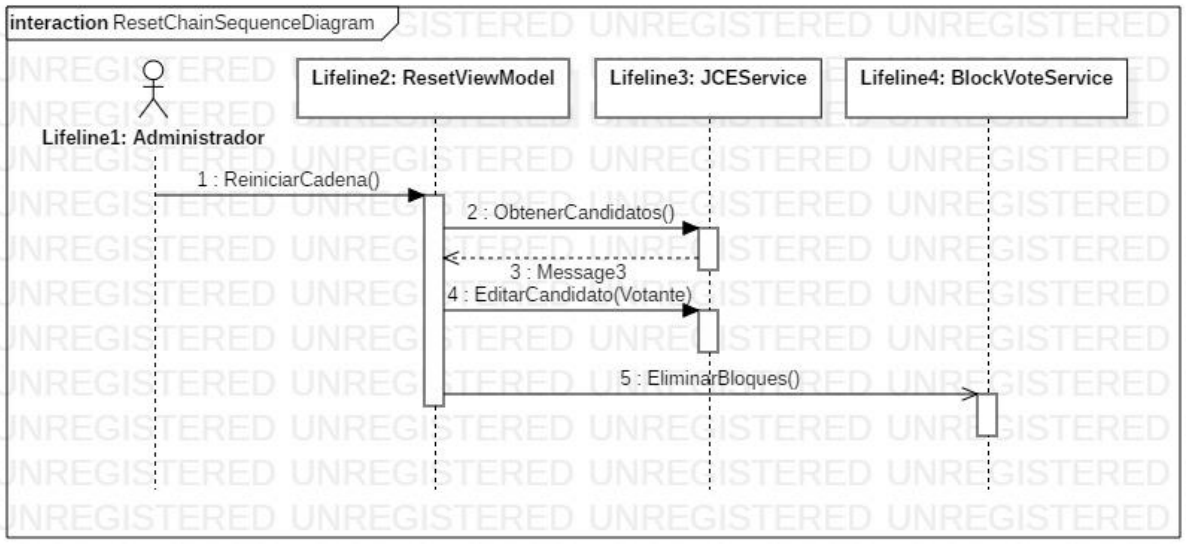


Figura 64: Diagrama de Secuencias Reiniciar Cadena de Bloques

Fuente: Elaboración propia

4.6.2.5 Obtener Resultados

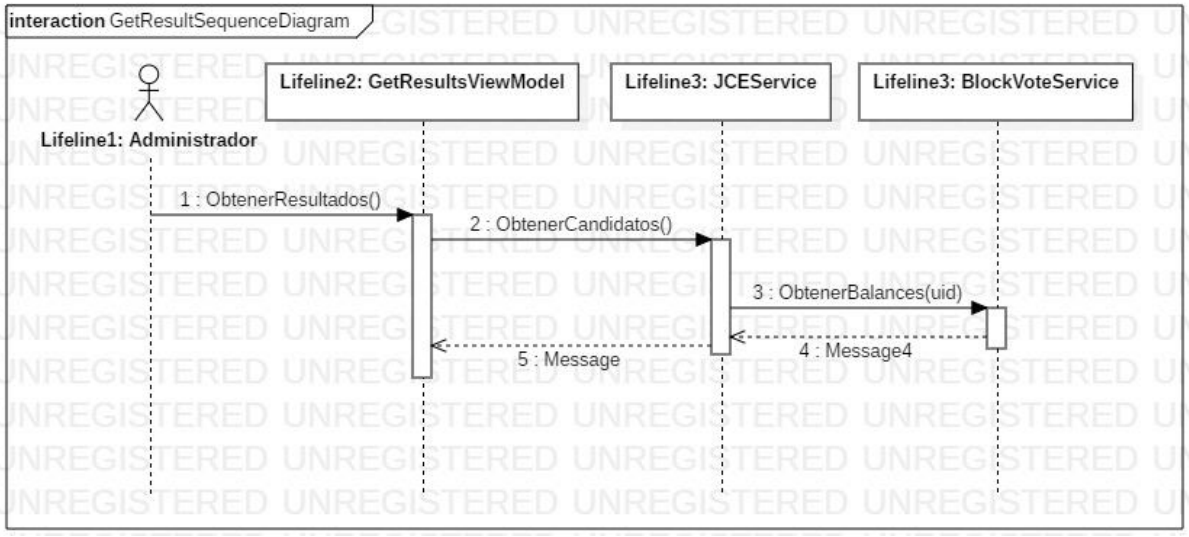


Figura 65: Diagrama de Secuencias Obtener Resultados

Fuente: Elaboración propia

4.6.3. Diagramas de clases

4.6.3.1. Cliente de Votación en Estación de votación

El cliente de votación es una aplicación de escritorio que utiliza un patrón arquitectónico llamado Model-View-ViewModel (MVVM). Este permite el desacoplamiento de la lógica de negocio y la lógica de la interfaz gráfica, además, como consecuencia, hace que la aplicación sea más mantenible.

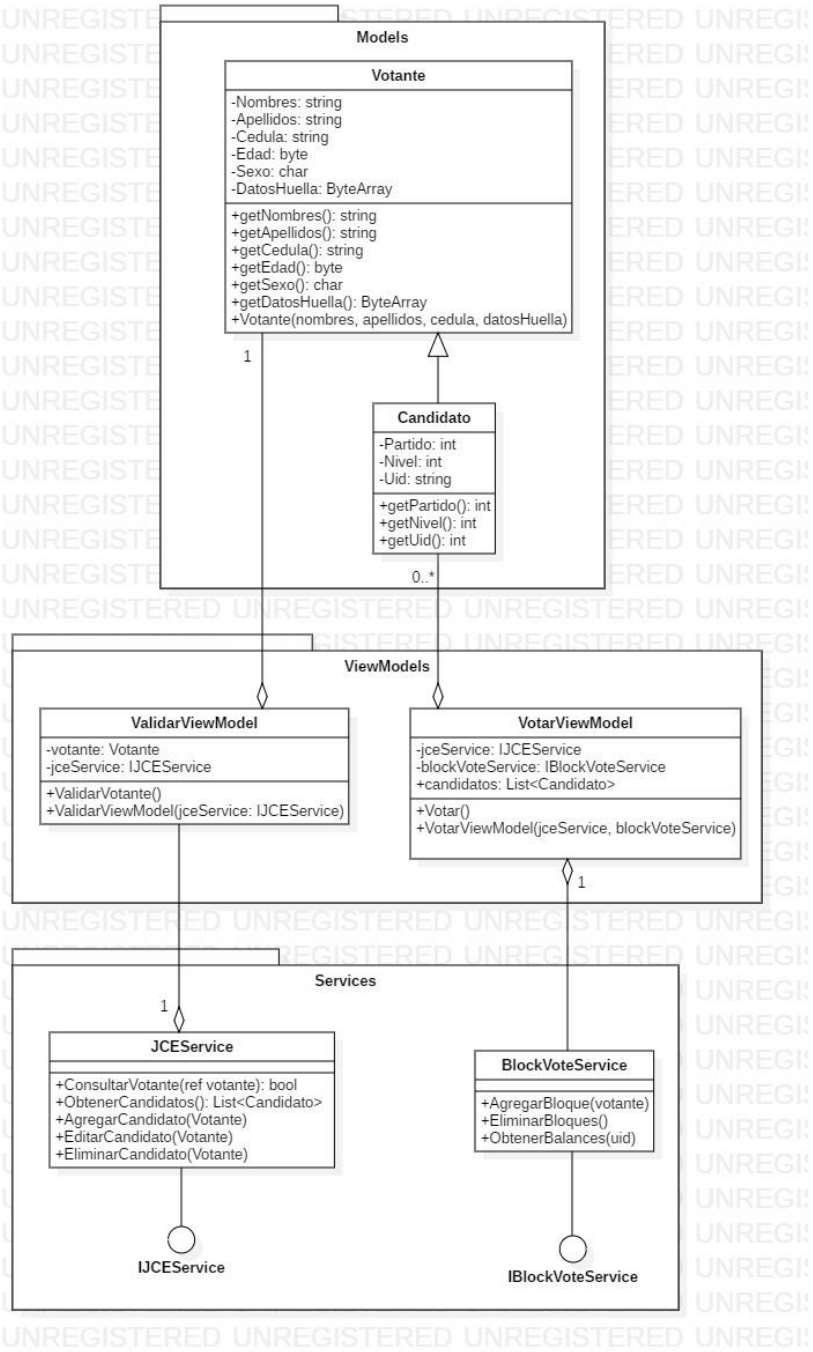


Figura 66: Diagrama de Clase de Aplicación de votación

Fuente: Elaboración propia

4.6.3.2. Cliente de Administración

El cliente de Administración permite administrar los candidatos, reiniciar la cadena de bloques y visualizar los resultados. Este es una aplicación de escritorio que utiliza el patrón arquitectónico MVVM.

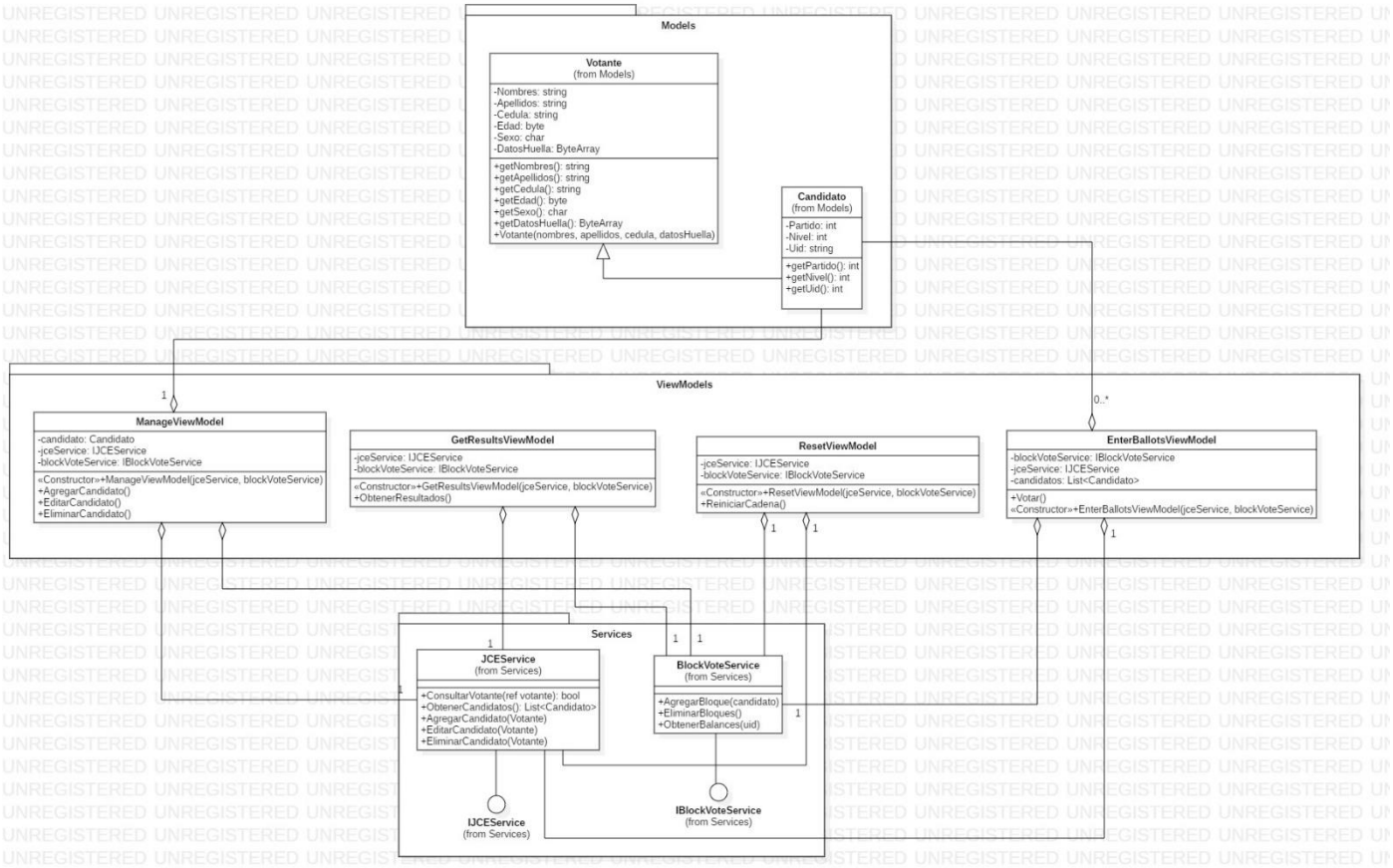


Figura 67: Diagrama de Clase de Cliente de Administración

Fuente: Elaboración propia

4.7. Bases de datos del sistema

A continuación, el diagrama de Entidad Relación de la base de datos. La JCE proveerá un Web Service que se conectará a la base de datos. El sistema BlockVote utilizara este servicio para validar a los votantes y para persistir a los datos relacionados a los candidatos.

4.7.1. Diagramas de Base de Datos

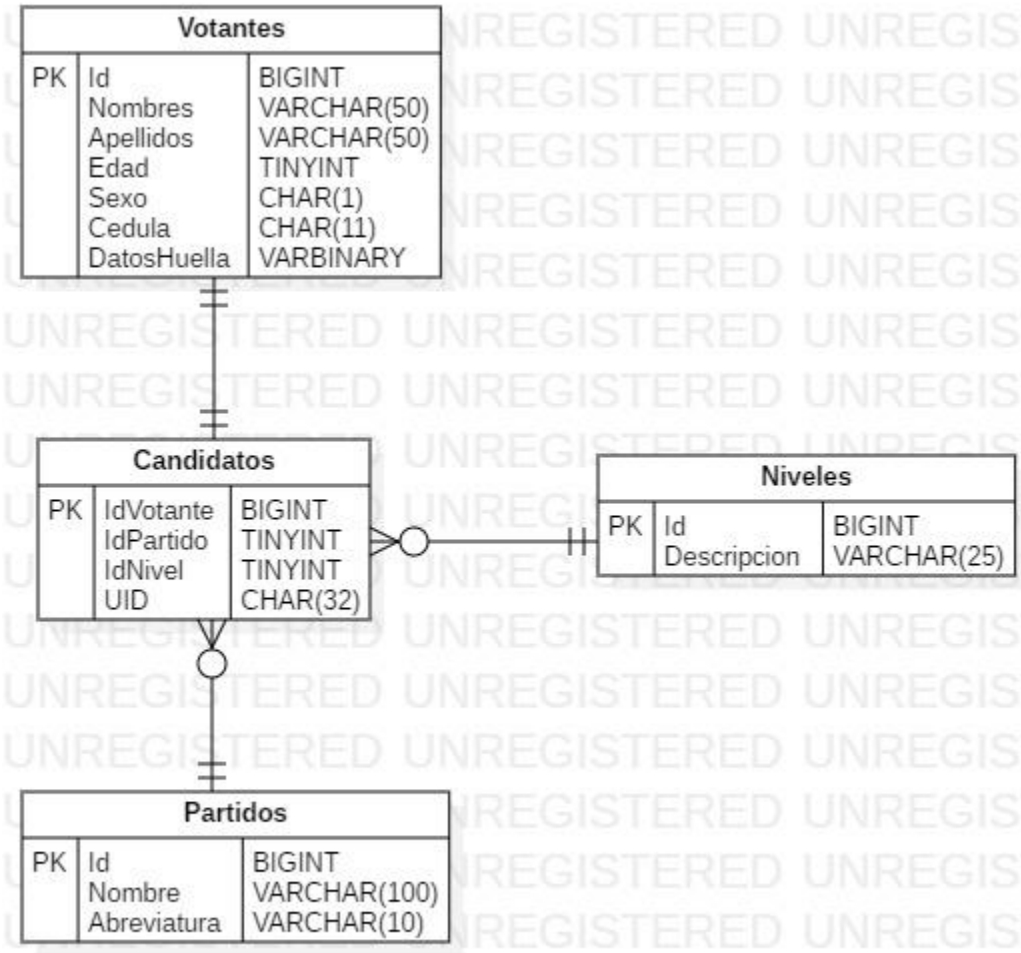


Figura 68: Diagrama de Entidad-Relación de BlockVote

Fuente: Elaboración propia

4.7.2. Sistema de Base de Datos

Como sistema de base de datos, recomendamos PostgreSQL, ya que es una base de datos de código abierto y gratuita, pero al mismo tiempo muy estable, confiable y segura.

4.8. Diseño de la Cadena de Bloques

La cadena de bloques de BlockVote se basa en que cuando un votante realiza su voto, en realidad está transfiriendo una crypto-moneda a el candidato seleccionado. Esta crypto-moneda no tiene valor comercial, sino para indicar la confianza del votante a ese candidato. De esta manera, se puede verificar si el voto se realizó correctamente si el candidato recibió una transferencia de la billetera del votante. Además, se pueden obtener los resultados durante y después del periodo de votación al observar los balances de los candidatos.

4.8.1. Distribución física y geográfica de nodos

Como se ha mencionado antes, la cadena de bloques funciona de forma descentralizada, lo que significa que se requieren de varios nodos para sustentarla. Para esto proponemos el establecimiento de servidores que servirán como nodos en cada junta electoral del país y de varios nodos especiales que servirán como validadores de transacciones. Estos son necesarios, porque para crear bloques, las estaciones de votación no utilizarán una Prueba de Trabajo (PoW), sino que, cada bloque será validado por estos nodos validadores mediante una Prueba de Autoridad (PoA).

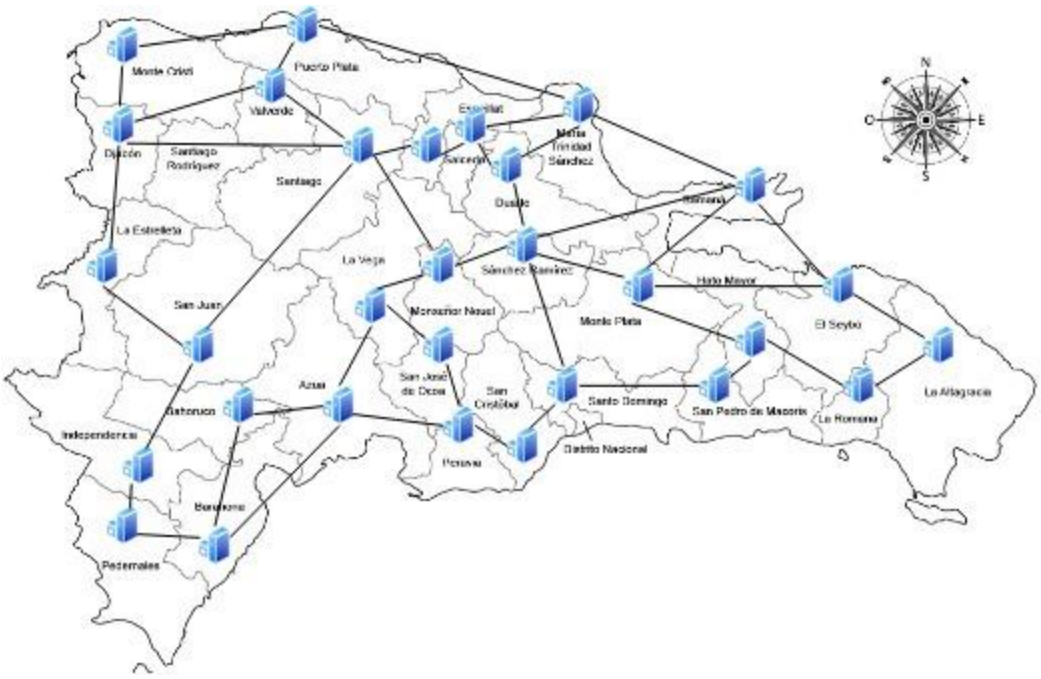


Figura 69: Distribución de nodos de la cadena de bloques

Fuente Elaboración propia

Los nodos validadores deben de ser administrados por organismos autónomos del sector público y privado. Algunos candidatos son: La Junta Central Electoral, la Cámara de Cuentas, el Banco Central, la Universidad Acción Pro-Educación y Cultura, la Pontificia Universidad Madre y Maestra, la Universidad Pedro Henríquez Ureña, entre otros.

Los nodos de las juntas electorales expondrán una interfaz, por la cual las estaciones de votación de una provincia se conectarán para agregar bloques. Las estaciones de votación instaladas en los colegios se comunicarán a los nodos de la junta electoral de esa provincia mediante HTTPS, para una transmisión segura de los votos.

4.8.2. Responsabilidades de las aplicaciones

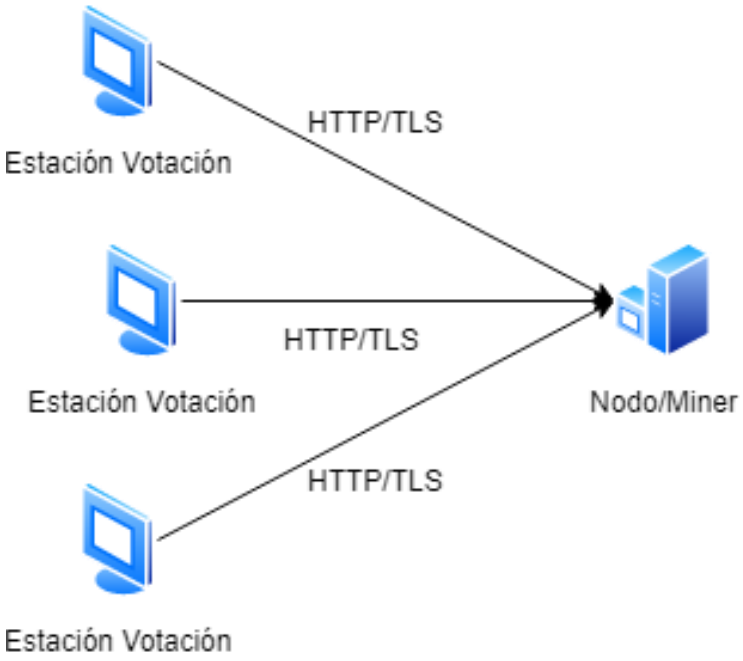


Figura 70: Conexión de las estaciones de votación a nodo

Fuente: Elaboración propia

Los clientes de votación realizaran el papel de las “aplicaciones billetera”. Las aplicaciones billetera son las encargadas de realizar transacciones en el mundo de las cripto-monedas. (Bitcoin Organization, 2019) En este contexto, son los clientes de votación que además de validar a los votantes, también realizan una transacción cuando se selecciona un candidato.

Los nodos son el equivalente a los programas de minería o “miners”, no solo almacenan una copia de la cadena de bloques, sino que también crean bloques y lo transmiten a todos los demás nodos.

El cliente de administración permite agregar bloques sin validación de los votantes, lo cual permite la integración entre el sistema de votación basado en papel y el SVE propuesto.

El cliente de administración permite, además, la generación de un par de llaves. Una llave privada que sirve para descifrar los votos y la pública, que es la que permite recibir los votos y es esta la que es utilizada por el cliente de votación para realizar la transferencia al candidato seleccionado. Esta llave publica es el equivalente a lo que en el contexto de las cripto-monedas se conoce como billetera o “wallet”.

El cliente de administración puede obtener los votos transferidos a los diferentes candidatos. Para obtener tales resultados, cada candidato debe llevar el papel generado al momento de registrarse en el sistema. Este papel contiene la llave privada, la cual es utilizada para desencriptar los votos transferidos, obteniendo así los balances o este caso, la cantidad de votos.

El cliente de administración puede reiniciar la cadena de bloques. Las razones para reiniciar la cadena de bloques son las siguientes:

- Para ahorrar espacio de almacenamiento: Dependiendo de la capacidad de los nodos, a estos se les podría agotar el espacio de almacenamiento.
- Para cumplir con el requisito de eliminar todas las boletas: En todos los SVE estudiados, existe un requisito que tienen en común y es el de eliminar las boletas, tanto físicas como virtuales.

4.8.3. Estructura de bloques

Los bloques que serán almacenados en la cadena de bloques tendrán la siguiente estructura:

Bytes	Campo	Descripción
32	PrevHash	Hash del bloque anterior en la cadena de bloques
32	Merkle Root	Es el hash derivado de los hashes de las transacciones
4	Time	Tiempo que durará el periodo de votación completo. Luego de que se expire este tiempo los nodos no aceptaran ningún otro bloque

Tabla 14: Estructura de la cabecera del bloque de BlockVote

Fuente: Elaboración propia

Para las transacciones, esta es la estructura.

Bytes	Campo	Descripción
Variable	TransactionInputCount	Cantidad de transacciones de entrada
Variable	TransactionInput	Lista de transacciones de entrada
Variable	TransactionOutputCount	Cantidad de transacciones de salida
Variable	TransactionOutput	Lista de transacciones de salida

Tabla 15: Estructura de una transacción del bloque de BlockVote

Fuente: Elaboración propia

La estructura del bloque que contiene tanto la cabecera como las transacciones es la siguiente:

Bytes	Campo	Descripción
72	BlockHeader	Cabecera del bloque
Variable	TransactionCount	Cantidad de transacciones
Variable	Transactions	Lista de Transacciones

Tabla 16:Estructura del cuerpo de transacciones del bloque de BlockVote

Fuente: Elaboración propia

4.9. Arquitectura y Despliegue

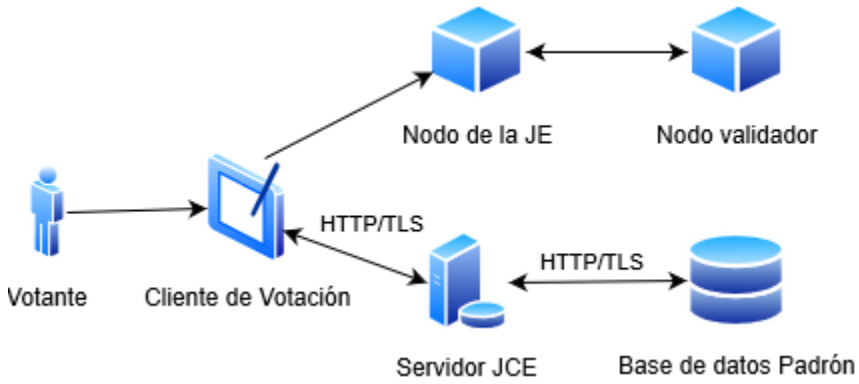


Figura 71: Despliegue del sistema BlockVote

Fuente: Elaboración propia

Esta es la arquitectura a nivel de nodos y equipos. El votante realiza su voto mediante un cliente con pantalla táctil y un lector de huellas dactilares. El cliente capta la cédula y la huella del votante y la compara con la huella almacenada en la base de datos de la JCE, de esta forma se valida que el votante es un ciudadano apto para votar. El cliente de votación obtiene una lista de candidatos junto con sus llaves públicas o direcciones de billeteras. Cuando el votante selecciona el candidato de preferencia, el cliente de votación genera un par de llaves para realizar una transferencia de un voto a dicho candidato. Por defecto la billetera temporal del votante tiene un voto por nivel, es decir que, en el nivel presidencial, cuando el votante selecciona un candidato, su billetera temporal tendrá un voto menos, luego en la siguiente lista, el votante seleccionara de nuevo y su billetera tendrá un voto menos y así un numero *n* de veces.

Para integrar ambos sistemas el administrador del sistema durante el tiempo de escrutinio puede habilitar el acceso al sistema saltándose la etapa de validación,

permitiendo así que los digitadores puedan ingresar votos por las boletas físicas validas captadas durante el periodo de votación clásico.

Para obtener los resultados en la etapa de conteo, el administrador puede obtener los balances utilizando las llaves privadas de los candidatos. Para esto los candidatos deben llevar sus llaves privadas e ingresarlas en el cliente de administración.

4.10. Prototipos de Interfaz Gráfica

Figura 72: Pantalla para cedula

Fuente: Elaboración propia

Figura 73: Pantalla para informar la colocación de huella dactilar en el dispositivo

Fuente: Elaboración propia

Figura 74: Pantalla para la selección del candidato presidencial

Fuente: Elaboración propia

Figura 75: Pantalla de confirmación de candidato

Fuente: Elaboración propia

Figura 76: Pantalla de administración de candidatos por niveles

Fuente: Elaboración propia

Figura 77: Pantalla para la creación, búsqueda, edición y eliminación de los candidatos presidenciales

Fuente: Elaboración propia

Figura 78: Pantalla para visualizar los resultados de los candidatos

Fuente: Elaboración propia

4.10. Estudio de Factibilidad de la Propuesta

Un SVE como este beneficia a la democracia, empodera a los votantes y facilita los procesos de electorales. Además, el uso de un SVE ayuda a disminuir los gastos en materiales gastables (marcadores, papel, papel del acta, tinta, etc.). Lo cual reduce la contaminación del medio ambiente provocados por los desechos. Sin embargo, una solución cualquiera que sea debe retornar algún beneficio para los interesados.

La factibilidad de una solución se puede dividir en tres:

1. Técnica: Disponibilidad de equipos y herramientas necesarias para implementar la solución.
2. Operativa: Disponibilidad de personal lo suficientemente capacitado y entrenado para implementar la solución.
3. Económica: Disponibilidad de los recursos monetarios para sostener la implementación de la solución.

4.10.1. Factibilidad Técnica

Para realizar esta solución es necesario componentes, que permita el reconocimiento del votante a través de datos biométricos. Para esto se cuentan con lectores de huellas con tecnología de punta y con gran precisión, que permiten validar si el ciudadano esta hábil para votar.

Esto es clave para garantizar la efectividad y confiabilidad del sistema, ya que este debe ser capaz de identificar cada ciudadano, utilizando datos sus datos biométricos. Obtener las huellas, nos permite reducir la coerción de votos, pero no evita que el votante sea coaccionado a votar por un candidato en específico, eso es algo personal y propio del votante.

Para almacenar los votos, utilizamos una arquitectura basada en cadena de bloques en lugar de una base de datos convencional, porque las cadenas de bloques por diseño, no permite la modificación de una transacción anterior y es muy tolerante a fallos. Las cadenas de bloques al funcionar en diferentes nodos que replican las transacciones a los otros nodos no tienen un solo punto de fallo, es decir, es casi imposible de interrumpir su servicio con un ataque DDoS.

La seguridad y la robustez de una cadena de bloques se fortalece al aumentar la cantidad de nodos que la sustentan, esto es observable en las cripto-monedas, donde para falsificar una transacción el atacante debe de contar con más del 50% del poder de procesamiento total de la red, y se dificulta conforme se van agregando mas nodos a la red. Esto hace de la cadena de bloques el medio ideal para almacenar información de gran valor como los votos o las boletas.

4.10.2. Factibilidad Operativa

Un SVE es un sistema difícil de desarrollar, sobre todo si se trata de uno que utilice cadena de bloques como medio para almacenar los votos. Por esto para desarrollar e implementar un sistema como este es necesario, personal humano capacitado en ciberseguridad y programación de cadena de bloques. Se requiere de personal especializado sobre todo en algoritmos de criptografía, porque la cadena de bloques está fuertemente basada en criptografía. Hoy en día hay una creciente preocupación por la ciberseguridad y también una creciente cantidad de profesionales enfocados en ciberseguridad, cada vez hay más cursos, diplomados y maestrías enfocadas en la capacitación en ciberseguridad y esto incluye la criptografía.

4.10.3. Factibilidad Económica

Toda solución, tiene un costo para implementarse y este sistema con semejante arquitectura tiene un costo elevado por la cantidad de equipos que requiere. El costo aproximado del SVE que JCE ha desarrollado en conjunto con DIGIWORLD S.R.L es de RD$1,017,093,000.00 y esto solo incluye recursos tecnológicos, según como lo indica el Contrato Para Adquisición De Bienes que la JCE y DIGIWORLD S.R.L acordaron (Lantigua, 2019).

Solo en boletas la JCE gasta alrededor de RD$ 44,827,595.84 cada elección (Junta Central Electoral, 2016). Este es un gasto recurrente que se repite cada cuatro años.

Implementar un SVE como el propuesto tendría un costo de alrededor de RD$ 810,499,421.00. El costo de las computadoras de gama baja o media que servirían como nodos seria de RD$ 156,800.00 y el costo de monitores con pantalla táctil de 7 pulgadas sería de RD$ 50,805,180.00. Consideramos que una aplicación como el cliente de votación puede correr en minicomputadoras como los Raspberry Pi 3, entonces el costo aproximado de estos seria de RD$ 127,012,950.00 y el costo aproximado de los lectores de huellas sería de RD$ 16,536,588.00. Los Verifi P6000TPM son lectores de alta precisión, muy duraderos y de buena calidad.

Producto	**Precio Unitario**	**Cantidad**	**Precio Total**
HP DC8200, Intel Core i3, 4GB RAM, 250GB HDD (Nodos)	4,900.00	32	156,800.00
Pantalla Touch STONE STI056WT-01	1,020.00	16603 x 3	50,805,180.00
Raspberry Pi 3 kit	2,550.00	16603 x 3	127,012,950.00
Verifi P6000TPM Lector de huella	12,699.00	16603 x 3	632,524,491.00
		Total	**810,499,421.00**

Tabla 17: Costo aproximado de los equipos para BlockVote

Fuente: Elaboración propia

La diferencia entre el costo aproximado del SVE de la JCE menos el total presentado en la Tabla 17, da como resultado RD$ 206,593,579.00, ese monto sería el ahorro en el costo de los equipos.

Esta solución reduciría el uso de las boletas, marcadores y tinta; lo cual reduciría el gasto en la producción y compra de estos materiales. También reduciría el uso del papel, lo cual beneficia positivamente el medio ambiente.

CONCLUSION

Los sistemas de votación tradicionales basados en papel requieren de mucha intervención humana, lo que aumenta el porcentaje de error a la hora de votar o en el proceso de escrutinio y conteo de boletas. Estos errores pueden desviar el curso de las elecciones y lastimar la democracia. Por esto, en países como Estonia y Noruega se han implementado sistemas de votación electrónicos que explotan los avances tecnológicos para mitigar estos errores, sin embargo, se han demostrado que estos sistemas aún son susceptibles a algunos ataques, como los ataques DDoS.

La naturaleza descentralizada de Cadena de Bloques hace que las criptomonedas como el Bitcoin, invulnerables ante ataques DDoS, ya que la cadena de bloques esta replicada en todos los nodos de red, lo que significa que, aunque se puedan anular varios nodos, ésta todavía sigue funcionando sin problemas.

La arquitectura de cadena de bloques también tiene otra característica importante para asegurar a sus usuarios: El anonimato. En el caso de las criptomonedas, sus usuarios pueden realizar transacciones sin ser vinculados con ellos.

Teniendo en cuenta estas características y otros mecanismos de seguridad que la cadena de bloques provee, hemos propuesto un SVE basado en cadena de bloques, ya que estas características son análogas a las que debe proveer un SVE seguro. El anonimato es análogo al derecho de secreto al voto, donde en el SVE propuesto aquí, los votantes no tienen vinculación con los votos.

El SVE propuesto cumple con los requisitos básicos:

- Autenticación: El SVE propuesto valida el votante contra el Padrón Electoral

- Unicidad: El sistema permitirá votar sólo una vez. Después de haber votado, el votante será marcado en la cadena de bloques como inhabilitado para votar por ese periodo de elección.
- Eficacia: El voto se procesa como una transferencia a la billetera del candidato seleccionado.
- Integridad: Una vez almacenado el bloque con la transacción del voto, este no puede ser modificado, ya que es almacenado en una cadena de bloques.
- Verificabilidad: En el proceso de conteo, los candidatos llevan sus llaves privadas para obtener sus balances, esto es, la cantidad de votos transferidos a sus billeteras.
- Confiabilidad: Al tener una arquitectura de cadena de bloques, no existe un punto común de falla, es decir, está descentralizado.
- Discreción: A la hora de votar, el cliente genera un par de llaves que permiten realizar una transferencia a los candidatos de forma anónima. Estas llaves se descartan una vez realizada la transferencia.
- Conveniencia: Se le presenta una interfaz sencilla, con pantalla táctil y se le pide poca información al votante: el número de cédula electoral y poner su huella dactilar.
- Costo-Efectivo: El cliente de votación puede ejecutarse en minicomputadoras como los Raspberry Pi 3 y los nodos pueden funcionar en ordenadores de gama media con algún sabor de Linux como sistema operativo. Esto reduce los costos de licenciamiento y equipos.

RECOMENDACIONES

En esta solución se cuenta con un nodo por cada provincia del país, es decir 32 nodos, más los nodos validadores. Por lo anterior se puede decir que la cadena de bloques de BlockVote es lo suficientemente robusta, pero, a pesar del auge tecnológico que ha tenido el país gracias a los esfuerzos de las autoridades y los proyectos como Republica Digital, todavía existen provincias o pueblos distantes donde no se puede establecer una conexión confiable a internet, lo cual reduce la cantidad de nodos y, por lo tanto, reduce la seguridad y robustez de la cadena de bloques.

Proponemos como alternativa el servicio de cadena de bloques que provee el servicio en la nube de Azure, de esta forma se puede multiplicar la cantidad de nodos y alcanzar mayor seguridad y robustez.

Una vez que un candidato se registra en BlockVote, el sistema genera una llave privada que puede ser utilizada para verificar los votos que le han sido transferidos. Mantener esta información segura es sumamente importante, por tanto en lugar de solo imprimir la llave privada, también estos podrían utilizar una aplicación móvil de billetera que le permitiría guardar de forma segura la llave privada; otra alternativa podría ser el utilizar una billetera fuera de conexión como por ejemplo una memoria USB, donde a la hora de realizar el conteo, estos conectan sus billeteras (que son memorias USB) en el ordenador donde se está ejecutando el cliente de administración y este automáticamente puede obtener las llaves de las billeteras conectadas.

En cuanto a los votantes estos podrían verificar si su voto fue realizado correctamente utilizando una aplicación móvil de verificación. La cual puede escanear el código QR y la aplicación mostraría por cual candidato votó. Esto no se incluyó, ya

que, durante nuestra investigación, notamos que todos los SVE que se han implementado, muestran el proceso de verificación como algo opcional.

En cuanto a la ley, proponemos que, a la hora de inscribir las candidaturas, los candidatos asistan personalmente y puedan registrarse en BlockVote y que puedan recibir su llave privadas. También que a la hora de elegir las instalaciones donde se realizarán las votaciones, se consideren lugares que tengan buen servicio eléctrico y buena conexión a internet. También que se anuncie los colegios en donde se instalará el sistema, junto con un instructivo para usarlo.

BIBLIOGRAFIA

AS Sertifitseerimiskeskus. (s.f.). *The Estonian ID Card and Digital Signature Concept: Principles and Solutions.* Obtenido de The_Estonian_ID_Card_and_Digital_Signature_Concept: https://www.id.ee/public/The_Estonian_ID_Card_and_Digital_Signature_Concept.pdf

ASOBAMCARIA. (2017). *Blockchain: mirando más allá del Bitcoin.* Colombia: 1084.

Ayed, A. B. (2017). A Conceptual Secure Blockchain-Based Electronic Voting System. *International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3*.

Basantes, A. K. (2018). *Análisis De La Utilización De La Tecnología Blockchain Para La Gestión De La Información En Sistemas De Alarmas Residenciales.*

Bitcoin Organization. (2019). *Developer Guide: Bitcoin Organization*. Retrieved from Bitcoin Web Site: https://bitcoin.org/en/developer-guide

Constitución de la republica Dominicana (Art. 124 2010).

Dolader Retamal, C., Bel Roig, J., & Muñoz Tapia, J. L. (s.f.). *LA BLOCKCHAIN: FUNDAMENTOS, APLICACIONES Y RELACIÓN CON OTRAS TECNOLOGÍAS DISRUPTIVAS.* Catalunya.

Drew Springall, T. F. (2014). *Security Analysis of the Estonian Internet Voting System.* Scottsdale, Arizona, USA: University of Michigan, Open Rights Group, U.K.

Erich Gamma, R. H. (1998). *Design patterns: Elements of Reusable Software.* Indianapolis: Addison Wesley.

Gritzalis, D. (2002). Secure Electronic Voting New trends, new threats... *7th Computer Security Incidents Response Teams Workshop Syros.* Greece. Obtenido de https://www.terena.org/activities/tf-csirt/meeting7/gritzalis-electronic-voting.pdf

INTECO. (2014). *Una moneda criptográfica.* Madrid.

Internet Policy Institude. (2001). *Report of the National Workshop on Internet Voting: Issues and Research Agenda.* Maryland: National Science Foundation.

Junta Central Electoral. (2010). *Presentación Unidades EyT.* Retrieved from https://issuu.com/publicacionesjce/docs/presentacioneyt_prensa_02-04-2010_20101011_142511

Junta Central Electoral. (2016). *Compras y Contrataciones Abril Junio 2016.* Obtenido de https://jce.gob.do/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=8125&language=es-ES&PortalId=1&TabId=240

Junta Central Electoral. (2017). *Informe Sobre Los Equipos Adquiridos En Las Elecciones 2016.* Obtenido de https://jce.gob.do/portaltransparencia/Repositorio/Vista-Escritorio?Command=Core_Download&EntryId=9561

Junta Central Electoral. (2019). *Respuestas de Cuestionario JCE.* Santo Domingo.

Kenneth E Kendall, J. E. (2011). *Análisis y diseño de sistemas.* México: Pretince Hall.

Lantigua, L. B. (2019). *Contrato Para Adquisición De Bienes Para Voto Automatizado JCE.* Obtenido de https://jce.gob.do/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=12847&language=es-ES&PortalId=1&TabId=240

Ledger. (2019). *Ledger Nano S.* Obtenido de https://shop.ledger.com: https://cdn2.shopify.com/s/files/1/2974/4858/products/nanohero.png?v=1562751818

Ley Electoral No. 275-97 (1997).

Norwegian Minitry of Local Goverment And Regional Development. (9 de Septiembre de 2011). *Use case specification: 9.1 Authentication.* Obtenido de Government.no: https://www.regjeringen.no/globalassets/upload/krd/kampanjer/valgportal/e-valg/anskaffelse/use_case_9.1_authentication.pdf

NSW Electoral Commission. (2019). *iVote® refresh project for the 2019 NSW State election.* Sydney.

OSCE/ODIHR Election Expert Team. (2012). *Norway Internet Voting Pilot Project Local Government Elections 12 September 2011.* Warsaw. Obtenido de https://www.osce.org/odihr/88577?download=true

Pressman, R. S. (2010). *Ingenieria del Software. Un enfoque práctico.* New York: McGraw-Hill.

Schmuller, J. (n.d.). Aprendiendo UML en 24 Horas. In *Aprendiendo UML en 24 Horas.* Prentice Hall.

Sommerville, I. (2011). *Ingeniería de Software.* Naucalpan de Juárez: Pearson Educación de México, S.A.

Tools: zen-tools.com. (n.d.). Retrieved from zen-tools.com: http://zen-tools.com/images/projects/RUCM_files/ss1.jpg

GLOSARIO

Sistema de Votación Electrónico (SVE): “Un sistema de votación electrónico (e-voting) es un sistema de votación en el cual los datos de las elecciones son almacenados, persistidos y procesados en primer lugar como información digital” (Gritzalis, 2002 como citado en VoteHere, Inc., 2002)

Sistema Electrónico de Captación Directa (DRES): Son SVE que solo permiten realizar votos desde los centros electorales.

i-Voting: Se refiere a la capacidad de realizar votos desde cualquier dispositivo con conexión a internet. Los SVE de este tipo son más convenientes que los DRES, pero conllevan más riesgos a nivel de seguridad.

Criptografía: “Criptografía es la práctica y estudio de técnicas para la comunicación segura en presencia de terceros” (The CryptoParty handbook, 2013)

Criptografía de Llave Pública: En este tipo de criptografía se utilizando dos llaves, una pública y otra privada. Con la llave pública se cifra y con la llave privada se descifra la información cifrada con la llave pública.

Criptomoneda: Es una moneda virtual, cuyo valor se sustenta en el tiempo y energía invertidos en generarla. Estas monedas no son reguladas por instituciones u organizaciones. Son muy difíciles de imitar, ya que se basan en criptografía para generarlas.

Cadena de Bloques: “Cadena de bloques es una estructura de datos que contiene bloques de transacciones. Cada bloque en la cadena está conectado al bloque anterior en la cadena” (Ayed, 2017)

Hash: Es un conjunto de caracteres alfanuméricos de longitud fija. Es la representación de alguna información o dato, sin importar su longitud.

Resiliencia: Se refiere a la capacidad de recuperación de su operación de un sistema informático después de un desastre.

Negación de Servicio Distribuido (DDoS): Es un tipo de ataque, donde se construye o se infecta varios computadores para que estos puedan saturar un servidor objetivo con peticiones, como consecuencia el servidor no puede responder a las peticiones auténticas, porque tiene que manejar las peticiones de los computadores infectados.

Prueba de Trabajo (PoW): Provoca que para calcular o crear bloques nuevos se deba realizar tareas con alto coste computacional.

Minero o Miner: Son software dedicados a crear bloques válidos para una cadena de bloques, esto es comúnmente realizado a través de PoW.

ANEXOS

Universidad APEC

UNAPEC

DECANATO DE INGENIERÍA E INFORMÁTICA

ESCUELA DE INFORMÁTICA

"ANTEPROYECTO"

"ANÁLISIS Y DISEÑO DE UN SISTEMA DE VOTACIÓN ELECTRÓNICO BASADO EN CADENA DE BLOQUES PARA LA JUNTA CENTRAL ELECTORAL DE LA REPUBLICA DOMINICANA PARA EL AÑO 2024"

SUSTENTANTES:

REINIS ESPINAL CRUZ 2015-0395

VICTOR D. MONTERO ADAMES 2015-0569

DEPARTAMENTO DE SOCIALES
PROYECTO DE TRABAJO DE GRADO
APROBADO
FIRMA
FECHA 26-3-19

PROFESOR:

EDDY GUZMÁN ALCÁNTARA SOLANO

Santo Domingo, D.N.

Marzo 2019

Universidad APEC

UNAPEC

DECANATO DE INGENIERÍA E INFORMÁTICA

ESCUELA DE INFORMÁTICA

“ANTEPROYECTO”

“ANÁLISIS Y DISEÑO DE UN SISTEMA DE VOTACIÓN ELECTRÓNICO BASADO EN CADENA DE BLOQUES PARA LA JUNTA CENTRAL ELECTORAL DE LA REPUBLICA DOMINICANA PARA EL AÑO 2024”

SUSTENTANTES:

REINIS ESPINAL CRUZ 2015-0395

VICTOR D. MONTERO ADAMES 2015-0569

PROFESOR:

EDDY GUZMÁN ALCÁNTARA SOLANO

Santo Domingo, D.N.

Marzo 2019

1. INDICE

2. TEMA DE INVESTIGACIÓN

ANÁLISIS Y DISEÑO DE UN SISTEMA DE VOTACIÓN ELECTRÓNICO BASADO EN CADENA DE BLOQUES PARA LA JUNTA CENTRAL ELECTORAL DE LA REPUBLICA DOMINICANA PARA EL AÑO 2024

3. INTRODUCCIÓN

Esta es la propuesta del diseño de un sistema de votación electrónico cuya forma de persistir los votos se hace mediante Blockchain. Se presentará el marco teórico, el diseño metodológico, las bibliografías y referencias sobre la que se basa el trabajo propuesto, así como un índice preliminar del mismo.

El sistema de votación de la Junta Central Electoral (JCE) de la Republica Dominicana ha tenido variaciones de procedimientos de votación con el tiempo; procedimientos poco confiables para la población dominicana, la cual ha aceptado los cambios para que cada fase hacia el poder presidencial sea transparente y eficaz. La JCE aún persiste buscando nuevas maneras con fines de garantizar un proceso diáfano y, por consiguiente, proponemos una de las mejores tecnologías a nivel mundial que maneja datos encriptados conocida como "*BlockChain"* (Cadena de bloques) para aplicar la misma en nuestro sistema de votación.

El BlockChain integrado en nuestro sistema de votación permitirá almacenar data encriptada en una base de datos descentralizada con total anonimidad compartiendo la información en máquinas distribuidas sin posibilidad de alterar información existente, por lo que esta propuesta está enfocada en el estudio y planeamiento para una futura implementación teniendo encuentra todos los puntos clave.

4. JUSTIFICACIÓN

Se propone un diseño para un sistema de votación electrónico basado en la tecnología cadena de bloques (Blockchain) para las elecciones del 2024 en República Dominicana, teniendo en cuenta que nuestro país carece de procedimientos veraces y transparentes en cuanto a los sufragios se refiere. La tecnología de la cadena de bloques (Blockchain) nos permite hacer unas elecciones verídicas y totalmente transparentes ya que esta consiste en tener un registro inalterable de cualquier dato mediante un proceso de encadenamiento en bloques.

En previas ocasiones las elecciones han presentado dificultades, por ejemplo, a la hora de verificar los resultados, llevando esto a conflictos entre la sociedad y los delegados y hasta los mismos candidatos. Es por esto por lo que se decidió elaborar una propuesta para el uso de cadena de bloques (Blockchain) en las elecciones del país.

Un sistema como este podría acabar con las “elecciones casi arbitrarias” por parte de los gobiernos en curso, dando un resultado más concreto y válido a la hora de elegir nuestros representantes, quienes son los encargados de llevar nuestro país a la mejora continua y/o desarrollo.

5. DELIMITACIÓN DEL TEMA Y PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN

La Junta Central Electoral (JCE) es un organismo autónomo, encargado de realizar y organizar elecciones de diferentes niveles. Esto incluye la recolección de votos, conteo de estos y además de emitir los resultados. (Constitución de la republica Dominicana, 2010)

La República Dominicana se encuentra afectada de forma muy notable por la corrupción en todos los niveles y procesos gubernamentales. Unos de estos procesos son el de las elecciones electorales, donde sufragio tras sufragio los resultados obtenidos en la misma se ponen en tela de juicio debido a los métodos obsoletos y de fácil manipulación que se utilizan para recolectar las votaciones. Debido a esto todos los procesos y métodos anteriormente usados resultan ser de poca veracidad para el pueblo dominicano y los mismos candidatos, en especial lo que no salen victoriosos. Un ejemplo claro y en el cual está basada la investigación son los constantes fraudes electorales que ocurren al utilizar dispositivos electrónicos para la recolección de los votos. Una vez uno de estos dispositivos es vulnerado, todos los demás dispositivos con las mismas características pueden serlo por igual.

Que un atacante logre vulnerar un dispositivo de votación masiva en el justo momento que se están presentando los votos de una nación pone en riesgo urgente la seguridad nacional y el futuro de esta. Considerando esto, es de suma importancia la utilización de tecnologías que permitan mantener la integridad de dicha actividad en donde sea que ocurran elecciones electrónicas, pero en el caso de nuestra investigación enfocado a la República Dominicana.

La mejor tecnología para llevar procesos de ese tipo que permitan la escalabilidad y presten primordial importancia a la integridad de los datos es conocida como BlockChain o cadena de bloques. Implementando esta tecnología se lograría asegurar la integridad de los datos que se manipulan en el proceso.

6. OBJETIVOS GENERALES Y ESPECÍFICOS

6.1 Objetivo General

- Proponer un Diseño de un sistema de votación electrónico utilizando Cadena de Bloques, en las elecciones electorales de la Republica Dominicana en el año 2024.

6.2 Objetivos Específicos

- Diagnosticar el proceso de elecciones de la República Dominicana en los últimos 12 años.
- Analizar los sistemas de votaciones electrónicos utilizados por la JCE anteriormente.
- Determinar las ventajas y desventajas de un sistema de votación electrónico.
- Analizar teóricamente la tecnología de cadena de bloques.
- Analizar y Diseñar un sistema de votación más seguro.

7. MARCO TEÓRICO REFERENCIAL

7.1 Antecedentes del problema

Los sistemas de votos electrónicos no son algo nuevo o solo de este siglo. De hecho, en los años 80 David Shaum diseñó un sistema de votación que usa criptografía de llave pública. Este sistema mantenía la identidad de los votantes anónima, para desvincularlos de las boletas. (Ayed, 2017)

Estonia fue el primer país en el mundo en implementar un sistema de votación electrónico. Estonia lo ha estado utilizando desde el año 2007, y le ha resultado beneficioso. Aunque este sistema no utiliza Blockchain como medio para persistir los votos. Este sistema utiliza la identificación que todos los ciudadanos estonios tiene, la cual tiene un chip integrado que el sistema utiliza para procesar votos. (Ayed, 2017) Otros países han optado por un sistema electrónico de votación, tales como: Estados Unidos y Noruega.

Desde el año 2000 la Junta Central Electoral (JCE), ha estado realizando esfuerzos para automatizar las elecciones. En el 2002 la JCE introduce el escaneo de las Actas de Votación y en el año 2004 introduce el mecanismo de digitación ciega y aleatoria el cual consiste en mostrar parcialmente la boleta al digitador, de modo que los datos sensitivos sean protegidos. Luego en el año 2008 la JCE pudo integrar un dispositivo portátil, robusto que permitiera realizar casi todo el proceso de escanear, analizar y transmitir las boletas. A este dispositivo se nombró como “EyT” y este fue utilizado en las elecciones del 2012 de forma exitosa. (Junta Central Electoral, 2017)

La JCE, en busca de mejorar el proceso de las elecciones, de reducir el tiempo de respuesta y disminuir la complejidad del proceso de las elecciones Congresuales y

Municipales, contrato los servicios de Indra Sistemas, S.A, para automatizar las elecciones del 2016. Estos equipos no cumplieron su objetivo, resultando en fracaso: En ninguna prueba se pudo conseguir que se transmitiera más del 74% de los Colegios Electorales que participaban en cada prueba. (Junta Central Electoral, 2017)

Recientemente, se ha acordado entre varios partidos y la JCE, el uso de un sistema de voto automático. Este no tiene nombre comercial, pero es un sistema desarrollado por la JCE para realizar las votaciones de las primarias, tanto abiertas como cerradas. Si bien este sistema será el que se utilizará en las primarias, se está contemplando su uso en las elecciones del 2020.

7.2 Antecedentes Bibliográficos

"El Poder Ejecutivo lo ejerce el Presidente o la Presidenta de la República, quien será elegido o elegida cada cuatro años por voto directo." (Constitución de la republica Dominicana, 2010)

"Los derechos fundamentales reconocidos en esta Constitución determinan la existencia de un orden de responsabilidad jurídica y moral, que obliga la conducta del hombre y la mujer en sociedad. En consecuencia, se declaran como deberes fundamentales de las personas los siguientes: Votar, siempre que se esté en capacidad legal para hacerlo y Velar por el fortalecimiento y la calidad de la democracia, el respeto del patrimonio público y el ejercicio transparente de la función pública." (Constitución de la republica Dominicana, 2010)

“La Junta Central Electoral velará porque los procesos electorales se realicen con sujeción a los principios de libertad y equidad en el desarrollo de las campañas y transparencia en la utilización del financiamiento. En consecuencia, tendrá facultad para reglamentar los tiempos y límites en los gastos de campaña, así como el acceso equitativo a los medios de comunicación.” (Constitución de la republica Dominicana, 2010)

“Disponer cuantas medidas considere necesarias para resolver cualquier dificultad que se presente en el desarrollo del proceso electoral, y dictar, dentro de las atribuciones que le confiere la ley, todas las instrucciones que juzgue necesarias y/o convenientes, a fin de rodear el sufragio de las mayores garantías y de ofrecer las mejores facilidades a todos los ciudadanos aptos para ejercer el derecho al voto.” (Ley Electoral No. 275-97)

“El secreto del voto es, a la vez, un derecho y un deber para el elector. A nadie le es lícito, bajo ningún pretexto, excepto a la persona que le ayude a prepararlo, cuando así lo permita esta ley, averiguar por cuáles candidatos o en qué sentido ha votado. Tampoco le está permitido al elector exhibir, de modo alguno, la boleta con que vote, ni hacer ninguna manifestación que signifique violar el secreto del voto.” (Ley Electoral No. 275-97)

"El sistema basado en Cadena de Bloques será seguro, confiable y anónimo, y ayudará a incrementar el número de votantes, así como la confianza de los ciudadanos en sus gobiernos" (Ayed, 2017)

"La Cadena de Bloques será verificable y distribuida públicamente, de forma que nadie será capaz de corromperla" (Ayed, 2017)

Sobre las debilidades de los sistemas de votación electrónicos tanto centralizados como descentralizados, Chica (2018) afirma lo siguiente:

> Las brechas más importantes encontradas en los sistemas que utilizan protocolos tradicionales son estos que tienen que ver con la seguridad, y estos pueden ser minimizados usando Cadena de Bloques, el cual se ha mostrado sus muchos usos en criptomonedas como Bitcoin o Etherium, donde este tipo de tecnología ha brindado muchos beneficios. (p. 66)

"Las funciones Hash son funciones que toman una entrada de longitud variable y retorna un valor de longitud fija, también conocido como un "digest"." (Houtven, 2017)

"Un sistema de votación electrónico es un sistema de votación en el cual la elección es grabada, almacenada y procesada en primer lugar como información digital" (Gritzalis, 2002)

“Crear un sistema de votación en línea seguro requiere el uso de mecanismos de seguridad robustos que son relativamente complejos de diseñar.” (Rodríguez-Henríquez & Ortiz-Arroyo, 2007)

"La raíz merkle es almacenada en la cabecera del bloque. Cada bloque también persiste el hash de la cabecera del bloque anterior, encadenado los bloques juntos. Esto asegura que la transacción no puede ser modificada sin modificar el bloque que lo introdujo y los bloques que le siguen." (Bitcoin Organization, 2019)

Algunas clases de sistemas son “sistemas críticos” en los que la falla del sistema podría derivar en una lesión a individuos, daño al ambiente o pérdidas económicas mayores. Los ejemplos de sistemas críticos incluyen sistemas embebidos en dispositivos médicos, como una bomba de insulina (crítica para la protección), sistemas de navegación de aeronaves (críticos para la misión) y sistemas de transferencia de dinero en línea (críticos para la empresa). (Sommerville, 2011)

7.3 Definición de términos básicos o glosario

Sistema de Votación Electrónico (SVE): “Un sistema de votación electrónico (e-voting) es un sistema de votación en el cual los datos de las elecciones son almacenados, persistidos y procesados en primer lugar como información digital” (Gritzalis, 2002 como citado en VoteHere, Inc., 2002)

Sistema Electrónico de Captación Directa (DRES): Son SVE que solo permiten realizar votos desde los centros electorales.

i-Voting: Se refiere a la capacidad de realizar votos desde cualquier dispositivo con conexión a internet. Los SVE de este tipo son más convenientes que los DRES, pero conllevan más riesgos a nivel de seguridad.

Criptografía: “Criptografía es la práctica y estudio de técnicas para la comunicación segura en presencia de terceros” (The CryptoParty handbook, 2013)

Criptografía de Llave Pública: En este tipo de criptografía se utilizando dos llaves, una pública y otra privada. Con la llave pública se cifra y con la llave privada se descifra la información cifrada con la llave pública

Criptomoneda: Es una moneda virtual, cuyo valor se sustenta en el tiempo y energía invertidos en generarla. Estas monedas no son reguladas por instituciones u organizaciones. Son muy difíciles de imitar, ya que se basan en criptografía para generarlas.

Cadena de Bloques: “Cadena de bloques es una estructura de datos que contiene bloques de transacciones. Cada bloque en la cadena está conectado al bloque anterior en la cadena” (Ayed, 2017)

Hash: Es un conjunto de caracteres alfanuméricos de longitud fija. Es la representación de alguna información o dato, sin importar su longitud.

Estructura de Datos: Es la forma en que se ordenan y almacenan los datos.

Ciber-Delincuente o Ciber-Criminal: Persona con gran habilidad para la ciencia de computación y que utiliza dicha habilidad para realizar fechorías a través de los medios electrónicos.

Resiliencia: Se refiere a la capacidad de recuperación de un sistema informático después de un desastre.

Lenguaje de Modelado Unificado (UML): “El Lenguaje de Modelado Unificado es un conjunto compuesto por 13 diferentes tipos de diagrama para modelar sistemas de software” (Sommerville, 2011)

Documento de Visión: Documento donde se establece el alcance y los objetivos de un proyecto de software.

Especificación de Requerimientos de Software (ERS): "Una especificación de requerimientos de software (ERS) es un documento que se crea cuando debe especificarse una descripción detallada de todos los aspectos del software que se va a elaborar, antes de que el proyecto comience" (Pressman, 2010)

Especificación de Diseño de Software (EDS): Es una especificación que detalla con figuras la composición y arquitectura de un sistema de software. Esta es independiente del lenguaje que se utilice.

Patrones de Diseño: Es una descripción de un problema y su solución, sin tener que repensar en dicha solución otra vez. Es decir, es una solución reutilizable.

Aplicación Centralizada: Son aquellas cuya lógica está en un solo nodo y sus clientes se conectan a esta para utilizar sus servicios.

Aplicación Descentralizada: Son aquellas en la cual la misma aplicación esta replicada en diferentes nodos, de modo que todos son clientes y servidores al mismo tiempo. Bitcoin es un ejemplo de esta.

Voto: Es la preferencia de un candidato ante otros en una elección.

Boletas: Es papel donde se marca el candidato por el cual se desea votar.

8. DISEÑO METODOLÓGICO

8.1 Enfoque, tipo y diseño de la investigación

Este trabajo tiene un enfoque cualitativo, ya que consiste en el análisis y diseño de un sistema, no en la recopilación de datos numéricos, y, por lo tanto, se realizará una investigación aplicada. Se presentarán los requerimientos y la arquitectura del sistema propuesto, así como un costo aproximado del mismo.

Se utilizarán un método deductivo, ya que se examinarán los sistemas de votaciones electrónicos en general para obtener un análisis y diseño de un sistema votación que utilice Cadena de Bloques como principal medio de almacenamiento de los votos.

8.2 Técnicas e instrumentos de recolección de datos o información

Se consultarán y entrevistarán a expertos, documentos institucionales, especificaciones, estándares, entre otros.

9. FUENTES DE DOCUMENTACIÓN

9.1 Primarias

Ayed, A. B. (2017). A Conceptual Secure Blockchain-Based Electronic Voting System. *International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3*.

Bitcoin Organization. (2019). *Developer Guide: Bitcoin Organization*. Obtenido de Bitcoin Web Site: https://bitcoin.org/en/developer-guide

Junta Central Electoral. (2017). *INFORME SOBRE LOS EQUIPOS ADQUIRIDOS EN LAS ELECCIONES 2016.*

Ley Electoral No. 275-97 (1997).

Nakamoto, S. (s.f.). *Bitcoin: A Peer-to-Peer Electronic Cash System.*

Pressman, R. S. (2010). *Ingenieria del Software. Un enfoque práctico.* New York: McGraw-Hill.

Sommerville, I. (2011). *Ingeniería de Software.* Naucalpan de Juárez: Pearson Educación de México, S.A.

9.2 Segundarias

Constitución de la republica Dominicana (Art. 124 2010).

Gritzalis, D. (2002). Secure Electronic Voting New trends, new threats... *7th Computer Security Incidents Response Teams Workshop Syros.* Greece. Obtenido de https://www.terena.org/activities/tf-csirt/meeting7/gritzalis-electronic-voting.pdf

Houtven, L. V. (2017). *Crypto 101.* Obtenido de https://github.com/crypto101/crypto101.github.io/raw/master/Crypto101.pdf

Nakamoto, S. (s.f.). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Obtenido de https://bitcoin.org/bitcoin.pdf

Rodríguez-Henríquez, F., & Ortiz-Arroyo, D. (2007). Yet Another Improvement over the Mu-Varadharajan e-voting Protocol. *Computer Standards & Interfaces*.

Sommerville, I. (2011). *Ingeniería de Software.* Naucalpan de Juárez: Pearson Educación de México, S.A.

The CryptoParty handbook. (2013). Obtenido de http://cryptoparty.is/files/cryptoparty-handbook-2013-08-21/cryptoparty-handbook-2013-08-21.pdf

10. TABLA DE CONTENIDO PRELIMINAR

1. **¿Qué características hacían el EyT apto para las elecciones 2012?**

   Las unidades de Escaneo y Transmisión (EyT), formaron parte de la solución tecnológica, para la transmisión de resultados desde los recintos electorales, mediante el escaneo de las relaciones de votación y posterior transmisión mediante comunicación móvil 3g. Luego de escaneadas, estas se incorporan al sistema de cómputo electoral para su digitación y procesamiento. Como resultado se obtienen boletines municipales que son transmitidos a la sede central para ser consolidados y posteriormente incorporados en los boletines nacionales que emite la Junta Central Electoral.

2. **¿Cuáles beneficios brindaban las unidades EyT?**

   Las unidades de Escaneo y Transmisión (EyT), además de ser un equipo robusto, ligero y portable, permitían disminuir considerablemente los tiempos necesarios para el procesamiento y divulgación de resultados, además de garantizar un soporte confiable de los resultados electorales. En el pasado se tenía que esperar que se terminara el escrutinio en el colegio electoral, para luego iniciar el traslado de la valija hacia la Junta Electoral para procesar la relación de votación, con lo que se tenía que esperar por las largas filas para la entrega de valijas. Con el uso de las EyT en los recintos, los tiempos se agilizan, en vista que las informaciones son recibidas en pocos minutos en las Juntas Electorales, después de concluido el proceso de escrutinio en los colegios electorales, por el escaneo, procesamiento y transmisión de la actas de votación y por ende se eliminan las largas filas en las Juntas Electorales por la entrega de valijas y procesamiento de las actas.

   Beneficios:

   - Escaneo y digitalización de las actas desde los recintos.
   - Validación del acta escaneada.
   - Encriptación de imágenes para la transmisión.
   - Consolidación centralizada
   - Utilización de llaves de Seguridad.
   - Backup de las imágenes en dispositivos de Memorias USB.
   - Utilización de llaves de Seguridad.
   - Verificación y Confirmación electrónica del envío total de las Actas de todos los colegios del recinto (cierre del recinto).
   - Entrega de constancia impresa de la trasmisión del acta.
   - Entrega inmediata de las imágenes de actas a los centros de cómputos de los partidos y medios de comunicación.

3. **¿Cuáles eran los posibles inconvenientes de las unidades EyT?**

   Los posibles inconvenientes están relacionados con la imposibilidad de realizar las operaciones de escaneo o transmisión de las relaciones de votación:

- No funcionamiento por falla energética, solamente tenían capacidad para 4 horas de autonomía.
- Si el escáner presentaba fallas, no sería posible procesar y transmitir las relaciones de votación.
- Si no había disponibilidad de señal móvil no se podía realizar la transmisión.
- Los componentes físicos de la tarjeta madre son fijos y no permiten actualizaciones futuras(CPU, RAM, Network)

4. ¿Cómo funcionan las unidades EyT?

Las unidades EyT, están configuradas con una placa madre con todo integrado, pantalla táctil, puertos de comunicación de red, escáner, modem 3g y baterías de respaldo, entre otros. Las unidades se instalan en los recintos electorales esperando que se cierre el proceso de votación a las 6:00PM.. Al concluir el escrutinio manual de los votos, se procede a llenar el acta de votación con los resultados de la mesa, luego firmada, sellada y plastificada el acta, se procede con el escaneo, verificación, autentificación, proceso y transmisión. El acta digitalizada pasa por los procesos automáticos de OCR (reconocimiento óptico de caracteres), ICR (reconocimiento inteligente de caracteres) y OMR (Reconocimiento óptico de marcas), para luego realizar una atomización de los datos referentes a los votos, para realizar una digitación ciega de los mismos para reconfirmar los valores reconocidos por los procesos automáticos. En caso de existir alguna diferencia, los datos son reasignados a otro digitador para su digitación.

5. ¿Por qué decidieron migrar de los EyT a los escáneres de Indra?

En los procesos electorales, hay factores que impactan los tiempos para la divulgación de resultados, por causa del escrutinio manual de los votos, en vist a del nivel de complejidad del conteo y llenado de las relaciones de votación con los resultados, donde se pueden producir descuadres por errores de suma o de llenado. En vista de buscar alternativas mediante el uso nuevas tecnologías que eviten las referidas situaciones y además garanticen la intensión del votante, la autogeneración de las actas y transmisión de resultados, sin ser votación electrónica. Se optó por una solución de escrutinio automatizado, la cual conserva la votación tradicional con boletas y luego realiza el conteo mediante el reconocimiento inteligente de marcas en la boleta.

6. ¿Cuáles son las características de las unidades INDRA?

La solución de Indra se compone de tres unidades:

1. Tableta para registrar la concurrencia de electores. Este equipo posee un sistema operativo Android, con pantalla de 7 pulgadas, autonomía energética de 12 horas y lector de huellas integrado para la validación biométrica de los electores.
2. Escáner para el escrutinio automatizado de las boletas. Este equipo está dotado de una autonomía energética de 4 horas, con escáner integrado con autoalimentador de páginas, lo cual le permite procesar lotes de boletas.
3. Impresora láser para la impresión del acta de votación con los resultados de la mesa.

7. ¿Cuáles beneficios brindaban las unidades INDRA?

- Permite registrar la concurrencia de los electores en la mesa.
- Validación de los electores vía las huellas dactilares.
- Verificación de los datos del ciudadano de forma digital, incluyendo la
- foto.
- Consulta de los electores que no pertenezcan al colegio electoral, del
- lugar donde le corresponde votar en el municipio
- Escaneo y digitalización de las boletas de votación.
- Escrutinio automatizado mediante el reconocimiento y asignación de votos de las boletas electorales.
- Validación de la integridad física de las Boletas Electorales (voto, firma, sello).
- Impresión/digitalización de la relación de votación.
- Escaneo y transmisión de las relaciones de votación luego de ser firmadas.
- Transmisión de resultados.

8. ¿Cuáles eran los posibles inconvenientes de las unidades de Indra?

- No funcionamiento por falla energética, aunque tenían capacidad para funcionar 12 horas el capta huellas respectivamente, si el capta huellas se descargaba totalmente no era posible encenderlo hasta sobrepasar el 30% de carga.
- El no funcionamiento del capta huellas, afecta el registro electrónico de concurrentes y la validación mediante huellas del elector.
- La cámara para lectura de la cédula no está bien sujeta a la base y imposibilita la lectura de la cédula.
- En el caso del escáner aunque tiene capacidad de 4 horas de autonomía, debido a la manipulación en el traslado o instalación, se podía desconectar la conexión entre la base donde reside la batería y el escáner, lo que afectaba el suministro

de corriente e impide la operación de la unidad hasta la intervención de un personal técnico.

- Si el escáner presentaba fallas para escanear, no sería posible realizar el escrutinio automatizado.
- Si no había disponibilidad de señal móvil, no se podía realizar la transmisión.
- Imposibilidad de Operación por problemas en el sistema operativo de las unidades.
- Problemas de comunicación en los puertos USB.

9. ¿Cómo funcionan las unidades de Indra?

Las unidades para el registro de concurrentes y escrutinio automatizado se instalan en los colegios electorales antes de la apertura de los mismos el día de las elecciones. El capta huellas, permitía realizar la validación electrónica mediante la confirmación visual de la foto y las huellas dactilares de los electores de la mesa.

La unidad de escrutinio automatizado, al finalizar el proceso de votación, el presidente del colegio procedía a clasificar las boletas por nivel para luego hacer lotes de digitalización y procesar las mismas. En el proceso de escrutinio automatizado se identificaba la integridad de la boleta mediante la identificación del voto, firma y sello en las mismas. Al ser clasificada como válida, se reconocía el marcado y asignación de voto. En caso de que no se pudiera determinar automáticamente la intención del voto, el presidente y el secretario de la mesa manualmente deberían determinar cual fue la intención del votante y proceder con la asignación o anulación del mismo. Terminado este proceso se procedía con la generación del acta de resultados, firma del acta, escaneo y transmisión de resultados.

10. Mencionar los datos técnicos de las unidades EyT e Indra, tales como:

EyT

Especificaciones Técnicas JCE-3000 (EyT)	
Modelo	CIE-3000A
Mother Board (M/B)	POS - Poll Book CN700 M/B
Procesador	VIA
Chipset	CN700
Procesador - Velocidad	800mhz
Memoria RAM	1 GB
Disco Duro	120GB SATA 2.5
Tarjeta de Video	Integrada VGA
Chasis (Case)	Todo Inetgrado, Formato Compacto
Sistema Operativo	Windows XP SP2 Emmbeded
Power Supply	135 W 19v 7.1A
Batería Integrada	Battery Backup Integrado 7200mah 11.1v
Puertos USB	6 (4 Internos, 2 Externos)
Monitor	12.1 Touch Screen Resistive Type
Red	Ethernet 10/100 y WI-FI b+g
Memoria de Backup	Compact Flash Card 4GB
Periféricos Integrados	
Impresora	SII Thermal Printer P2K-112
Fax Modem	Billionton Systems Inc. MDCAzs 33.6kbps
Escáner	Plustek OpticSlim M12 Plus USB Portable Scanner
Lector de Huellas	Wison OS106mdl USB
Lector de Código de Barras	Intermec EA-15
Lector de Banda Magnética	Fametech TYSSO BMR-830
Lector de Tarjetas Inteligentes	EZM11xpu-0616 Castle Technology USB
Maleta para Portección y Transporte	
Maleta Reforzada	Pelican 1600 Series Orange Case

Indra		
Capta Huellas	**Escáner Escrutinio Automatizado**	**Impresora**
• Pantalla táctil 7'' 1200 x 800 • Sistema Operativo Android 4.4 • Procesador ARM QuadCore a 1.8ghz • Lector de huellas FIB • Batería Interna de 12 horas de autonomía • Memoria Interna 16gb • Memoria externa MicroSD • Modem USB Externo	• Pantalla LCD táctil 8'' 1200 x 800 • Sistema Operativo Windows 8.1 embebido • Procesador Atom Quadcore 2.0 ghz • Velocidad escaneo de 20 páginas por minuto • Dúplex 200 o 300 dpi	• Tipo de Impresión Laser • Resolución 600 x 600 dpi • Tamaño de impresión (8.5'' x 11'') • Velocidad de Impresión 19 ppm

• Puertos USB 2.0 • Lector de códigos QR y códigos de barras de las cédulas. • Peso aproximado 2.5 lbs.	• Memoria Interna 32gb • Puerto USB 2.0 • Modem 3G USB • Batería Interna con 4 horas de autonomía	

11. Facilitar las fotografías de los equipos EyT e Indra

EyT

2.- Unidades de Conteo de Votos Automatizado (CVA)

1.- Dispositivo para el Registro de Concurrentes (DRC)

12. Facilitar los manuales de uso o funcionamiento

No es posible entregar este requerimiento, en vista que los mismos contienen elementos de seguridad del proceso electoral que son de carácter privados y exclusivos de la JCE.

Sistema de votación eléctronico basado en la tecnología Blockchain

34	02:32	Active	Ideas
Responses	Average time to complete	Status	

1. ¿ Has votado alguna vez ?

Si	26
No	8

2. ¿ En ocasiones no has ido a ejercer tu derecho a votar?

Afirmativo, siempre he ido	19
Negativo, no he ido en ocasio...	15

3. De ser negativa la respuesta anterior, ¿ Cuales fueron las razones de no votar ?

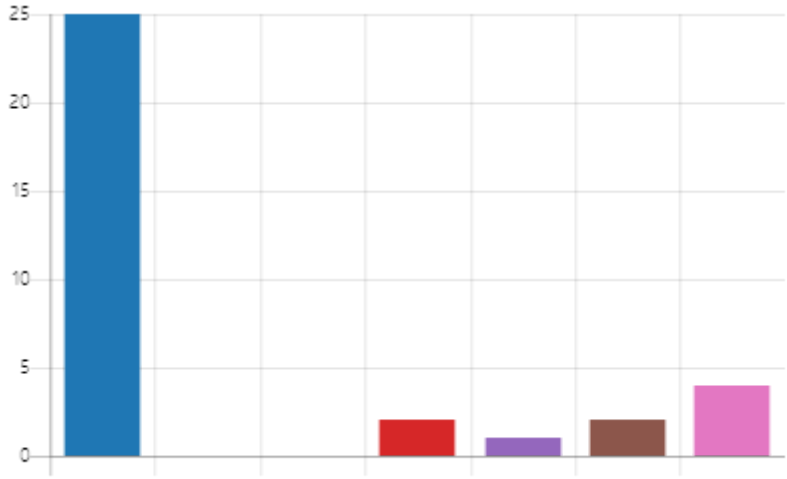
Me gustaría que fuese un siste...	4
No confio en el sistema votaci...	11
No existe mucha opciones de ...	5
Se arman conflictos	3
Other	4

4. ¿ Crees que existen muchas personas que no se preocupan en votar ?

Si	30
No se	1
Tal vez	3
No	0

5. ¿ Qué público de personas consideras sin precupación por votar ?

18-29	25
30-39	0
40-49	0
50-59	2
60-69	1
Más de 70	2
No se	4



6. ¿ Crees que con un nuevo sistema de votación digital totalmente seguro podría incentivar a que voten ?

Si	17
Tal vez	12
No se	4
No	1

7. ¿ Te agradería contar con otro sistema para votar ?

Si	28
Tal vez	6
No	0

8. ¿ Que tan factible consideras que es el sistema de votación actual ?

34	4.71
Responses	Average Number

9. ¿ En algún momento te gustaría contar con un sistema de votación digital totalmente seguro ?

Si	32
Tal vez	2
No	0

10. ¿ Has escuchado de blockchain ?

Si	21
No	13

11. ¿ Considera factible esta tecnología incorruptible integrada a un sistema de votación digital en la República Dominicana ?

Si	23
Tal vez	6
No se	5
No	0