ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

DISEÑO DE LA INFRAESTRUCTURA TECNOLÓGICA PARA EL VOTO DIGITAL EN ECUADOR

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

SANTACRUZ GUARQUILA ANDREA ALEXANDRA

andrea.santacruzg@gmail.com

VALENZUELA CANTOS FERNANDO MOISÉS

fermovalcan@gmail.com

DIRECTOR: PhD. MAFLA GALLEGOS LUIS ENRIQUE

enrique.mafla@epn.edu.ec

Quito, Octubre 2014

DECLARACIÓN

Nosotros, Andrea Alexandra Santacruz Guarquila y Fernando Moisés Valenzuela Cantos, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Santacruz Guarquila Andrea Alexandra	**Valenzuela Cantos Fernando Moisés**

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Andrea Alexandra Santacruz Guarquila y Fernando Moisés Valenzuela Cantos, bajo mi supervisión.

PhD. Luis Enrique Mafla Gallegos

DIRECTOR DE PROYECTO

AGRADECIMIENTOS

A Dios por cada oportunidad que nos presenta a través de un nuevo día de vida, para convertir nuestros sueños en metas cumplidas.

A nuestras familias por su apoyo incondicional y fuerza brindada a lo largo de todos estos años.

Al Señor PhD. Enrique Mafla, por su paciencia y honrosa colaboración para el desarrollo y terminación del presente Proyecto de Titulación.

A nuestros profesores de la Facultad de Ingeniería de Sistemas, quienes a lo largo de estos años han contribuido en nuestra formación profesional y humana a través de sus conocimientos y ejemplo.

A la Escuela Politécnica Nacional por la oportunidad brindada de educarnos en la universidad más prestigiosa del país.

Andrea Santacruz

AGRADECIMIENTOS

A todas las personas que han brindado su aporte en este largo camino.

Fernando Valenzuela

DEDICATORIA

A Dios, por haber guiado mi camino con rectitud e infinito amor. Presentarme nuevas oportunidades y lecciones de vida para aprender.

A mi madre, por ser mi fuente de motivación para superar los obstáculos presentados y ser una persona de bien.

A mi padre, por su apoyo y consejo constante respecto a las decisiones que he tomado en mi vida.

A mi tío Patricio, por su ejemplo y ayuda en los momentos difíciles de mi vida.

A mis hermanos por su compañía, apoyo y alegrías brindadas siempre.

A mis amigos, por compartir tantas experiencias enriquecedoras a lo largo de todo este tiempo.

A mi director de tesis, por su guía y paciencia durante la realización del presente Proyecto de Titulación

A mis maestros, por sus conocimientos y experiencia transmitida durante toda mi carrera.

Andrea Santacruz

DEDICATORIA

A mis padres, familia y amigos.

Fernando Valenzuela

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

PRESENTACIÓN

Este proyecto de titulación propone un diseño de infraestructura tecnológica para votación digital abordado desde tres perspectivas: diseño del software, de red y de seguridad, con el fin aportar con una guía para la implementación de un sistema de votación digital en nuestro país.

Este documento se encuentra dividido en 4 capítulos y una sección de anexos:

En el capítulo 1 “INTRODUCCIÓN”, se define la problemática del voto digital, se identifican las fuentes de información para recolección y posterior análisis de requerimientos. Este capítulo incluye una descripción de procesos llevados a cabo el día de las elecciones y los problemas que se suscitan. Finalmente se presentan las metodologías y herramientas utilizadas para el desarrollo de este proyecto.

En el capítulo 2 “ANÁLISIS”, se realiza un análisis de la situación actual del voto digital, para lo cual se ha investigado la experiencia de tres países pioneros en la implementación de sistemas de votación digital. A continuación se presenta el levantamiento de requerimientos funcionales y no funcionales, estos son recolectados a través de historias de usuario y casos de uso del proceso electoral. Para terminar este capítulo, se elabora una valoración de los riesgos generales de los sistemas de votación digital, empleando la Guía de Gestión de Riesgos para Sistema de Tecnologías de Información propuesta por NIST SP 800-30. [1]

En el capítulo 3 “DISEÑO”, se presenta el diseño de red, de software y de seguridad basados en los requerimientos y controles propuestos en el capítulo 2. El diseño de la red se realiza empleando el enfoque modular del modelo de seguridad para redes de empresas SAFE de Cisco. El diseño del software se realiza empleando SCRUM como metodología de desarrollo y añadiendo artefactos considerados necesarios para el desarrollo del prototipo de software.

En el capítulo 4 “CONCLUSIONES Y RECOMENDACIONES”, contiene las conclusiones y recomendaciones obtenidas durante el desarrollo del presente proyecto.

En la sección de Anexos, se dispone de información complementaria para el desarrollo de este trabajo.

[1] National Institute of Standards y Technology.

RESUMEN

Nuestro país ha planteado un proyecto de modernización del proceso electoral. Este proyecto consiste en el uso de un sistema de votación digital, el cual automatice los distintos procesos que se llevan a cabo el día de las elecciones. Sin embargo, el sistema de votación digital posee características especiales como: garantizar el anonimato del voto y al mismo tiempo asegure que el ciudadano ha emitido un solo voto.

Por esta razón, el presente proyecto de titulación propone un diseño de la Infraestructura de Votación Digital para Ecuador, basado en el análisis en los requerimientos del proceso electoral ecuatoriano y en el análisis de riesgos que presentan este tipo de sistemas.

El enfoque inicial del proyecto permite contemplar leyes y reglamentos que norman el proceso electoral actual. Esta normativa constituye la base de requerimientos de la infraestructura propuesta. El análisis de riesgos está basado en los requerimientos d la infraestructura tecnológica para votación digital y en las experiencias de países que ya han implementado procesos electorales automatizados.

CAPITULO I

1 INTRODUCCIÓN

En este capítulo se abordará la problemática del voto digital en Ecuador, el estado de la legislación respecto a votación digital y un análisis del proceso manual de sufragio. En el subcapítulo 1.1, se define la problemática de la automatización del voto en nuestro país. En el subcapítulo 1.2, se presenta el análisis de la normativa del voto digital en Ecuador. Este análisis consiste en especificar las características y el rol de la Función Electoral. Posterior, se presenta los artículos en la Constitución de la República y en el Código de la Democracia que deben guiar el proceso de automatización del voto. En el subcapítulo 1.3 se realiza un análisis de las fases del proceso de votación y sus problemas. Finalmente en el subcapítulo 1.4 se presenta la selección de metodologías y herramientas que se usarán para la elaboración de este proyecto de titulación.

1.1 DEFINICIÓN DEL PROBLEMA

El proceso de sufragio en Ecuador se divide en votación y escrutinio. El proceso de votación se compone de procedimientos manuales, mientras que el proceso de escrutinio está parcialmente automatizado. Los procedimientos manuales generan problemas por errores operativos. Estos errores se deben principalmente por la manipulación incorrecta de los implementos entregados en el paquete electoral. El tiempo que toma llevar a cabo los procesos (10 horas para recepción de votos y tiempo adicional para el escrutinio), en las personas provoca cansancio y falta de concentración. Esto también causa que no se sigan las indicaciones para la recepción y conteo de votos tal como se describe en la Ley Electoral y en las capacitaciones realizadas por el CNE.

El proceso realizado actualmente no brinda las garantías necesarias para verificar que cada voto haya sido efectivamente contabilizado. Además, el tiempo que transcurre entre el cierre de las Juntas Receptoras del Voto y la publicación oficial de los resultados genera incertidumbre y desconfianza en la ciudadanía.

Por estos motivos, la automatización el proceso de recepción de votos y escrutinio se plantea como una solución a esta problemática. La automatización permite obtener resultados más rápidos y precisos que en un proceso manual; y disminuye la exposición de la información al manejo de personas.

La solución propuesta a este problema es desarrollar una infraestructura tecnológica compuesta por: servidores que serán los encargados de procesamiento de los datos y de alojar a los sistemas para recepción y escrutinio de votos; equipos terminales los cuales captarán los votos de los ciudadanos; y una infraestructura de red que garantice la seguridad de la información.

1.2 ANÁLISIS DE LA NORMATIVA DEL VOTO DIGITAL EN EL ECUADOR

Este subcapítulo específica las competencias de la Función Electoral y los artículos de la ley Electoral y la Constitución de la República que deben guiar la automatización del proceso de sufragio.

1.2.1 FUNCIÓN ELECTORAL

La Constitución otorga a la Función Electoral el papel de garantizar el cumplimiento de los derechos políticos de los ciudadanos, los cuales son expresados a través del sufragio. Esta función está conformada por el Consejo Nacional Electoral y por el Tribunal Contencioso Electoral. Ambos poseen autonomía administrativa, financiera y organizativa; además cuentan con jurisdicción nacional, de acuerdo al artículo 217 de la Constitución de la República.

1.2.1.1 Órganos de la Función Electoral

1.2.1.1.1 Consejo Nacional Electoral

"Se integra con cinco Consejeras o Consejeros principales con sus respectivos suplentes, los mismos que ejercen sus funciones por seis años y se renovarán parcialmente cada tres años." [1]

Las funciones de este organismo son: "Organizar, dirigir, vigilar y garantizar de manera transparente y eficaz los procesos electorales, convocar a elecciones, realizar los cómputos electorales, proclamar los resultados y posesionar a quienes resulten electas o electos, entre otras funciones." [1]

El representante legal del Consejo Nacional Electoral es su Presidente.

1.2.1.1.2 Tribunal Contencioso Electoral

"El Pleno es el órgano colegiado compuesto por juezas y jueces electorales." [1]

En el artículo 220 de la Constitución indica que este Órgano "se conformará por cinco miembros principales, que ejercerán sus funciones por seis años. El Tribunal Contencioso Electoral se renovará parcialmente cada tres años, dos miembros en la primera ocasión, tres en la segunda, y así sucesivamente. Existirán cinco miembros suplentes que se renovarán de igual forma que los principales." [2]

Las funciones de este órgano son: "(…) administrar justicia en materia electoral y dirimir conflictos internos de las organizaciones políticas, entre otras funciones." [1]

1.2.1.1.3 Juntas Receptoras del Voto (JRV)

Este organismo electoral es de carácter temporal, se integra por 7 miembros. 1er Vocal Principal, 2do Vocal Principal, 3er Vocal Principal, Secretario, Primer Vocal Suplente, Segundo Vocal Suplente y Tercer Vocal Suplente. El primer Vocal principal desempeña la función de Presidenta o Presidente de la JRV[2]; el organismo se completa con una Secretaria o Secretario y tres Vocales Suplentes.

[2] Junta Receptora del Voto

Las funciones de las Juntas Receptoras del Voto son: instalar las mesas de votación, captar los votos de ciudadanos habilitados para sufragar, realizar el escrutinio y enviar la documentación de los resultados a las autoridades pertinentes.

1.2.2 EL VOTO EN LA CONSTITUCIÓN DE LA REPÚBLICA

De acuerdo a la jerarquía de las normas jurídicas, es necesario analizar como primer punto la Constitución. En el artículo 1 se señala que "La soberanía radica en el pueblo, cuya voluntad es el fundamento de la autoridad, esta se ejerce a través de los órganos del poder público y de las formas de participación directa previstas en la Constitución.".

La forma de participación directa que involucra a todos los ciudadanos ecuatorianos es la ejercida a través del voto. En el artículo 62 se indica: "Las personas en goce de derechos políticos tienen derecho al voto universal, igual, directo, secreto y escrutado públicamente" (…)

Por lo tanto la constitución concede a los ciudadanos ecuatorianos -de nacimiento o por naturalización[3]-, el derecho político de votar. Este artículo también especifica las cualidades del voto que el estado garantiza a los ciudadanos al momento de ejercerlo.

1.2.3 EL VOTO EN LA LEY ELECTORAL

Esta ley está compuesta por 5 títulos, estos son: De la Función Electoral, Participación y Observación, Financiamiento y Control del Gasto Electoral, De la Administración y Justicia Electoral, y Organizaciones Políticas.

[3] Concesión o adquisición por parte de un extranjero de los derechos de los naturales de un país. http://www.wordreference.com/definicion/naturalizaci%C3%B3n

El título “De la Función Electoral” contiene la información sobre los procesos electorales del día de votación y menciona los mecanismos empleados para el sufragio, votación y escrutinio.

El análisis de los procesos electorales se los realizará con base en los capítulos del título “De la Función Electoral”. El artículo 113 de esta normativa trata específicamente del tema de la votación electrónica. El artículo señala que el Consejo Nacional Electoral tiene la potestad de decidir, en función del avance tecnológico, que medios utilizará para manejar los procesos concernientes al sufragio y escrutinio. Esta ley también otorga al Consejo Nacional Electoral el poder cambiar su normativa interna para que esta se ajuste a los cambios del avance de nuevas tecnologías.

1.2.4 NORMATIVA PARA LA PARTICIPACIÓN POLÍTICA DE PERSONAS CON DISCAPACIDAD

1.2.4.1 Constitución del Ecuador

Art. 47.- “El Estado garantizará políticas de prevención de las discapacidades y, de manera conjunta con la sociedad y la familia, procurará la equiparación de oportunidades para las personas con discapacidad y su integración social.” [3]

“Se reconocen a las personas con discapacidad, los derechos a:

10. El acceso de manera adecuada a todos los bienes y servicios. Se eliminaran las barreras arquitectónicas.

11. El acceso a mecanismo, medios y formas alternativas de comunicación, entre ellos, el lenguaje de señas para personas sordas, el oralismo y el sistema braile.” [3]

Art. 48: “El estado adoptará a favor de las personas con discapacidad medidas que aseguren:

1. La inclusión social, mediante planes y programas estatales y privados coordinados, que fomenten su participación política, social, cultural, educativa y económica.
4. La participación política, que asegurará su representación, de acuerdo a la ley.” [4]

Art. 65: “(…) El estado adoptará medidas de acción afirmativa para garantizar la participación de los sectores discriminados.” [5]

1.2.4.2 Convención de los Derechos de las personas con Discapacidad

Art. 29. “Participación en la vida política y pública
Los Estados miembros garantizarán a las personas con discapacidad los derechos políticos y la posibilidad de gozar de ellos en igualdad de condiciones con los demás y se comprometerán a:

a) Asegurar que las personas con discapacidad puedan participar plena y efectivamente en la vida política y pública en igualdad de condiciones con las demás, directamente o a través de representantes libremente elegidos, incluidos el derecho y la posibilidad de las personas con discapacidad a votar y ser elegidas, entre otras formas mediante:
   i) La garantía de que los procedimientos, instalaciones y materiales electorales sean adecuados, accesibles y fáciles de entender y utilizar.
   ii) La protección del derecho de las personas con discapacidad a emitir su voto en secreto en elecciones y referéndum públicos sin intimidación, y a presentarse efectivamente como candidatas en las elecciones, ejercer cargos y desempeñar cualquier función pública a todos los niveles de gobierno, facilitando el uso de nuevas tecnologías y tecnologías de apoyo cuando proceda.
   iii) La garantía de la libre expresión de la voluntad de las personas con discapacidad como electores y a este fin, cuando sea necesario y a

petición de ellas, permitir que una persona de su elección les preste asistencia para votar.” [6]

1.2.4.3 Código de la Democracia

Art. 11.- El Ejercicio del derecho al voto se realizará de conformidad con las siguientes disposiciones:

1. El voto será obligatorio para las ecuatorianas y ecuatorianos mayores de dieciocho años, incluyendo a las personas privadas de la libertad sin sentencia ejecutoriada.
2. El voto será facultativo para las personas entre dieciséis y dieciocho años de edad, las mayores de sesenta y cinco años, las ecuatorianas y ecuatorianos que habitan en el exterior, los y las integrantes de las Fuerzas Armadas y la Policía Nacional en servicio activo, las personas con discapacidad y las personas analfabetas.

   (…) El Consejo Nacional Electoral reglamentará y establecerá las condiciones necesarias para facilitar el ejercicio del sufragio a las personas con discapacidad.

Art. 111.- El Consejo Nacional Electoral garantizará los mecanismos idóneas para las personas con discapacidad puedan ejercer su derecho al sufragio, incorporándolos en la normativa electoral que se dicte.

Art. 115. (…) El Consejo Nacional Electoral reglamentará la forma de votación que deba ser implementada para los casos de personas cuya discapacidad impida el ejercicio del sufragio (…).

1.2.4.4 Reglamento para la participación de personas con discapacidad

Art. 3.- “Las personas con discapacidad tienen derecho al voto asistido, el cual podrán ejercer con la asistencia de una persona acompañante.” [7]

Art. 4. “En cada reciento electoral habrá por lo menos una mesa electoral de atención de personas con discapacidad, mujeres embarazadas y adultos mayores ubicada en la planta baja, en donde solicitarán el apoyo que corresponda según sus condiciones, para ejercer su derecho al voto.” [7]

Art. 5. “El Consejo Nacional Electoral dispondrá para las personas con discapacidad visual, una plantilla de lectura en Braile por cada diez juntas receptora del voto y una cada recinto electoral en el exterior, la cual se colocará conjuntamente con la papeleta de votación, con la finalidad de que estas personas puedan ejercer su derecho al voto sin necesidad de ser asistidos, de ser el caso.” [7]

Art. 6. “El Consejo Nacional Electoral adoptará las siguientes medidas de acción afirmativa; cuando el caso lo amerite:

c) El Consejo Nacional Electoral incluirá la discapacidad como eje transversal en todas sus actividades de difusión, capacitación e información, así también incluirá lenguaje positivo y mecanismos de acceso a la comunicación e información para personas con discapacidad sensorial.
d) El Consejo Nacional Electoral exigirá a las organizaciones políticas que implementen en su campaña electoral mecanismos de accesibilidad tales como la interpretación del lenguajes de señas, subtítulos y utilizarán un lenguaje inclusivo.
e) El Consejo Nacional Electoral garantizará el acceso de información a través de mecanismos, medios y formas de alternativas de comunicación, como la lengua de señas, para personas sordas y; para personas con deficiencia visual, el sistema Braile.
f) En coordinación con las Fuerzas Armadas y Policía Nacional, la sociedad civil y los actores políticos, el Consejo Nacional Electoral creará un programa de

> Voto en Casa, el cual consiste en acercar la mesa electoral hasta el domicilio de las personas con discapacidad, mujeres embarazadas, adultos mayores y personas con enfermedades catastróficas, previamente identificadas por el Consejo Nacional Electoral; (…)" [7]

Art. 7. "El Consejo Nacional Electoral propenderá la selección de recintos electorales que cuenten con la accesibilidad al espacio físico para las personas con discapacidad; y dotará del material electoral adecuado." [7]

Mesa de Atención preferente

El número de mesas de atención preferente se determinará en función del número de juntas receptoras del voto del recinto electoral:

- En recintos con 10 a 30 juntas receptoras del voto -> 1 mesa con 2 miembros.
- En recintos con 31 juntas receptoras del voto -> 2 mesas con 2 miembros cada una.
- En recintos con menos de 10 juntas receptoras del voto, estas funciones se llevarán a cabo en la mesa de información.

Voto en casa

Criterio de selección para beneficiarios del proyecto voto en casa:

- Personas con más del 75 % de discapacidad.
- Personas con Hemiplegia o paraplegia.
- Personas mayores de 65 años.

1.3 ANÁLISIS DE LOS PROCESOS ELECTORALES DEL CNE[4]

El análisis de los procesos electorales se tomará como referencia el día de votación. Este día se divide en 4 fases, estas son:

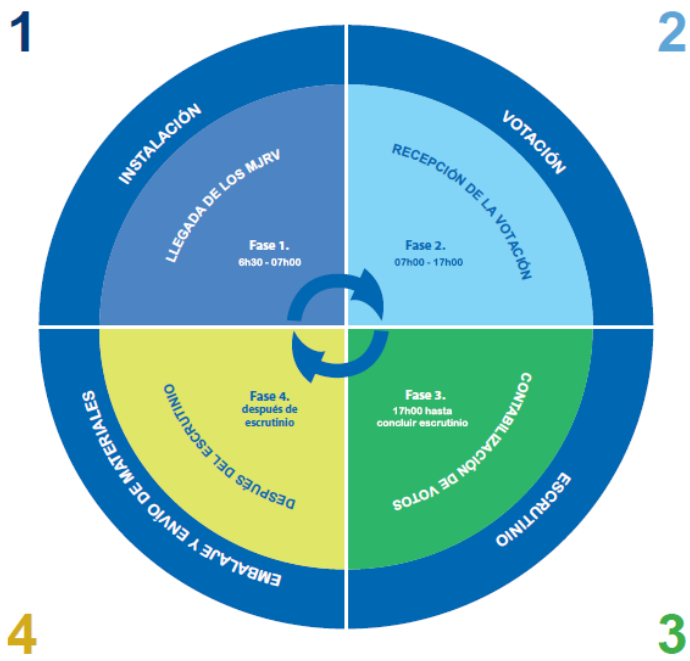


Figura 1-1. Guía de Procedimientos de la Juntas Receptoras del Voto Fuente: http://capacitacionelectoral.cne.gob.ec/mod/resource/view.php?id=59

1.3.1 INSTALACIÓN

El objetivo de esta fase es preparar el lugar e implementos para la recepción de votos. En esta fase se realiza las siguientes actividades:

1. La instalación inicia a las 6h30 cuando los miembros designados para integrar cada JRV se presentan ante el Coordinador del Recinto Electoral y reciben el paquete electoral.
2. La JRV debe verificar que el paquete electoral se encuentre íntegro y tenga todos los elementos que indica el checklist.

[4] Concejo Nacional Electoral

3. Al terminar la instalación de la JRV, el secretario debe llenar, hacer firmar el Acta de Instalación a las personas correspondidas.
4. Si una JRV no cuenta con mínimo 4 miembros, entonces no puede iniciar sus actividades. En este caso debe elegirse a cualquier otra persona para completar el número requerido de miembros.

Los problemas identificados en esta fase son:

1. Si un paquete electoral se encuentra incompleto, el secretario de la JRV indica como observación en el Acta de Instalación lo sucedido, mas no se toma una acción sobre este problema.
2. Si una JRV no cuenta con mínimo 4 miembros para iniciar su actividad, entonces se selecciona de los presentes, personas al azar para completar el mínimo de miembros requeridos. Las personas seleccionadas pueden desconocer el proceso de sufragio.

Para ampliar la información sobre las actividades de esta fase, en el Anexo B se encuentra un mapa de procesos de la fase de instalación.

1.3.2 VOTACIÓN

La fase de votación consiste en permitir sufragar a los ciudadanos empadronados[5]. En esta fase se realiza las siguientes actividades:

1. La votación inicia a las 07h00.
2. La JRV verifica la identidad del ciudadano que se presenta para sufragar. Si el ciudadano consta en el Padrón Electoral, entonces se le entrega las papeletas de votación.
3. El ciudadano realiza su voto y deposita en las urnas correspondientes.

[5] Persona inscrita en el padrón o registro electoral y se encuentra habilitada para sufragar. http://es.thefreedictionary.com/empadronado

4. La JRV registra en el Padrón Electoral la participación del ciudadano en el proceso de sufragio.
5. La fase termina a las 17h00.

Los documentos y materiales usados durante la recepción del voto son los siguientes:

- Padrón Electoral.
- Certificados de Votación.
- Certificados de Presentación.
- Papeletas de Votación (todas las dignidades).
- Material Genérico (esferográficos, almohadilla para huellas dactilares). [8]

Los problemas identificados en esta fase son:

1. El derecho de los ciudadanos a emitir un voto en secreto no se cumple en personas con discapacidad física como pérdida de visión o extremidades superiores. Los ciudadanos con estas discapacidades tienen que ser asistidas por una tercera persona.
2. Un miembro de la JRV puede entregar papeletas adicionales a un votante por error o deliberadamente.
3. Al terminar de emitir un voto, el ciudadano debe firmar en el Padrón Electoral para dejar constancia que ejerció su voto. Sin embargo, el votante puede firmar en un casillero incorrecto, esto provoca una inconsistencia en el registro de ciudadanos que ya votaron
4. El documento de identificación del votante puede ser falsificado.
5. La JRV puede permitir sufragar a una persona sin constar en el Padrón Electoral.
6. El votante puede sustraer papeletas de votación entregadas para sufragar.

Para ampliar la información sobre las actividades de esta fase, en el Anexo C se encuentra un mapa de procesos de la fase de votación.

1.3.3 ESCRUTINIO

Esta fase tiene como fin realizar el conteo de los votos depositados en las urnas y publicar los documentos de resultados oficiales de la votación. El proceso de escrutinio se lo realiza a nivel de: JRV, Juntas Intermedias, Junta Provincial Electoral y Nacional.

En esta fase se realiza las siguientes actividades:

1. El escrutinio inicia a las 17h00.
2. La JRV realiza el conteo voto a voto de válidos, nulos y blancos. Al final del conteo realiza las Actas de Escrutinio y envía los resultados a las Juntas Intermedias.
3. Las Juntas Intermedias computan los resultados de las Actas de Escrutinio de cada JRV. Si existen actas de escrutinio con inconsistencias numéricas, entonces las Juntas Intermedias declaran el acta rezagada. Las Juntas Intermedias remiten a las Juntas Provinciales Electorales los resultados del conteo de votos y las actas declaradas rezagadas.
4. Las Juntas Provinciales Electorales examinan cada acta rezagada y determinan una solución. Estas juntas computan los votos válidos por cada candidato. Los resultados del conteo son documentados y remitidos al CNE.
5. El CNE se encarga del escrutinio nacional. Este escrutinio consiste en examinar las actas levantadas por las juntas provinciales y determinar si existen inconsistencias numéricas. Corregir estos errores y proclamar sus resultados definitivos de la votación.

Los Delegados de las Organizaciones Políticas, observadores nacionales e internacionales pueden ver el proceso de escrutinio en todos los niveles, más no interferir ni calificar el voto.

Los problemas identificados en esta fase son:

1. La calificación del voto es subjetiva ya que depende del criterio de los miembros de la JRV.
2. Las actas de escrutinio pueden ser llenadas de forma incorrecta o poseer inconsistencias numéricas.

Para ampliar la información sobre las actividades de esta fase, en el Anexo D, E, F y G se encuentran respectivamente los mapas de procesos de la fase de escrutinio a nivel de JRV, Junta Intermedia, Junta Provincial Electoral y Escrutinio Nacional.

1.3.4 ENVÍO Y EMBALAJE

El objetivo de esta fase es documentar los resultados del proceso y enviar el material electoral guardado en sobre y fundas respectivas. Esta fase es realizada únicamente por la JRV.

El envío y embalaje del material electoral es realizado con la ayuda de un flujograma de los documentos electorales. El flujograma contiene el detalle donde se almacena cada documento y material electoral existente.

Los problemas identificados en esta fase son:

1. Los materiales y documentos usados durante el proceso de votación pueden ser guardados en sobres o fundas incorrectas.
2. El presidente y/o secretario pueden olvidar firmar los sobres que son entregados a los Coordinadores del Recinto Electoral.

Para ampliar la información sobre las actividades de esta fase, en el Anexo H se encuentra un mapa de procesos de la fase de envío y embalaje.

1.4 SELECCIÓN DE LA METODOLOGÍA Y HERRAMIENTAS

En este subcapítulo se realizará la selección de metodologías y herramientas para el desarrollo de este proyecto de titulación. Las metodologías y herramientas a elegir son: guía para la evaluación de riesgos, arquitectura de red segura, metodología ágil de desarrollo y servidor de aplicaciones.

La Guía para la evaluación de riesgos se usará para establecer los pasos a seguir en la identificación y evaluación de los riesgos de un sistema de votación digital, y determinar los controles que deben ser implementados para mitigar estos riesgos. La Arquitectura de red segura se empleará como modelo para diseñar una red de datos de acuerdo a buenas prácticas. La metodología ágil de desarrollo servirá de ayuda para determinar las etapas del proceso de desarrollo y artefactos para generar un prototipo del software de votación. El servidor de aplicaciones se usará para ejecutar el software de votación.

1.4.1 GUIA PARA LA EVALUACIÓN DE RIESGOS

Las guías para la evaluación de riesgos consideradas para la selección son: ISO 27005, NIST SP 800-30 y OCTAVE. La selección de la guía para la evaluación de riesgos se considerará los siguientes criterios:

- La participación de personal del CNE es necesaria.
- Costo de acceso a la documentación de la guía para evaluación de riesgos.
- Nivel de conocimiento de la guía para evaluación de riesgos.

La información de cada metodología ha sido recabada de las siguientes fuentes [9], [10] y [11].

GUÍA / CRITERIO	OCTAVE	NIST SP800-30	ISO 27005
¿La participación del personal del CNE es requerido para realizar la evaluación de riesgos?	Sí.	No.	No.
¿El acceso a la documentación de la guía para evaluación de riesgos tiene un costo?	No.	No.	Sí.
¿Se tiene experiencia o conocimiento utilizando esta guía de evaluación de riesgos?	No.	Sí.	No.

Tabla 1-1. Criterios para selección de Guía para Evaluación de Riesgos.

La guía para la evaluación de riesgos seleccionada es NIST SP 800-30 porque:

- Se tiene mayor conocimiento de la aplicación de esta guía.
- La documentación respecto a la guía es de libre acceso, no tiene un costo por su uso.
- La participación de personal del CNE no es requerida.

1.4.2 ARQUITECTURA DE RED SEGURA

Para el diseño de la red de datos de la infraestructura de votación se usará SAFE. Esta arquitectura de seguridad para redes es desarrollada por Cisco. Los enfoques de SAFE son defensa en profundidad y un diseño modular. Cada módulo representa un área funcional de la red. La arquitectura se centra en identificar las amenazas que afectan a los módulos de la red y en los medios para combatirlas. Este enfoque

disminuye la probabilidad de que el fallo de un módulo ponga en peligro todos los recursos de la red.

Esta arquitectura de red ha sido seleccionada porque recoge las mejores prácticas de diseño y configuración de redes seguras y la documentación es de libre acceso.

1.4.3 METODOLOGÍA DE DESARROLLO SCRUM

Para el desarrollo del prototipo del software de votación se utilizará una metodología ágil. Este tipo de metodologías brindan flexibilidad en el cambio de requerimientos y manejan una documentación menos formal en el desarrollo del proyecto. Su principal ventaja es la rápida reacción ante los cambios en los requerimientos durante la implementación.

Las metodologías ágiles más utilizadas actualmente son:

- Scrum.
- XP.

Los criterios para evaluar y seleccionar la metodología ágil a emplearse son:

- Versatilidad sobre los cambios de requerimientos.
- Simplicidad.
- Retroalimentación sobre iteraciones.
- Interacción entre equipo de trabajo.
- Conocimiento de la metodología.

Los criterios de evaluación tendrán valores entre 0 a 5. 5 puntos serán asignados si la metodología cumple muy satisfactoriamente la característica citada. La puntuación irá disminuyendo hasta 0 puntos si la metodología no cumple con la característica.

A continuación se presenta la tabla comparativa de las dos metodologías señaladas previamente.

CARACTERÍSTICA	SCRUM	XP
Versatilidad sobre los cambios de requerimientos.	5	5
Simplicidad.	4	5
Retroalimentación sobre iteraciones.	5	4
Interacción entre equipo de trabajo.	5	5
Conocimiento de la metodología.	4	3
Total	**23**	**22**
Promedio	**4.6**	**4.4**

Tabla 1-2. Comparación de las metodologías ágiles SCRUM y XP. Fuente: http://es.slideshare.net/ejordi/metodologas-de-desarrollo-giles-scrum-xp.

Con base en los resultados de la tabla anterior se ha decidido utilizar la metodología SCRUM.

1.4.4 SERVIDOR DE APLICACIONES

La ejecución del software de votación requiere de un servidor de aplicaciones. La selección del servidor de aplicaciones se determinará de acuerdo a los siguientes criterios:

- Tipo de Licencia.
- Compatibilidad con Frameworks Java debido a que el lenguaje de desarrollo será Java.
- Costo.

Los servidores de aplicaciones considerados para esta selección son: IBM WebSphere Application Server, Weblogic, y JBoss Application Server.

Servidor / Característica	IBM WAS[6]	Weblogic	JBoss
Tipo de Licencia	Propietaria.	Propietaria.	GNU de código abierto.
Compatibilidad con Frameworks Java	Media.	Media.	Alta.
Precio	IBM WebSphere Application Server for Developers Authorized User 1256,32 $ [12]	WebLogic Server Standard Edition for Developers 202,73 $ [13]	Gratuito.

Tabla 1-3. Comparación de los servidores de aplicaciones IBM WAS, WebLogic y JBoss. Fuente: Realizado por los autores.

[6] WebSphere Application Server

CAPÍTULO II

2 ANÁLISIS

Este capítulo tiene tres objetivos. EL primer es analizar la situación actual del voto digital en el mundo y en el Ecuador, además de conocer la tecnología que actualmente se está usando en sistemas de votación. El segundo objetivo es realizar el levantamiento de los requisitos de software, de red y de seguridad. El último objetivo es obtener los controles que deben ser incorporados al diseño de la infraestructura tecnológica a través de la realización de una valoración de riesgos de un sistema de votación digital.

El capítulo se dividirá en tres secciones. En la sección 2.1., se analizará la experiencia de tres países que han automatizado su proceso de votación y las primeras prueba piloto de automatización del proceso electoral en Ecuador. Los requerimientos de software, de red y de seguridad se examinarán en la sección 2.2., En la sección 2.3., se llevará a cabo la valoración de riesgos del sistema de votación digital, para lo cual se empleará la Guía de Gestión de Riesgos NIST SP 800-30.

2.1.1 ANÁLISIS DE LA SITUACIÓN ACTUAL

En este subcapítulo se presentarán datos sobre países que son referentes en el mundo en el uso de sistemas de votación digital, los problemas que han tenido y las soluciones planteadas. Al final de esta sección se analizará el estado del proyecto de automatización del proceso electoral en Ecuador.

2.1.1.1 EXPERIENCIA DE OTROS PAÍSES CON SISTEMAS DE VOTACIÓN DIGITAL

Varios países a nivel mundial han intentado llevar a cabo el proceso de votación empleando sistemas electrónicos, con los siguientes fines técnicos y sociopolíticos:

- Incrementar la eficiencia en la recepción de votos.

- Mejorar la precisión en el escrutinio.
- Reducir los tiempos para conocer los resultados de la votación.
- Mejorar la auditoría del proceso de votación.
- Facilitar el ejercicio de voto para la población analfabeta.
- Demostrar las capacidades de la nueva tecnología.
- Aumentar la confianza en los procesos electorales.
- Proveer mejor información a partidos políticos y a ciudadanos.
- Ampliar las facilidades para la emisión del sufragio. [14]

Para este análisis se tomará como referencia 3 países: Bélgica, ya que fue el pionero en voto electrónico en Europa, y en este país el voto es obligatorio; el siguiente es Estados Unidos, ya que su sistema electoral es complejo y existen diversos de métodos de votación, se han presentado varios problemas en el uso de tecnologías para automatizar el proceso, sin embargo este país no ha abandonado su utilización; y finalmente se revisará el sistema Venezolano, ya que llevan por años utilizando el voto electrónico basado en DRE[7] y es un caso exitoso en Latinoamérica.

2.1.1.1.1 Bélgica

Características del sistema electoral

- Sufragio Obligatorio.
- El electorado habla 3 idiomas.
- Sistema electoral emplea la forma de listas abiertas.[8]

[7] Sistemas de voto electrónico de registro directo.
[8] El elector tiene tantos votos como candidatos, y puede seleccionar sus candidatos dentro de una lista o entre listas. Los partidos o movimientos solo pre-estructuran las listas.

Problemas y Soluciones

Bélgica antes de iniciar la automatización del voto digital realizó un estudio de factibilidad de implementar un nuevo sistema de votación que incorpore los nuevos recursos tecnológicos. También este país realizó reformas legales para impulsar la aplicación del sistema de votación automatizado.

Los problemas y soluciones que se dieron durante la automatización del sistema son [12]:

PROBLEMAS	SOLUCIONES
El coste de implementación del primer sistema de votación digital fue muy elevado.	Se plantea extender el uso del sistema de votación a todo el territorio de manera progresiva.
Con el primer sistema de votación se registran votos de personas extranjeras de la Unión Europea. Estas personas sufragaron a pesar de no que no debían estar facultadas para hacerlo.	Se resuelve iniciar una licitación para la adquisición de un nuevo sistema de votación. El desarrollo del nuevo sistema de votación incluyó pruebas piloto en condiciones reales y certificaciones por parte de firmas independientes como Pricewaterhouse Coopers.

Tabla 2-1. Problemas y soluciones del proceso de automatización belga

Tecnología del sistema de votación

El actual sistema de votación belga fue diseñado por la compañía privada Smartmatic. Este sistema está compuesto por una máquina electrónica de votación con pantalla táctil e imprime en papel un documento de comprobación o prueba del sufragio para auditorias posteriores de los resultados automatizados. [15]

2.1.1.1.2 Estados Unidos

Características del sistema electoral

- Cada Estado decide el sistema de votación a usar.
- La Comisión Electoral Federal se encarga de establecer los estándares que tienen que cumplir los sistemas de votación.
- La ley electoral esta especificada en la ley federal y estatal. Sin embargo, la ley estatal reglamenta en su mayoría los aspectos de la ley electoral.
- El método de elección es sufragio indirecto.[9]

Problemas y Soluciones

Estados Unidos tiene amplia experiencia en la automatización de sistemas de votación. Sin embargo, este país ha vivido grandes problemas a causa de usar métodos de sufragio distintos al manual.

PROBLEMAS	SOLUCIONES
El Estado de Florida experimentó problemas en los años 2000 y 2002 por el uso de un sistema poco confiable –sistema de tarjetas perforadas- y por inconvenientes con la usabilidad del sistema, respectivamente.	El Congreso estadounidense aprueba las leyes HAVA[10] y VIVA[11] para corregir y optimizar los sistemas electorales en todo el territorio. La ley VIVA exigió que todos los sistemas de votación imprima en papel un comprobante del voto.
Varios Estados presentaron problemas con sus sistemas de votación digital que no cumplían con las disposiciones de la ley	Organizaciones no gubernamentales ni políticas de Estados Unidades han formado equipos de expertos para

[9] Consiste en que los votantes eligen a representantes para formar un cuerpo electoral, llamado Colegio electoral. El Colegio Electoral elige al cargo público correspondiente.
[10] Help America Vote Act
[11] Voting Integrity and Verification Act

VIVA. Estos sistemas perdieron miles de votos y no poseían un sistema de backups ni imprimían un comprobante del voto.	examinar los sistemas de votación. El resultado de estas investigaciones ha servido al gobierno para prohibir el uso de ciertos sistemas que no cumplen con las leyes.

Tabla 2-2. Problemas y soluciones del proceso de automatización estadounidense

Tecnología del sistema de votación

Actualmente este país está adoptando la tecnología desarrollada por la empresa Smartmatic. Este sistema es el usado por Bélgica. El 6 de marzo del 2014 en el Condado de Rice se llevó a cabo una prueba pública del equipo de votación electrónica. Esta prueba fue abierta a los delegados de las organizaciones políticas, candidatos, prensa y público general, para que puedan comprobar su seguridad y exactitud. [16]

2.1.1.1.3 Venezuela

Características del sistema electoral

- El sistema electoral es mixto porque combina elementos del sistema de Representación por Mayoría con elementos del sistema de Representación Proporcional. [17] La Representación por Mayoría aplica a la elección de presidente de la República, gobernadores de los Estados y alcaldes de los Municipios. La Representación Proporcional de las Minorías aplica para elección de senadores, diputados al Congreso de la República, diputados a las Asambleas Legislativas de los estados federados, concejales de los municipios y miembros de las juntas parroquiales.
- La ley venezolana determina específicamente la completa automatización de los procesos de votación, escrutinio, totalización y adjudicación.

Problemas y Soluciones

Los problemas presentados en el proceso electoral venezolano son:

PROBLEMAS	SOLUCIONES
Denuncias de fraude en el conteo de votos manual.	El conteo de votos se realiza con máquinas que poseen un lector óptico.
Las autoridades venezolanas determinan que las máquinas con lectores ópticos no cumplen sus estándares de seguridad, eficiencia, agilidad, simplicidad.	El Comité Nacional Electoral implementa el Sistema de Registro Directo del Voto. Las máquinas y el código fuente se sometieron a procesos de auditoría que aportan confianza al proceso.
En las elecciones de 2013 se presentaron anomalías en el proceso de votación. Actores políticos venezolanos argumentan que no se garantiza la transparencia necesaria para los electores.	Venezuela prescribió como mandato legal la realización de auditorías al sistema de votación. El proceso de auditoria inicia desde la convocatoria a elecciones y finaliza luego de la entrega de los resultados automáticos. Este país también desarrollo una normativa para tipificar y sancionar las potenciales infracciones que se pueden dar durante la programación del sistema de votación, la transmisión de datos y el escrutinio. Estas leyes también reglamentan los elementos principales para establecer la validez o no de la votación electrónica.

Tabla 2-3. Problemas y soluciones del proceso de automatización venezolano

Tecnología del sistema de votación

El sistema de votación venezolano consta de cuatro pasos:

1. Autentificación: el votante debe grabar su huella dactilar en el documento de registro a través de una máquina llama captahuella.
2. Votación: el ciudadano ejerce el voto haciendo uso de la máquina de votación electrónica con pantalla táctil. Su voto se almacenada en la máquina y se imprime un comprobante de papel. El votante debe depositar el comprobante en una urna tradicional.
3. Escrutinio y transmisión: los votos generados por los votantes permanecen almacenados aleatoriamente en la memoria de la máquina. Al cierre del proceso, las actas de escrutinio se imprimen y los datos encriptados se remiten al Centro Nacional de Totalización a través de la red de datos de la empresa de telecomunicaciones estatal. El sistema de totalización únicamente recibe datos de las máquinas de votación autenticadas y autorizadas por la autoridad electoral.
4. Auditoría de cierre: los miembros de mesa cotejan los comprobantes de votación colocados en la urna tradicional frente a los resultados calculados por la máquina.

2.1.1.1.4 Conclusiones

De la experiencia de los tres países se puede concluir lo siguiente:

- Previo al inicio de la automatización del proceso se debe realizar un estudio de factibilidad del proyecto para plantear estrategias de implementación o cambios si se requiere en el proceso electoral.

- El respaldo de una normativa legal clara es importante para determinar el alcance y limitaciones de un sistema de votación digital. Y también porque los delitos e infracciones deben ser especificados, sancionados y considerados desde el inicio de la construcción del sistema de votación hasta la entrega de resultados.
- La automatización del proceso de sufragio crea una brecha entre la población que no tiene conocimiento de temas tecnológicos o de ingeniería. Por lo tanto, la divulgación del proceso de automatización, la capacitación a la población y las auditorías al sistema son indispensables para brindar confianza a la ciudadanía.
- Un sistema de votación debe ser continuamente evaluado y mejorado no solo por instituciones del gobierno sino también por terceras partes.

2.1.2 SITUACIÓN ACTUAL DEL PROYECTO DE AUTOMATIZACIÓN DEL VOTO EN ECUADOR

Ecuador planteó en el año 2012 modernizar el sistema de votación. Para tal objetivo, nuestro país solicitó el apoyo a Venezuela, Rusia y Argentina. La estrategia de Ecuador es someter a prueba los sistemas de votación de estos países para seleccionar una tecnología. La tecnología seleccionada servirá de base para desarrollar un sistema de votación propio de Ecuador.

El 23 de febrero del 2014, el CNE de Ecuador realizó el primer ejercicio de votación digital en el cual participaron aproximadamente 900.000 personas. Los electores fueron de las provincias del Azuay, Santo Domingo de los Tsáchilas y La Morita en Pichincha. En estas provincias se utilizaron tecnologías implementadas en Argentina, Venezuela y Rusia, respectivamente. [18]

Sistema de Votación argentino: este sistema consiste en equipos de registro e impresión del voto, y una papeleta con inteligente. La papeleta debe ser introducida

en la máquina para poder votar. Los votos son almacenados en el chip de la papeleta electrónica. El escrutinio consiste en que cada una de estas papeletas sea pasada nuevamente por la máquina para ser contadas.

Sistema de Votación venezolano: este sistema almacena, contabiliza, totaliza y transmite los resultados como un proceso integral. [19] Este sistema está compuesto por máquinas con pantalla táctil e imprime un comprobante del voto en papel. [20]

Sistema de Votación ruso: este sistema consiste en una máquina de pantalla táctil que registra y almacena los votos, también incorpora un dispositivo de identificación del elector. Las máquinas se activan con una tarjeta de seguridad que contiene un código de barras. El sistema únicamente almacena los votos y no imprime en papel un comprobante. Las máquinas poseen una tira auditora para registrar todos los movimientos y cifras que se ingresan al sistema. [21] Las funcionalidades de este sistema son: captación de los votos, automatización de la cuenta de votos, elaboración de actas con los resultados de la votación, y transmisión segura de datos al centro de totalización. [22]

En la tabla 1.4 se presenta datos comparativos de los tres tipos de tecnología usadas en las elecciones de febrero de 2014 en Ecuador.

Característica	Azuay - Tecnología argentina	Santo Domingo de los Tsáchilas - Tecnología venezolana	La Morita Pichincha - Tecnología rusa
Número de electores.	600 mil personas.	300 mil personas.	194 personas.
¿Los electores fueron capacitados en el uso de esta tecnología previo al día de votación?	Si	Si	Si
Autenticación Biométrica.	No	Si	No
Imprime comprobante del voto en papel.	Si [23]	Si [24]	No [21]
¿Posee un sistema de respaldo de la información?	Si, almacena la información en un chip e imprime los votos en papel.	Si, guardar dos registros digitales y uno en papel de cada voto.	No, únicamente almacena los votos en cada máquina.
¿Se presentó problemas durante el proceso de votación?	Si, hubo fallos en el sistema. Problemas con las fotografías de candidatos de una misma lista. Quejas de los electores por demora. Desconocimiento del uso de los equipos. [25]	Ninguno.	Ninguno.

Tabla 2-4. Tabla comparativa de las tecnologías de sufragio probadas en Elecciones 2014 de Ecuador

El CNE posterior a las elecciones dio a conocer lo siguiente:

- El tiempo promedio de sufragio de los 3 sistemas de votación fue de dos a tres minutos. [26]
- Tiempo para emitir resultados luego del cierre de las JRV fue de 2 horas.

La tecnología de sistemas de votación que obtuvo los mejores resultados es la venezolana, porque:

- Los electores no tuvieron problemas con el uso de este sistema.
- Todas las fases del proceso de sufragio pueden ser automatizadas con esta tecnología.
- El sistema almacena 2 registros digitales y uno en papel de cada voto.
- Posee autenticación biométrica.
- La autenticación del votante se realiza a través de una máquina distinta a la que captura los votos.

Sin embargo se han identificado errores por parte del CNE en el proceso para automatizar el proceso de votación, estos se mencionan a continuación:

1. En la actual Ley Electoral y Constitución de la República no hay artículos específicos sobre la votación electrónica. Todo queda a discreción del CNE.
2. Las leyes sobre protección de datos no han sido revisadas ni actualizadas. Esto es necesario para tipificar los delitos informáticos y sancionar en caso de presentarse.
3. Cualquier sistema propuesto por el CNE debe someterse a escrutinio público.

En un sistema tradicional de votación únicamente se debe confiarse en el CNE. Pero la adquisición de un sistema automatizado requiere confiar en la empresa que ha producido el sistema, en sus trabajadores y cualquier tercera parte que tenga contacto con el software o hardware. Si el sistema es proporcionado por una

empresa, esto conlleva posiblemente a que el software y hardware sean propietarios y no se disponga de todas la información para analizar sus vulnerabilidades.

Otro factor a considerar es el lugar de almacenamiento de las máquinas y su distribución a los distintos recintos electorales. Esta logística requiere implementar procedimientos para la cadena de custodia de los equipos. En este sentido el CNE no ha dado a conocer a la ciudadanía información al respecto.

2.2 LEVANTAMIENTO DE REQUERIMIENTOS FUNCIONALES

El objetivo de este subcapítulo es definir los requerimientos necesarios que el sistema de votación digital debe implementar. El subcapítulo se divide en tres secciones: requerimientos de software, requerimientos de red y requerimientos de seguridad. Los requerimientos son obtenidos de las leyes vigentes en el país descritas en el Capítulo I y en la experiencia de países que han implementado la votación digital. A continuación se detallan cada uno de los tipos de requerimientos.

2.2.1 REQUERIMIENTOS DE SOFTWARE

Los requerimientos funcionales de software fueron obtenidos a través del análisis de la normativa que reglamente el proceso electoral en el Ecuador, los procesos de sufragio establecidos en el artículo 115 de la Ley Electora y los problemas identificados de los procesos analizados en el capítulo I.

Adicional se ha considerado las estadísticas sobre personas con discapacidad empadronadas para las elecciones del 23 de febrero del 2014. El detalle de estas estadísticas se encuentra en el Anexo K.

El levantamiento de los requerimientos de software se realiza a través de Historias de Usuario. De estas historias se obtienen:

- El product backlog o lista de requisitos del software.

- Los módulos del software.
- Los actores que interactúan con el software.
- Limitaciones del software.

Las historias de usuario y el Producto Backlog se encuentran en los anexos I y J.

2.2.1.1 Módulos del software

Los requisitos del software de votación deben agruparse en módulos para facilitar su implementación. Estos módulos son: Autenticación, Votación, Conteo, Resultados.

2.2.1.1.1 Módulo de Autenticación

Las funciones de este módulo son:

- Permitir a los miembros de la JRV validar que el votante se encuentre habilitado en el Padrón Electoral para sufragar.
- Generar un token físico de autenticación, para el ingreso a la aplicación.
- Validar que el votante ingrese un número de cédula correcto a través del token físico.
- Verificar que el votante pertenezca a la JRV desde la cual intenta sufragar.
- Validar que el votante únicamente sufrague una vez.
- Determinar si el votante puede acceder o no a la papeleta de votación digital.

Las interacciones entre este módulo y el votante, las notificaciones tienen que presentarse en mensajes en texto en la pantalla y en audio.

Se considera a un votante habilitado cuando:

- El votante consta en el Padrón Electoral como habilitado.
- El votante va a emitir su voto por primera vez.
- El votante envía su voto desde la JRV asignada para él.

2.2.1.1.2 Módulo de Votación

Las funciones de este módulo son:

- Permitir al votante elegir los candidatos de su preferencia a través de la papeleta de votación digital. Para el caso de personas con discapacidad visual se dispondrá de láminas plásticas en braile. Cada lámina tendrá mapeada una de las papeletas de votación digital.
- Permitir al votante emitir su voto en blanco, nulo o válido.
- Enviar los votos encriptados.
- Firmar digitalmente el voto emitido por un votante habilitado.
- Rechazar el voto emitido por un votante no habilitado.
- Permitir al votante corregir su voto.
- Imprimir el comprobante en papel del voto emitido.
- Desligar la identificación del voto de su voto emitido.

Las interacciones entre este módulo y el votante, las notificaciones tienen que presentarse en mensajes en texto en la pantalla y en audio.

2.2.1.1.3 Módulo de Conteo

Las funciones de este módulo son:

- Desencriptar y permutar los votos recibidos.
- Almacenar y generar un reporte de los votos que no pudieron ser desencriptados.
- Contabilizar los votos en claro.

2.2.1.1.4 Módulo de Resultados

La función de este módulo es:

- Generar reportes digitales de los resultados finales del proceso de sufragio.
- Imprimir los reportes digitales.

- Permitir exportar los datos a otra fuente de datos para realizar consultas personalizadas.

Los reportes digitales son:

- Obtener el nombre de la dignidad, los nombres de los candidatos, su organización política y sus votos obtenidos. Los datos serán agrupados por la dignidad y ordenados en forma descendente por el número de votos obtenidos por cada candidato.
- Obtener el nombre de las provincias, los nombres de los candidatos, su organización política y sus votos obtenidos. Los datos serán agrupados por provincia y ordenados en forma descendente por el número de votos obtenidos por cada candidato.
- Obtener el nombre de las provincias, el nombre de la dignidad, el nombre de las organizaciones políticas y su número de votos obtenidos. Los datos serán agrupados en forma descendente por el número de votos obtenidos por cada organización política.

2.2.1.2 Actores del software

Los actores del software de votación son el votante y el publicador de resultados.

2.2.1.3 Limitaciones del software

- El prototipo de software se desarrollará bajo la plataforma Java.
- El prototipo de software utilizará librerías de libre distribución.
- El prototipo de software no realizará la asignación de escaños.
- El prototipo de software emulará el comportamiento de los servidores de firmas ciegas y de autenticación, con métodos de autenticación simples.

2.2.1.4 Supuestos

- Para el desarrollo del sistema se asume canales de comunicación segura.
- Para el diseño del prototipo se asume que existe un padrón electoral a ser expuesto en los servicios web de autenticación.
- Se asume que existe un listado de candidatos para la presentación y voto.
- Se asume que los electores fueron capacitados en el uso del software de votación.
- Se asume que existe una infraestructura PKI.

2.2.2 REQUERIMIENTOS DE RED

Los requerimientos de red fueron analizados en torno a los siguientes criterios:

- Función principal de la red.
- Número proyectado de usuarios concurrentes.
- Ancho de banda.
- Tolerancia a fallos.
- Cantidad de bytes enviados en cada sesión. [27] [28]

Las estadísticas de las votaciones en el Ecuador desde el año 2004 hasta 2014 fueron la base para determinar los requerimientos de red.

Los requerimientos se detallan a continuación.

2.2.2.1 Función Principal de la Red

La tarea primordial de la red es realizar transacciones[12] en tiempo real. Por lo tanto, el desempeño[13] asume una muy alta prioridad y por lo tanto se eleva el costo de la red.

[12] Las transacciones son operaciones que se ejecutan entre dos partes utilizando un esquema predefinido, compuesto por varias operaciones que se implementan secuencialmente.

Para obtener un alto desempeño de la red, se requiere:

- La velocidad del procesador: esta velocidad tiene una relación directamente proporcional con el rendimiento de la red. La velocidad del CPU de los dispositivos de red los hacen capaces de procesar toda la información que les llega en menor tiempo.
- Número de núcleos del procesador: un procesador con más de un core tiene mejor velocidad de cálculo y disminuye el tiempo de respuesta. [29]
- Reducir el número de paquetes enviados: es ventajoso usar paquetes de tamaño grande para hacer menos envíos posibles y evitar la sobrecarga.
- Memoria insuficiente de los conmutadores.
- Diseñar la red con norma Ethernet a 1000 Mbps: a mayor velocidad del medio de transmisión se van eliminado los cuellos de botella que vuelven lento el tráfico dentro de la red. Esta configuración, es “ampliamente recomendable para todas aquellas redes informáticas que tienen un elevado volumen de tráfico”. [30]
- Tarjetas de red no defectuosas.

2.2.2.2 Número proyectado de usuarios concurrentes

El padrón electoral de Ecuador proyecta un crecimiento promedio anual de 296.929,6 personas. Esta medición se obtuvo de datos entre los años 2004 y 2014. El número de electores tiene una relación directamente proporcional al número de JRV necesarias.

Por lo tanto, el diseño de red debe considerar este crecimiento y planearse de forma modular para facilitar la escalabilidad.

---

[13] Es una medida concreta que permite saber si una red está funcionando en forma óptima

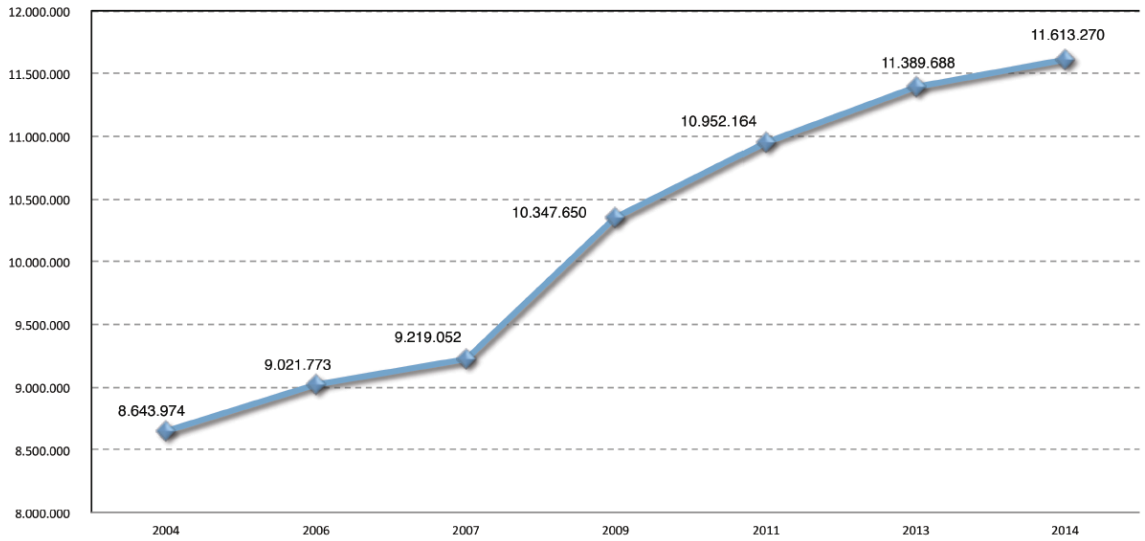


Figura 2-1. Crecimiento del Padrón Electoral en Ecuador. Fuente: http://www.slideshare.net/roxanasilvach/estadisticas-del-registro-electoral-2014 pág. 9

En las elecciones de febrero de 2014, el número de votantes fue de 11.613.270 y se distribuyen por provincias de la siguiente manera:

Provincias	Electores Totales	Mujeres	Hombres	Juntas Totales
AZUAY	608766	313503	295263	2160
BOLIVAR	155507	78644	76863	590
CAÑAR	215830	109658	106172	766
CARCHI	136194	67802	68392	506
CHIMBORAZO	390652	202420	188232	1378
COTOPAXI	328909	168844	160065	1144
EL ORO	488527	238881	249646	1734
ESMERALDAS	358037	174272	183765	1310
GALAPAGOS	18485	8636	9849	71
GUAYAS	2865319	1442381	1422938	9666
IMBABURA	335032	170904	164128	1191
LOJA	371137	186339	184798	1359
LOS RIOS	596756	290271	306485	2039
MANABI	1111377	545018	566359	3851
MORONA SANTIAGO	111894	53877	58017	560
NAPO	74114	36199	37915	304
ORELLANA	95697	43614	52083	392
PASTAZA	62468	30381	32087	267
PICHINCHA	2117734	1081423	1036311	7264
SANTA ELENA	219041	108269	110772	763
STO DGO TSACHILAS	326932	161093	165839	1125
SUCUMBIOS	124805	56054	68751	486
TUNGURAHUA	427061	218247	208814	1488
ZAMORA CHINCHIPE	72996	34452	38544	349
TOTAL GENERAL	**11613270**	**5821182**	**5792088**	**40763**

Tabla 2-5. Distributivo De Electores A Nivel Nacional Para Las Elecciones Seccionales 2014, Desagregado Por: Provincia, Cantón, Circunscripción, Parroquia Y Zona Electoral. Fuente; http://goo.gl/zcHVkd

El número total de JRV fue de 40763 como se indica en la tabla 1.7. Cada JRV representa a un terminal de votación, es decir un usuario de la red. El número de usuarios concurrentes por lo tanto son 40763 para el año 2014.

Considerando que el crecimiento promedio anual del Padrón Electoral es de 296.929,6. Entonces, el cálculo del número de JRV necesarias para el año 2015 es el siguiente:

$$x = \frac{\text{Electores totales 2014}}{JRV\ totales\ 2014} = \frac{11613270}{40763} = 284{,}897 \text{ personas por JRV}$$

$$\text{JRV totales 2015} = \frac{\text{Electores totales} + \text{crecimiento promedio anual}}{284{,}897}$$

$$\text{JRV totales 2015} = \frac{11613270 + 296929{,}6}{284{,}897} = \frac{11910199{,}6}{284{,}897} = 41805{,}282$$

Año	# Juntas Electorales Concurrentes
2014	40763
2015	41805,282

Tabla 2-6. Usuarios concurrentes actuales y proyectados.

El número de usuarios concurrentes proyectados de la red para el año 2015 es 41805,282 Juntas Electorales.

2.2.2.3 Ancho de banda

La estimación del ancho de banda de la red debe asegurar que sea suficiente para el futuro crecimiento de la red. Para realizar esta estimación se determinará a continuación el tamaño de la trama para el peor caso.

2.2.2.3.1 Estimación del tamaño de la trama

El cálculo del tamaño de la trama será establecido con respecto a los datos de la provincia del Guayas. Esta provincia es utilizada por ser la que contiene la mayor población a nivel nacional, representando así el peor caso.

Elecciones Seccionales del 2014, en la provincia del Guayas se inscribieron 8 agrupaciones políticas y fueron elegidas las siguientes dignidades:

- 1 Prefecto/a.
- 1 Viceprefecto/a.
- 25 alcaldesas o alcaldes.
- 137 Concejalas/les urbanos.
- 24 Concejalas/les rurales.
- 29 Juntas parroquiales rurales.
- 145 Vocales de las Juntas Parroquiales rurales.

Por lo tanto la trama de mayor tamaño corresponderá a la elección de la dignidad "Concejales Urbanos" con 137 personas y "Vocales de las Juntas Parroquiales rurales" con 145 personas. Además para el área urbana se tiene 9219 JRV y el área rural de 447 JRV.

El número de organizaciones políticas multiplicado por el número de personas a elegirse da como resultado el número total de candidatos totales.

Área	# Organizaciones Políticas	# Personas Elegidas por Dignidad	# Candidatos por Dignidad	# JRV
Urbana	8	137	1096	9219
Rural	8	145	1160	447

Tabla 2-7. Datos de Agrupaciones Políticas y Número de Candidatos de la Provincia del Guayas.

Con base a los datos de la tabla 1-9, la determinación del tamaño de la trama a transmitirse por la red para el peor caso será considerando la elección de Concejales Urbanos. Entonces para el peor caso se tiene 1096 candidatos y 9219 JRV.

Para representar un voto a un candidato, se utilizará 3 números.

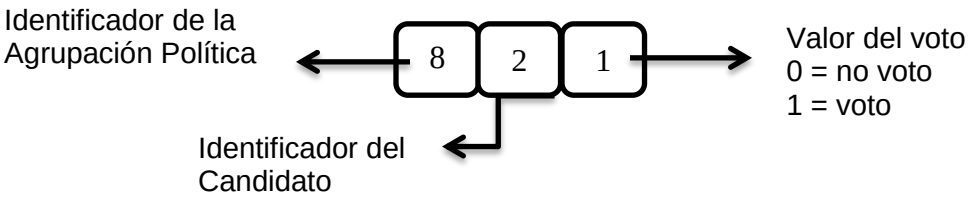


Figura 2-2. Representación de un Voto para un Candidato.

El primer número representa la agrupación política a la cual pertenece el candidato, el segundo número representa el código del candidato y el tercer número indica si obtuvo un voto o no.

El tamaño total del voto será determinado con base a la cantidad de candidatos por la longitud requerida para representar el voto de un candidato, esto es 3 como se explicó anteriormente.

Los candidatos totales presentados se determinarán bajo la siguiente operación:

$$x = \ \#\ de\ personas\ por\ dignidad\ * \#\ agrupaciones\ políticas$$

$$x = \ 137\ * 8$$

$$1096$$

A esta cifra se le añade el valor de dos “candidatos” extras, que representarán a las opciones de blanco y nulo.

$$\#\ candidatos\ Totales = \ 1096 + 2$$

$$\#\ candidatos\ Totales = \ 1098$$

La longitud del voto total se obtiene multiplicando el número de candidatos totales por 3:

$$longitud\ del\ voto = \ 1098\ * 3$$

$$longitud\ del\ voto = \ 3294$$

Cada número del voto será almacenado en un tipo de dato *short*, este tipo de dato ocupa 2 bytes. El rango de números representados por un short va desde -32768 a 32767.

Por lo tanto para finalizar, la longitud del voto se multiplica por 2 bytes, así obtenemos el valor un voto en bytes.

$$valor\ del\ voto\ en\ claro \ = \ 3294 \ * 2$$
$$valor\ del\ voto\ en\ claro = \ 6588\ bytes$$

El paso siguiente es determinar la longitud de la cadena encriptada. Para esto se considerará el estándar de encriptación RSA.

Dentro de este protocolo, se utilizará una llave de 2048 bits, que es lo recomendado en la actualidad. [31] Esta llave permitirá encriptar un máximo de 245 bytes. Entonces para obtener el tamaño de la trama encriptada, se dividirá la longitud del texto plano para la cantidad máxima de caracteres a ser encriptados con la llave de 2048 bits.

$$número\ de\ bloques = \ \frac{6588}{245} = 26.889.. \approx 27$$

Por lo tanto se tendrán 27 bloques a ser encriptados. Cada bloque encriptado sin importar su longitud va a medir 256 bytes, por lo que el total de la trama encriptada será:

$$tamano\ trama\ encriptada = \ 27 * 256 = 6912\ bytes$$

Este proceso se repetirá según el número de servidores Mix por los que vaya a pasar el dato encriptado. De acuerdo al diseño de seguridad planteado serán 3 servidores mix.

Número de capas de encriptación	Cadena en claro(bytes)	Número de bloques	Cadena encriptada (bytes)
Primera encriptación	6588	27	6912
Segunda encriptación	6912	29	7424
Tercera encriptación	7424	31	7936

Tabla 2-8. Capas de Encriptación y Longitud de Trama.

La cadena encriptada por tres ocasiones conteniendo el voto tendrá una longitud de 7936 bytes. Adicionalmente hay que añadir a este valor el tamaño de la estructura xml que posee la información al viajar como servicio web de tipo SOAP, que se estima en 300 bytes. Por lo tanto el estimado total del tamaño de la petición del voto del peor escenario será de 8236 bytes.

Finalmente para obtener un estimado del ancho de banda necesario, se multiplicará el tamaño del mensaje en el peor de los casos por la cantidad de peticiones concurrentes, que será el número de Juntas receptoras del voto y obtendremos el total del ancho de banda necesario para las peticiones.

$$Ancho\ de\ Banda = 8236\ bytes\ * 9219\ JRV$$
$$Ancho\ de\ Banda = 75927684\ bytes$$

Por lo tanto para el peor de los casos se requerirá un ancho de banda de por lo menos 72,41 mps.

2.2.2.4 Tolerancia a fallos

Los dispositivos de red, servidores y los enlaces deben ser redundantes. La redundancia mitiga el riesgo quedar fuera de servicio debido a fallos en los equipos de comunicaciones, servidores o el medio de transmisión.

2.2.3 REQUERIMIENTOS DE SEGURIDAD

En esta sección se realizará el levantamiento de requerimientos de seguridad. Los requerimientos de seguridad son establecidos en relación a las características del voto prescritas en la Constitución de la República y en los requerimientos de software y de red.

- El voto debe ser directo, es decir cada votante elige a sus gobernantes directamente, sin ninguna intermediación por parte de otra persona u órgano colegiado que no sea el CNE.
- El voto debe ser secreto, es un respaldo del sistema electoral con el fin de imposibilitar que otra persona pueda influir en la decisión de voto de un elector.
- El voto debe ser escrutado públicamente.
- Una persona que no conste en el Padrón Electoral no puede sufragar.
- Una persona no puede sufragar más de una vez.
- Una persona no puede ser vinculada con un voto.
- Los canales de comunicación deben ser seguros.
- La información a ser enviada debe ser cifrada.
- La información debe almacenarse cifrada.
- Únicamente terminales autorizadas pueden enviar votos.
- Los canales de comunicación deben tener el suficiente ancho de banda para transmitir todos los votos sin sobrecargarse.
- La red debe implementar redundancia para proveer alta disponibilidad.

- Se debe realizar backups de la información.

2.3 ANÁLISIS DE RIESGOS

El objetivo de este subcapítulo es analizar los riesgos que afectan al sistema de votación digital y proponer controles para mitigarlos. El análisis de riesgo se realiza con las fases indicadas en la Guía de Gestión de Riesgos para Sistemas de Tecnología de la Información NIST SP 800-30. Cada sección de este subcapítulo corresponde a un paso de la guía. En la sección 2.3.1., se realiza la caracterización del sistema. La sección 2.3.2., contiene la identificación de las amenazas. Estas amenazas se clasifican según su naturaleza. En la sección 2.3.3., se describe las principales vulnerabilidades que presenta el sistema de votación digital. La sección 2.3.4., contiene el análisis de los controles que posee el sistema de votación digital. En la sección 2.3.5., se determina la probabilidad de ocurrencia que una amenaza explote alguna vulnerabilidad del sistema de votación digital. La sección 2.3.6., contiene el análisis del impacto que una amenaza explote alguna vulnerabilidad. En la sección 2.3.7, se determina la valoración de riesgos. Finalmente en la sección 2.3.8., se realizan recomendaciones sobre los controles de la sección 2.3.4.

2.3.1 CARACTERIZACIÓN DEL SISTEMA

La caracterización del sistema consiste en identificar los recursos e información que constituyen la infraestructura tecnológica de votación digital. Recopilar estos datos es esencial para conocer el ambiente de procesamiento de la infraestructura tecnológica de votación digital e identificar los riesgos que le afectan.

Con base a los requerimientos de software, de red y seguridad, los recursos e información que componen la infraestructura tecnológica de votación digital son:

- **Hardware**
  - Servidores de aplicaciones y base de datos.
  - Switches,
  - Routers,
  - Equipos de seguridad de red.
- **Software**
  - Servidor de aplicaciones,
  - Gestor de base de datos,
  - Sistema de votación incluye autenticación del elector, recepción y conteo de votos
- **Datos e Información**
  - Datos de autenticación para la votación,
  - Votos emitidos,
  - Papeleta digital que contiene la lista de los candidatos de los movimientos políticos,
  - Padrón Electoral.
  - Llaves públicas y privadas para encriptación de votos.
- **Personas**
  1. Miembros de la JRV
  2. Votante: Emisor del voto
  3. Personal de Soporte Técnico
  4. Personal de administración de servidores
- **Misión de la Infraestructura tecnológica de votación digital**
  - Captar los votos de los ciudadanos de manera íntegra y confiable, considerando la normativa vigente en las leyes.
  - Proveer datos certeros de los resultados del proceso de sufragio en menor tiempo y con menor exposición a la manipulación del personal y otros agentes externos.

2.3.1.1 Características del Sistema

En función de estos datos se ha caracterizado el sistema bajo las siguientes consideraciones:

- **Límites de la Infraestructura tecnológica de votación digital**
  - El sistema contempla la captación de los votos de cada ciudadano, el escrutinio de los mismos y los reportes de los resultados,
  - El sistema no realiza la elaboración del padrón electoral.
  - El sistema no realiza la asignación de escaños.
- **Funciones de la Infraestructura tecnológica de votación digital**
  - Validar que un ciudadano este habilitado para votar,
  - Receptar el voto emitido de cada ciudadano,
  - Garantizar un envío seguro de la información generada en las JRV,
  - Determinar la validez de los votos captados,
  - Escrutar los votos captados,
  - Emitir un informe de los votos asignados a cada candidato,
  - Asegurar que un ciudadano pueda emitir solamente un voto,
  - Asegurar que los votos tienen que llegar íntegros a su destino,
- **Datos e Información Crítica**
  - Los datos enviados a través de este sistema son: la identificación del votante, votos, llaves públicas de los servidores, papeleta de votación.
  - Por la naturaleza de la información y misión del sistema, todos los datos que se manejan son considerados críticos.

2.3.2 IDENTIFICACIÓN DE AMENAZAS

Las amenazas son eventos que pueden desencadenar un incidente sobre los activos de la organización produciendo daños materiales o inmateriales. Las amenazas que se identificaron provienen de tres tipos de fuentes, estas son:

- Humanas

- Naturales
- Ambientales

2.3.2.1 Amenazas Humanas

Fuente	Motivación	Acción de la amenaza
Hacker, cracker	• Desafío. • Ego. • Rebeldía.	• Hacking.[14] • Ingeniería Social. • Intrusión al sistema para robo de información. • Acceso no permitido.
Criminal Computacional	• Obtener rédito económico. • Divulgación de información. • Alteración de la información. • Destrucción de la información.	• Modificación de la información. • Intercepción de la información • Intrusión al sistema. • Soborno. • Suplantación de identidad.
Terrorista	• Venganza. • Chantaje. • Desprestigio de entidades o gobiernos. • Destrucción.	• Ataques físicos a instalaciones. • Ataques a los sistemas. • Bomba. • Ataque del sistema (por ejemplo, la negación de servicio distribuido). • Penetración del sistema. • Manipulación sistema.

[14] Búsqueda de conocimientos sobre sistemas informáticos, sus mecanismos de seguridad, vulnerabilidades y como explotarlas.

		• Guerra de información.
Espías	• Ventaja competitiva. • Espionaje económico.	• Explotación económica. • Robo de información. • Penetración al sistema. • Ingeniería Social. • Acceso a información clasificada.
Personal Negligente	• Descuido. • Distracción. • Curiosidad.	• Obviar algún control. • Divulgar claves o certificados. • Errores del sistema. • Asalto a un empleado.
Personal Malintencionado	• Venganza. • Retribución económica. • Ego.	• Comercio de información sensible. • Venta de información personal • Chantaje. • Sabotaje del sistema. • Acceso no autorizado al sistema.

Tabla 2-9. Amenazas Humanas. Fuente: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

2.3.2.2 Amenaza Natural

Fuente	Causa	Acción de la amenaza
Inundación	• Lluvia excesiva provoca desbordamiento de ríos y colapso de los sistemas de alcantarillado.	Causa daño físico a la infraestructura y evita que la gente se acerque al lugar de votación.
Terremoto y temblores	• Movimiento de las placas tectónicas	Causa daño físico a la infraestructura haciéndola inoperable y provocando la muerte de las personas.
Deslaves y hundimiento de tierras	• Lluvia • Inestabilidad del terreno • Explosión • Erosión	Causa daño físico a la infraestructura y evita que la gente acuda a los lugares de votación. También puede causar muerte a las personas.
Erupción Volcánica	• Presión por el acumulamiento de gases, rocas calientes, ceniza y material incandescente en el interior de la Tierra a lo largo de años.	Causa daño físico a la infraestructura haciéndola inoperable y provocando la muerte de las personas.
Tormentas Eléctricas	• La humedad del aire caliente que se eleva en una atmósfera inestable.	Puede causar daño físico a la infraestructura y muerte o heridas a las personas.
Tsunami	• Un terremoto con epicentro	Causa daño físico a la

	en el fondo del mar.	infraestructura convirtiéndola inoperable y provocando la muerte de las personas.

Tabla 2-10. Amenazas Naturales.

2.3.2.3 Amenaza del Ambiente

Fuente	Causa	Acción de la amenaza
Derrame de químicos	• Negligencia • Acciones deliberadas	• Daño físico a la infraestructura. • Inoperatividad de la infraestructura. • Impide al votante llegar al lugar para sufragar.
Corte de energía a largo plazo	• Daño en el sistema eléctrico del sector.	• Inoperatividad de la infraestructura.
Fuga de agua masiva	• Tubería en mal estado • Choque de algún vehículo contra un hidrante.	• Daño físico a la infraestructura. • Impide al votante llegar al lugar para sufragar.

Tabla 2-11. Amenazas Ambientes.

2.3.3 IDENTIFICACIÓN DE VULNERABILIDADES

El objetivo de este paso es obtener una lista de vulnerabilidades de la Infraestructura tecnológica de votación digital. Una vulnerabilidad es un defecto o debilidad del sistema.

Debido a que la Infraestructura tecnológica de votación digital aún no ha sido diseñada, la búsqueda de vulnerabilidades se realizará con base en los requerimientos de software, de red, de seguridad y los recursos de la infraestructura tecnológica de votación digital.

Las vulnerabilidades de la Infraestructura tecnológica de votación digital se dividirán en tres grupos:

- Humanas.
- Naturales.
- Ambientales.

A continuación se presenta el detalle de cada grupo de vulnerabilidades, su posible ejecutor y la acción de la amenaza correspondiente:

2.3.3.1 Humanas

Vulnerabilidad	Amenaza	Acción de la amenaza
Personal que acepte sobornos.	• Criminal Computacional. • Espías. • Personal malintencionado.	Modificación e intercepción de la información. Intrusión al sistema. Soborno. Suplantación de identidad. Explotación económica. Robo de información. Ingeniería Social.

		Acceso a información clasificada. Comercio de información sensible. Chantaje. Sabotaje del sistema.
Personal sin capacitación técnica.	• Personal Negligente.	Obviar algún control. Divulgar claves. Errores del sistema.
Desconocimiento del personal sobre las actividades a realizar en caso de emergencias.	• Personal Negligente.	Obviar algún control. Divulgar claves. Errores del sistema.
Personal no ha recibido capacitación sobre ataques a través de ingeniería social.	• Hacker, cracker. • Criminal Computacional.	Hacking. Ingeniería Social. Intrusión al sistema. Acceso no permitido. Modificación e intercepción de la información.
Curiosidad.	• Personal Negligente y Malintencionado.	Obviar algún control. Provocar errores en el sistema. Sabotaje del sistema. Acceso no autorizado al sistema.
Chantaje y amenazas al personal por parte de un criminal.	• Criminal Computacional. • Terroristas.	Modificación e intercepción de la información. Intrusión al sistema. Suplantación de identidad. Ataques físicos a instalaciones. Ataques a los sistemas. Bomba. Manipulación sistema. Guerra de información.
Personal que no cumpla	• Hacker, cracker.	Robo de información.

las políticas de seguridad.	• Criminal Computacional. • Personal Malintencionado. • Espía.	Penetración al sistema. Ingeniería Social. Acceso a información clasificada. Comercio de información sensible. Chantaje. Hacking. Modificación e intercepción de la información. Suplantación de identidad.

Tabla 2-12. Vulnerabilidades Humanas.

2.3.3.2 Naturales

Vulnerabilidad	Amenaza	Acción de la amenaza
Ecuador se ubica en una zona de intensa actividad sísmica y volcánica	• Terremoto. • Temblores. • Erupción Volcánica. • Tsunami.	Causa daño físico a la infraestructura haciéndola inoperable y provocando la muerte de las personas.
Deforestación del territorio, sobrepastoreo, erosión inducida, minería desorganizada. [32]	• Deslaves y hundimiento de tierras. • Inundación.	Causa daño físico a la infraestructura y evita que la gente acuda a los lugares de votación. También puede causar muerte a las personas.
Ubicación de Ecuador en la zona ecuatorial. Esta zona presenta la mayor actividad de tormentas eléctricas. [33]	• Tormentas Eléctricas.	Puede causar daño físico a la infraestructura y muerte o heridas a las personas.

Tabla 2-13. Vulnerabilidades Naturales.

2.3.3.3 Ambientales

Vulnerabilidad	Amenaza	Acción de la amenaza
Infraestructura de recintos electorales en mal estado	• Fuga de agua masiva.	Daño físico a la infraestructura. Inoperatividad de la infraestructura. Impide al votante llegar al lugar para sufragar.
Pérdida de energía eléctrica en los sistemas de distribución	• Corte de energía a largo plazo.	Inoperatividad de la infraestructura.
Estado de los oleoductos para transporte de petróleo	• Derrame de químicos.	Daño físico a la infraestructura. Impide al votante llegar al lugar para sufragar.

Tabla 2-14. Vulnerabilidades Ambientales

2.3.4 ANÁLISIS DE CONTROLES

El objetivo de este paso es examinar los controles implementados o planeados para reducir al mínimo la probabilidad que una amenaza explote una vulnerabilidad del sistema.

La infraestructura tecnológica para votación aún no ha sido diseñada, el análisis de controles no se puede realizar. Sin embargo, en esta sección se propone una lista de controles con base en los requerimientos de software, de red y de seguridad.

Los controles propuestos se clasifican en tres grupos:

- Controles físicos.

- Controles técnicos.
- Controles administrativos.

2.3.4.1 Controles Físicos

- Cámaras de circuito cerrado.
- Sistemas de alarmas térmicos o de movimiento.
- Guardias de seguridad.
- Identificación del personal debe poseer fotografía.
- Las puertas del cuarto de datacenter y cuartos de almacenamiento de información debe ser de acero con seguros especiales.
- El acceso al datacenter y cuartos de almacenamiento de información debe ser biométrico.
- Disponer de una planta eléctrica.
- El cableado debe estar dentro de tubería.

2.3.4.2 Controles Técnicos

- Autenticación a nivel de la red.
- Listas de control de acceso (ACLs).
- Sistemas de prevención de intrusos en los diferentes módulos de la red.
- Desactivación de puertos físicos y lógicos innecesarios de los servidores y equipos terminales.
- Desactivación de servicios innecesarios de los servidores y equipos terminales
- Detectores de ataques de tipo DOS.
- Almacenamiento de información crítica encriptada.
- Usar canales de comunicación encriptados.
- Enviar información encriptada.
- Implementar sistema de redundancia de todos los equipos críticos.

2.3.4.3 Controles Administrativos

- Planificar la contratación de personas suficiente para realizar todas las actividades requeridas durante el proceso de sufragio.
- Contar con planes de recuperación y preparación para desastres.
- Realizar simulacros de emergencias para entrenamiento del personal.
- Llevar un registro y contabilidad de personal.
- Firmar acuerdos de confidencialidad con el personal.
- Hacer una clasificación de los niveles de confidencialidad de los datos.
- Establecer políticas de manejo de la información y acceso a sitios restringidos y sus sanciones en caso de incumplimiento.
- Capacitación y evaluación al personal sobre delitos informáticos, técnicas de hacking, ingeniería social.
- Establecer una cadena de custodia para el almacenamiento y de los equipos que se usarán en el proceso de votación.
- Planificación técnica de la ubicación de los recintos electorales para garantizar cobertura de red para implantación de voto digital y en zonas de bajo riesgo de catástrofe natural y ambiental.

2.3.5 DETERMINACIÓN DE LA PROBABILIDAD

El cálculo de la probabilidad de la ocurrencia que una vulnerabilidad sea explotada por una amenaza se debe considerar los siguientes factores:

- Motivación de la amenaza.
- Naturaleza de la vulnerabilidad.
- Existencia y eficacia de los controles.

Para esto, se emplea una escala cualitativa de la probabilidad, la cual se muestra en la tabla 2-16.

Grado	Definición
Alto	La fuente de amenaza, está altamente motivada, tenga la suficiente capacidad y los controles para prevenir la vulnerabilidad están siendo inefectivos.
Medio	La fuente de amenaza está motivada, cuenta con la suficiente capacidad, pero existen controles pueden impedir exitosamente el aprovechamiento de la vulnerabilidad.
Bajo	La fuente no tiene la suficiente capacidad o motivación, ó los controles impiden o al menos significativamente reducen la probabilidad de la ejecución de la vulnerabilidad.

Tabla 2-15. Definiciones de Probabilidad. Fuente: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

El análisis de la probabilidad será divido de acuerdo al tipo de fuente de la amenaza, estos son:

- Humanas.
- Naturales.
- Ambientales.

2.3.5.1 Análisis de la probabilidad de ocurrencia de amenazas humanas

Vulnerabilidad	Amenaza	Control	Probabilidad
Personal que acepte sobornos.	• Criminal Computacional. • Espías. • Personal malintencionado.	Se cuenta con políticas de seguridad de la información y sanciones en caso de incumplirlas.	Alto
Personal sin capacitación técnica.	• Personal Negligente.	La contratación del personal se realiza con planificación y de acuerdo a perfiles profesionales.	Bajo
Desconocimiento del personal sobre las actividades a realizar en caso de emergencias.	• Personal Negligente.	Se tiene planes para de preparación y recuperación ante desastres y capacitación al personal.	Bajo
Personal no ha recibido capacitación sobre ataques a través de ingeniería social.	• Hacker, cracker. • Criminal Computacional.	Se cuenta con planes de capacitación sobre hacking.	Bajo
Curiosidad.	• Personal Negligente y Malintencionado.	Se cuenta con políticas de seguridad de la información y sanciones en caso de incumplirlas.	Medio

Chantaje y amenazas al personal por parte de un criminal.	• Criminal Computacional. • Terroristas.	No se dispone de controles para este tipo de amenaza.	Alto
Personal que no cumpla las políticas de seguridad.	• Hacker, cracker. • Criminal Computacional. • Personal Malintencionado. • Espía.	Se cuenta con políticas de seguridad de la información y sanciones en caso de incumplirlas.	Medio

Tabla 2-16. Probabilidad de ocurrencia de amenazas humanas

2.3.5.2 Análisis de la probabilidad de ocurrencia de amenazas naturales

Vulnerabilidad	Amenaza	Control	Probabilidad
Ecuador se ubica en una zona de intensa actividad sísmica y volcánica.	Terremoto Temblores Erupción Volcánica Tsunami.	La distribución de los recintos electorales se lo realiza considerando las zonas de alto bajo riesgo. También se cuenta con planes de recuperación de desastres.	Bajo
Deforestación del territorio, sobrepastoreo, erosión inducida, minería desorganizada.	Deslaves y hundimiento de tierras Inundación.	La distribución de los recintos electorales se lo realiza considerando las zonas de alto bajo riesgo. También se cuenta con planes de recuperación de desastres.	Medio
Ubicación de Ecuador en la zona ecuatorial. Esta zona presenta la mayor actividad de tormentas eléctricas.	Tormentas Eléctricas.	La distribución de los recintos electorales se lo realiza considerando las zonas de alto bajo riesgo. También se cuenta con planes de recuperación de desastres.	Bajo

Tabla 2-17. Probabilidad de ocurrencia de amenazas naturales

2.3.5.3 Análisis de la probabilidad de ocurrencia de amenazas ambientales

Vulnerabilidad	Amenaza	Control	Probabilidad
Infraestructura de recintos electorales en mal estado.	Fuga de agua masiva.	La distribución de los recintos electorales se lo realiza de manera técnica. Considerando los factores de riesgo y accesibilidad a los recintos electorales.	Baja
Pérdida de energía eléctrica en los sistemas de distribución.	Corte de energía a largo plazo.	Una planta eléctrica alimentará la infraestructura tecnológica en caso de corte de energía. Y las estadísticas de pérdida de energía en los sistemas de distribución es 12% en el 2014. [34]	Baja
Estado de los oleoductos para transporte de petróleo.	Derrame de químicos.	La distribución de los recintos electorales se lo realiza de manera técnica. Considerando los factores de riesgo y accesibilidad a los recintos electorales.	Baja

Tabla 2-18. Probabilidad de ocurrencia de amenazas naturales

2.3.6 ANÁLISIS DEL IMPACTO

El análisis del impacto consiste en estimar la magnitud del daño cuando una amenaza explota una vulnerabilidad.

El análisis del impacto se evaluará de acuerdo a los criterios de: Pérdida de Integridad, Pérdida de Disponibilidad, y Pérdida de Confidencialidad. Para esto, se emplea una escala cualitativa la cual se muestra en la tabla 2-19.

Grado	Definición
Alto	Cuando se compromete las tres características de la seguridad de la información.
Medio	Cuando se compromete las dos características de la seguridad de la información.
Bajo	Cuando se compromete una características de la seguridad de la información.

Tabla 2-19. Definiciones del Impacto.

El análisis del impacto será divido de acuerdo al tipo de fuente de la amenaza, estos son:

- Humanas.
- Naturales.
- Ambientales.

2.3.6.1 Análisis del impacto de amenazas humanas

Vulnerabilidad	Amenaza	Pérdida de Integridad	Pérdida de Disponibilidad	Pérdida de Confidencialidad	Impacto
Personal que acepte sobornos.	Criminal Computacional Espías Personal malintencionado.	X	X	X	Alto
Personal sin capacitación técnica.	Personal Negligente.	X	X	X	Alto
Desconocimiento del personal sobre las actividades a realizar en caso de emergencias.	Personal Negligente.	X		X	Medio
Personal no ha recibido capacitación sobre ataques a través de ingeniería social.	Hacker, cracker Criminal Computacional.	X		X	Medio

Curiosidad.	Personal Negligente y Malintencionado.	X	X	X	Alto
Chantaje y amenazas al personal por parte de un criminal.	Criminal Computacional, Terroristas.	X	X	X	Alto
Personal que no cumpla las políticas de seguridad.	Hacker, cracker Criminal Computacional Personal Malintencionado Espía.	X		X	Medio

Tabla 2-20. Impacto de la ocurrencia de amenazas humanas

2.3.6.2 Análisis del impacto de amenazas naturales

Vulnerabilidad	Amenaza	Pérdida de Integridad	Pérdida de Disponibilidad	Pérdida de Confidencialidad	Impacto
Ecuador se ubica en una zona de intensa actividad sísmica y volcánica.	Terremoto Temblores Erupción Volcánica Tsunami.	X	X		Medio
Deforestación del territorio, sobrepastoreo, erosión inducida, minería desorganizada.	Deslaves y hundimiento de tierras Inundación.	X	X		Medio
Ubicación de Ecuador en la zona ecuatorial. Esta zona presenta la mayor actividad de tormentas eléctricas.	Tormentas Eléctricas.	X	X		Medio

Tabla 2-21. Impacto de la ocurrencia de amenazas naturales

2.3.6.3 Análisis del impacto de amenazas ambientales

Vulnerabilidad	Amenaza	Pérdida de Integridad	Pérdida de Disponibilidad	Pérdida de Confidencialidad	Impacto
Infraestructura de recintos electorales en mal estado.	Fuga de agua masiva.		X		Bajo
Pérdida de energía eléctrica en los sistemas de distribución.	Corte de energía a largo plazo.	X	X		Medio
Estado de los oleoductos para transporte de petróleo.	Derrame de químicos.		X		Bajo

Tabla 2-22. Impacto de la ocurrencia de amenazas ambiental

2.3.7 ANÁLISIS DEL RIESGO

El propósito del análisis del riesgo es valorar el nivel de riesgo de la infraestructura tecnológica para votación digital. Para la determinación de este nivel de riesgo se considera los resultados del análisis de probabilidad e impacto de que una amenaza explote una vulnerabilidad.

Con el fin de establecer una escala cuantitativa del riesgo, se usará la matriz del nivel de riesgo.

Probabilidad de la Amenaza	Impacto Bajo 10	Impacto Medio 50	Impacto Alto 100
Alto 1.0	1.0 x 10 = 10	1.0 x 50 = 50	1.0 x 100 = 100
Medio 0.5	0.5 x 10 = 5	0.5 x 50 = 25	0.5 x 100 = 50
Bajo 0.1	0.1 x 10 = 1	0.1 x 50 = 5	0.1 x 100 = 10

Tabla 2-23. Matriz de Niveles de Riesgo. Fuente: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

2.3.7.1 Niveles de Riesgo

De la tabla 2-24 obtenemos los niveles de riesgo y sus valores. Estos números son el resultado de la multiplicación entre la probabilidad y el impacto de que una amenaza explote una vulnerabilidad tenemos los siguientes niveles de riesgos.

Nivel	Rango de valores
Riesgo Bajo	1 - 5
Riesgo Medio	10 - 25
Riesgo Alto	50 - 100

Tabla 2-24. Niveles de riesgo y sus valores

Los niveles de riesgo representan el grado de riesgo al que un sistema informático está expuesto si una vulnerabilidad dada fuera ejercida. En la tabla 2.25 se muestra los niveles de riesgos y las acciones a tomar por cada nivel.

Nivel de Riesgo	Descripción del Nivel de Riesgo y medidas a tomar
Alto	Si una observación se evalúa como de alto riesgo, hay una fuerte necesidad de medidas correctivas. Un sistema existente puede seguir funcionando, pero un plan de acción correctiva debe ser puesto en marcha tan pronto como sea posible.
Medio	Si una observación tiene como riesgo medio, se necesitan acciones correctivas y un plan debe ser desarrollado para incorporar estas acciones en un plazo razonable de tiempo.
Bajo	Si una observación es evaluada como de bajo riesgo, la organización debe determinar si aún se requieren acciones correctivas o si deciden aceptar el riesgo.

Tabla 2-25. Niveles de riesgo y Acciones necesarias. Fuente: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

El análisis el análisis de riesgo de la infraestructura tecnológica para votación digital será divido de acuerdo al tipo de fuente de la amenaza, estos son:

- Humanas.
- Naturales.
- Ambientales.

2.3.7.2 Valoración de riesgo de amenazas humanas

Vulnerabilidad	Acción de la amenaza	Probabilidad	Probabilidad Ponderado	Impacto	Impacto Ponderado	Riesgo
Personal que acepte sobornos	Criminal Computacional Espías Personal malintencionado	Alto	1.0	Alto	100	100
Personal sin capacitación técnica	Personal Negligente	Bajo	0.1	Alto	100	10
Desconocimiento del personal sobre las actividades a realizar en caso de emergencias	Personal Negligente	Bajo	0.1	Medio	10	1
Personal no ha recibido capacitación sobre ataques a través de ingeniería social	Hacker, cracker Criminal Computacional	Bajo	0.1	Medio	50	5
Curiosidad	Personal Negligente y	Medio	0.5	Alto	100	50

	Malintencionado					
Chantaje y amenazas al personal por parte de un criminal	Criminal Computacional, Terroristas	Alto	1.0	Alto	100	100
Personal que no cumpla las políticas de seguridad	Hacker, cracker Criminal Computacional Personal Malintencionado Espía	Medio	0.5	Medio	50	25

Tabla 2-26. Valoración de riesgo de amenazas humanas

2.3.7.3 Valoración de riesgo de amenazas naturales

Vulnerabilidad	Acción de la amenaza	Probabilidad	Probabilidad Ponderado	Impacto	Impacto Ponderado	Riesgo
Ecuador se ubica en una zona de intensa actividad sísmica y volcánica.	Terremoto Temblores Erupción Volcánica Tsunami.	Bajo	0.1	Medio	50	5
Deforestación del territorio, sobrepastoreo, erosión inducida, minería desorganizada.	Deslaves y hundimiento de tierras Inundación.	Medio	0.5	Medio	50	25
Ubicación de Ecuador en la zona ecuatorial. Esta zona presenta la mayor actividad de tormentas eléctricas.	Tormentas Eléctricas.	Bajo	0.1	Medio	50	5

Tabla 2-27. Valoración de riesgo de amenazas naturales

2.3.7.4 Valoración de riesgo de amenazas ambientales

Vulnerabilidad	Acción de la amenaza	Probabilidad	Probabilidad Ponderado	Impacto	Impacto Ponderado	Riesgo
Infraestructura de recintos electorales en mal estado.	Fuga de agua masiva.	Baja	0.1	Bajo	10	1
Pérdida de energía eléctrica en los sistemas de distribución.	Corte de energía a largo plazo.	Baja	0,1	Medio	50	5
Estado de los oleoductos para transporte de petróleo.	Derrame de químicos.	Baja	0.1	Bajo	10	1

Tabla 2-28. Valoración de riesgo de amenazas ambientales

2.3.7.5 Análisis de Riesgos

Los resultados del análisis de riesgos indican que cuando la amenaza es de tipo humana, el riesgo de que una vulnerabilidad sea ejercida es muy alto.

Las parejas vulnerabilidad/amenaza que representan riesgo alto son:

Vulnerabilidad	Acción de la amenaza	Riesgo
Personal que acepte sobornos.	Criminal Computacional. Espías. Personal malintencionado.	100
Chantaje y amenazas al personal por parte de un criminal.	Criminal Computacional, Terroristas.	100
Curiosidad.	Personal Negligente y Malintencionado.	50

Tabla 2-29. Parejas vulnerabilidad/amenaza con riesgo alto

Los datos de la tabla 2-29 indican que:

- Una persona amenazada gravemente o alguien que recibe sobornos pueden realizar acciones que comprometen la seguridad de la información.
- Personal sin el suficiente conocimiento técnico puede ocasionar graves problemas de seguridad motivado por curiosidad.

Las parejas vulnerabilidad/amenaza que representan riesgo medio son:

Vulnerabilidad	Acción de la amenaza	Riesgo
Personal que no cumpla las políticas de seguridad	Hacker, cracker Criminal Computacional Personal Malintencionado Espía	25
Deforestación del territorio, sobrepastoreo, erosión inducida, minería desorganizada	Deslaves y hundimiento de tierras Inundación	25
Personal sin capacitación técnica	Personal Negligente	10

Tabla 2-30. Parejas vulnerabilidad/amenaza con riesgo medio

Los datos de la tabla 2-30 indican que:

- El incumplimiento de políticas de seguridad sin sanción puede ocasionar que el personal no siga las políticas de seguridad establecidas. Esto provoca que personas malintencionadas aprovechen para penetrar el sistema y hacer daño.
- Recintos electorales ubicados en zonas de riesgo de deslaves, hundimiento de tierra e inundaciones constituye peligro para la realización del proceso electoral con normalidad y también atenta contra la vida de las personas.
- Personal sin una capacitación técnica puede cometer acciones inintencionadas que comprometan la integridad, confidencialidad y disponibilidad de la información.

2.3.8 RECOMENDACIONES DE CONTROL

Se recomienda tener en consideración los siguientes puntos:

- Personas que manejen o tengan acceso a información confidencial deben contar con seguridad privada. El CNE debe realizar un análisis costo-beneficio de implementar esta medida.
- Las personas contratadas no solo deben tener conocimiento técnico, también deben ser personas honestas y confiables. Por lo tanto se recomienda establecer procesos y estrategias de selección y separación de personal.
- Se debe sancionar el incumplimiento de las políticas de seguridad. Si la gravedad de la infracción lo amerita, la sanción debe incluir prisión. Para esto es necesario apoyarse en las leyes de la República.
- Se debe trabajar en conjunto con los organismos de socorro como bomberos, cruz roja, entre otros para brindar respuesta inmediata en el caso de producirse una amenaza natural o ambiental.
- Los recursos de la infraestructura tecnológica de votación digital deben ser asegurados.

CAPÍTULO III

3 DISEÑO

En este capítulo se presentará el diseño de la infraestructura tecnológica propuesta para el proceso de votación digital. Los requerimientos fueron analizados en el capítulo II. En la sección 3.1 se presentará el diseño de red de la infraestructura tecnológica. El diseño estará compuesto los módulos: Core, Datacenter, Conectividad a Internet y Acceso Remoto. En la sección 3.2 se presentará el diseño del software. Este está compuesto a la vez por el diseño de datos, diseño arquitectónico y diseño a nivel de componentes. Finalmente en la sección 3.3 se presentará el diseño de seguridad. Este diseño se compondrá por los esquemas criptográficos de Firmas Ciegas y Redes de Mezcla o Mix. El esquema de Firmas Ciegas se empleará para la fase de Autenticación del voto y el esquema de Redes de Mezcla se empleará para la fase de Anonimato previo al conteo de votos.

3.1 DISEÑO DE LA INFRAESTRUCTURA TECNOLÓGICA

El diseño de la infraestructura tecnológica se basará en el enfoque modular de Cisco para construcción de redes escalables. [35] [36] [37] [38] La infraestructura tecnológica estará diseñada en módulos considerando los requerimientos de red y seguridad especificados en las secciones 2.2.2 y 2.2.3 respectivamente.

3.1.1 MÓDULOS DE LA RED DE VOTACIÓN

El diseño estará compuesto por cuatro módulos que cumplen roles específicos dentro de la red.

- Módulo Core, su función es enrutar y switchear el tráfico tan rápido como sea posible.
- Módulo Datacenter, su función es alojar las aplicaciones y datos del sufragio en servidores de base de datos y aplicaciones.

- Módulo de Conectividad a Internet, su función es proveer la conexión entre el Campus Empresarial y Acceso Remoto.
- Módulo de Acceso Remoto, su función proveer acceso seguro a usuarios remotos a la red de votación. [39] [40] [41] [42]

3.1.2 ENRUTAMIENTO DE LA RED DE VOTACIÓN

La comunicación entre los módulos de la red se realizará con enrutamiento estático. El enrutamiento estático será utilizado porque las direcciones ip de los servidores y los dispositivos de comunicación de la red no pueden variar. La ventaja de este tipo de enrutamiento es que “el procesamiento del CPU es mínimo y su configuración es fácil en redes pequeñas”. **Fuente especificada no válida.**

En la figura 3-1 se presenta el diseño de red de votación propuesto para la infraestructura tecnológica y en la tabla 3-1 se muestra la tabla de enrutamiento de la red de votación.

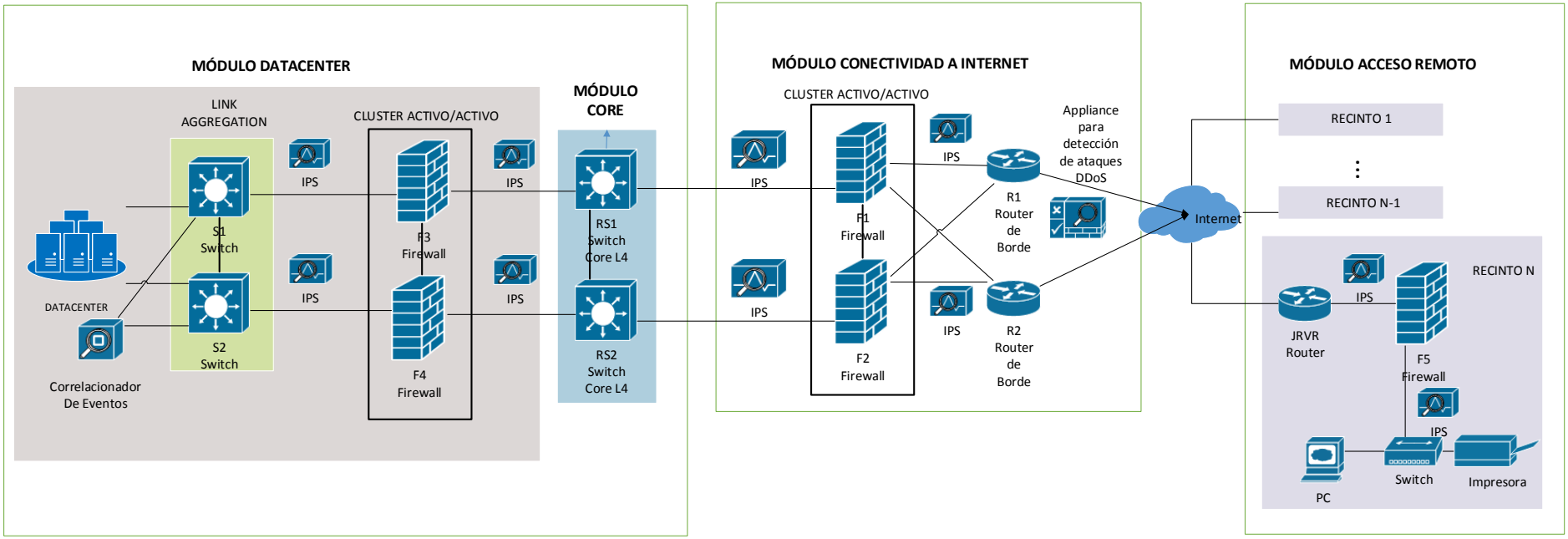


Figura 3-1. Arquitectura Modular propuesta para el Proceso de Votación Digital

No.	Dispositivo	Interfaz de red	Dirección IP	Mascara de subred	Gateway Predeterminado
1	R1	S0/0/0	Ip Pública	-	-
		S0/0/1	192.68.230.1	255.255.255.240	-
		S0/0/2	192.168.230.17	255.255.255.240	-
2	R2	S0/0/0	Ip Pública	-	-
		S0/0/1	192.168.230.33	255.255.255.240	-
		S0/0/2	192.168.230.49	255.255.255.240	-
3	RS1	S0/0/0	192.168.230.129	255.255.255.240	-
		S0/0/1	192.168.230.81	255.255.255.240	-
		S0/0/2	192.168.230.114	255.255.255.240	-
4	RS2	S0/0/0	192.168.230.161	255.255.255.240	-
		S0/0/1	192.168.230.82	255.255.255.240	-
		S0/0/2	192.168.230.146	255.255.255.240	-
5	F1	S0/0/0	192.68.230.113	255.255.255.240	-
		S0/0/1	192.68.230.65	255.255.255.240	-
		S0/0/2	192.68.230.2	255.255.255.240	-
6	F2	S0/0/0	192.68.230.66	255.255.255.240	-
		S0/0/1	192.68.230.18	255.255.255.240	-
		S0/0/2	192.68.230.145	255.255.255.240	-
7	F3	F0/1	192.68.230.177	255.255.255.240	-
		S0/0/1	192.68.230.97	255.255.255.240	-
		S0/0/2	192.68.230.130	255.255.255.240	-
8	F4	F0/1	192.68.230.193	255.255.255.240	-
		S0/0/1	192.68.230.98	255.255.255.240	-
		S0/0/2	192.68.230.162	255.255.255.240	-
9	Correlacionador	FastEthernet1	192.68.230.178	255.255.255.240	192.68.230.177
		FastEthernet2	192.68.230.178	255.255.255.240	192.68.230.193
10	Servidor JRV	FastEthernet1	192.68.230.179	255.255.255.240	192.68.230.177
		FastEthernet2	192.68.230.179	255.255.255.240	192.68.230.193
11	Servidor de Firma del Voto	FastEthernet1	192.68.230.180	255.255.255.240	192.68.230.177
		FastEthernet2	192.68.230.180	255.255.255.240	192.68.230.193
12	Servidor de Validación de la Firma del Voto	FastEthernet1	192.68.230.181	255.255.255.240	192.68.230.177
		FastEthernet2	192.68.230.181	255.255.255.240	192.68.230.193
13	Servidores Mix 1	FastEthernet1	192.68.230.182	255.255.255.240	192.68.230.177
		FastEthernet2	192.68.230.182	255.255.255.240	192.68.230.193
14	Servidores Mix 2	FastEthernet1	192.68.230.183	255.255.255.240	192.68.230.177
		FastEthernet2	192.68.230.183	255.255.255.240	192.68.230.193
15	Servidores de Conteo	FastEthernet1	192.68.230.184	255.255.255.240	192.68.230.177
		FastEthernet2	192.68.230.184	255.255.255.240	192.68.230.193
16	Servidor de Resultados	FastEthernet1	192.68.230.185	255.255.255.240	192.68.230.177
		FastEthernet2	192.68.230.185	255.255.255.240	192.68.230.193
17	Servidor Padrón	FastEthernet1	192.68.230.186	255.255.255.240	192.68.230.177

	Electoral	FastEthernet2	192.68.230.186	255.255.255.240	192.68.230.193
18	Servidor de Base de datos de la Papeleta Digital	FastEthernet1	192.68.230.187	255.255.255.240	192.68.230.177
		FastEthernet2	192.68.230.187	255.255.255.240	192.68.230.193
19	Servidor de Base de datos Voto	FastEthernet1	192.68.230.188	255.255.255.240	192.68.230.177
		FastEthernet2	192.68.230.188	255.255.255.240	192.68.230.193
20	Servidor de Base de datos Resultados	FastEthernet1	192.68.230.190	255.255.255.240	192.68.230.177
		FastEthernet2	192.68.230.190	255.255.255.240	192.68.230.193

Tabla 3-1. Tabla de Enrutamiento Estático

3.1.3 DESCRIPCIÓN DE LOS COMPONENTES DE LA RED

Los requerimientos de la red de votación y los requerimientos de seguridad descritos en la sección 2.2.2 y 2.2.3 son los siguientes:

- Transmitir los datos garantizando su integridad, confidencialidad y disponibilidad.
- Diseñar la red con norma Ethernet a 1000 Mbps.
- La red debe soportar la conexión de 41806 personas.
- El ancho de banda debe ser de 72,41 mps.
- Los dispositivos de red, servidores y los enlaces deben ser redundantes.
- El voto debe ser directo, es decir cada votante elige a sus gobernantes directamente, sin ninguna intermediación por parte de otra persona u órgano colegiado que no sea el CNE.
- El voto debe ser secreto, es un respaldo del sistema electoral con el fin de imposibilitar que otra persona pueda influir en la decisión de voto de un elector.
- Los canales de comunicación deben ser seguros.
- La información a ser enviada debe ser cifrada.
- Únicamente terminales autorizadas pueden enviar votos.

Para cumplir con estos requerimientos, la red se compone de los siguientes dispositivos:

- Appliance para detección de ataques DDoS.
- IPS.
- Antivirus.
- HIPS.
- Correlacionador de Eventos.
- WAF.
- Firewall de Base de Datos.

La función de cada dispositivo se presenta a continuación.

3.1.3.1 Appliance para detección de ataques DDoS

Este dispositivo se ubica antes de los routers fronterizos llamas R1 y R2 en la figura 3-1. Sus funciones son monitorear las aplicaciones y el tráfico de la red, detectar y bloquear usuarios maliciosos y detectar y bloquear solicitudes de acceso maliciosas.

3.1.3.2 IPS

Es un dispositivo que ejerce el control de acceso en una red informática. El IPS establece políticas de seguridad para determinar que terminales pueden tener comunicación con determinadas redes. El IPS reconoce el tráfico fuera del perfil permitido y lo descarta. El IPS es capaz de enviar alarmas en caso de detectar/bloquear tráfico malicioso.

3.1.3.3 Antivirus

El software antivirus es un programa de computación que detecta, previene y toma medidas para desarmar o eliminar programas de software malintencionados o malware, como virus y gusanos.
El software antivirus analiza archivos en busca de patrones que puedan indicar una infección por malware. Los patrones que busca se basan en firmas o definiciones de virus conocidos.

Los antivirus monitorean las actividades de virus en tiempo real y hacen verificaciones periódicas. La periodicidad de las verificaciones tienen que ser configuradas.

3.1.3.4 HIPS[15]

HIPS es un software que monitorea un solo servidor para identificar actividades sospechosas dentro del servidor. El HIPS detecta las actividades sospechosas por medio de políticas y reglas previamente establecidas. “La protección va desde la capa de red hasta la capa de aplicación” **Fuente especificada no válida.**. Estas políticas y reglas pueden ser configuradas para responder de dos maneras, una solo escribiendo en un log y la otra bloquear la actividad sospechosa.

El HISP analiza las llamadas al Sistema, los logs de las aplicaciones y modificaciones al file-system, y modificaciones a las regiones de la memoria.

HIPS escanea los atributos de cada objeto del software y crea un checksum de comprobación. Esta información se almacena en una base de datos segura para su posterior comparación. Si un programa intenta llevar una actividad no permitida, esta actividad es bloqueada y se registra una alerta,

3.1.3.5 Correlacionador de Eventos

Este dispositivo recoge las alarmas disparadas de todos los dispositivos de la red y correlaciona estos datos para determinar el tipo de ataque trata de ejecutarse. El correlacionador de eventos manda a ejecutar ACLs que tiene definidas en función del tipo de ataque detectado.

[15] Host Intrusion Prevention System

3.1.3.6 WAF[16]

El WAF es un software que analiza el tráfico web y protege al servidor de aplicaciones de ataques SQL Injection, Cross Site Scripting. El WAF se sitúa de manera lógica entre el software de votación y el terminal del cliente. La configuración del WAF se basa en establecer reglas para analizar peticiones al software de votación que pueden ser maliciosas. El WAF deniega por defecto todas las transacciones y solo acepta las que considera seguras. En la configuración del WAF se tiene que indicar el servidor al que enviar el tráfico.

Los ataques que bloquea el WAF son:

- Analiza las variables que llegan por GET o POST, detectando así un buffer overflow.
- Analizar que los valores pasados por GET o POST no contengan valores usados por Cross Site Scripting o SQL Injection como “select from”, “unión”, “concat”, etc.
- Monitorizan las respuestas del servidor web. Si detecta cadenas que identifica como cédula del votante o el voto deniega la respuesta al considerar que se trata de un ataque.

3.1.3.7 Firewall de Base de Datos

El firewall de bases de datos se coloca entre la aplicación web y el gestor de bases de datos. El firewall de bases de datos filtra mediante un conjunto de reglas preestablecidas, las peticiones que llegan al gestor de bases de datos. Así el firewall solo permitirá el paso a los usuarios y sentencias SQL autorizadas con anterioridad.

Un firewall de base de datos también puede llevar a cabo el monitoreo de las actividades, generación de bitácoras para identificar de qué lugar provienen los atacantes y el tipo de ataques más frecuentes. De esta manera se generan

[16] Web Application Firewall

estadísticas sobre comportamiento de los atacantes para tomar las medidas de seguridad necesarias.

3.1.3.8 Conexión De Recintos Electorales Con La Red De Votación

La conexión entre un recinto electoral y la red de votación se realiza por medio de una VPN IPSEC. Este tipo de VPN se elige para garantizar que únicamente las terminales autorizadas puedan conectarse a la red de votación.

Para el establecimiento de la VPN IPSEC se requiere que en el firewall de cada recinto electoral y en el firewall de la red de votación del módulo de conectividad a internet (este firewall se representa como F1 y F2 en la figura 3.1) se encuentren abiertos los puertos UDP 500 y los números de protocolo IP 50 y 51 por las dos filtros de firewall de entrada y salida permitidas. El puerto UDP 500 debe abrirse para permitir el tráfico del protocolo ISAKMP[17] y se reenvíe el tráfico a través de los firewall. El número del protocolo IP 50 debe ser configurado para permitir el tráfico de Protocolo de Seguridad IPSec ESP[18]. Por último, el número de protocolo P ID 51 debe ser configurado para permitir el tráfico del protocolo AH[19].

El establecimiento de la VPN IPSEC inicia cuando el votante emite su voto a través del software de votación. Para esto primero se inicia la sesión en el cliente VPN IPSec.

Antes de iniciar el envío de la información, el protocolo IKE se realiza la función de gestión automática de claves como el establecimiento de las SAs[20] correspondientes. Es decir establece una conexión cifrada y autenticada entre dos

[17] Internet Security Association and Key Management Protocol
[18] Encapsulating Security Protocol
[19] Authentication Header
[20] Sistemas Autónomos

entidades, a través de la cual se negocian los parámetros necesarios para establecer una asociación de seguridad IPSec.

3.2 DISEÑO DEL SISTEMA DE VOTO DIGITAL

En este subcapítulo se desarrolla el diseño del software en base a los requerimientos de software en la sección 2.2.1. La fase del diseño de software se compone de 3 diseños, estos son: diseño de datos, diseño arquitectónico y diseño a nivel de componentes. **Fuente especificada no válida.**

3.2.1 DISEÑO DE DATOS

El diseño de datos se representa a través del diagrama Entidad-Relación. En este diagrama se aprecian las diferentes entidades necesarias para la implementación del software de votación.

El diseño de datos del software de votación está compuesto por 3 diagramas entidad-relación. Los 3 diagramas representan al Padrón Electoral, Papeleta Digital y Voto.

En la figura 3-2 se muestra el diagrama entidad-relación del Padrón Electoral.

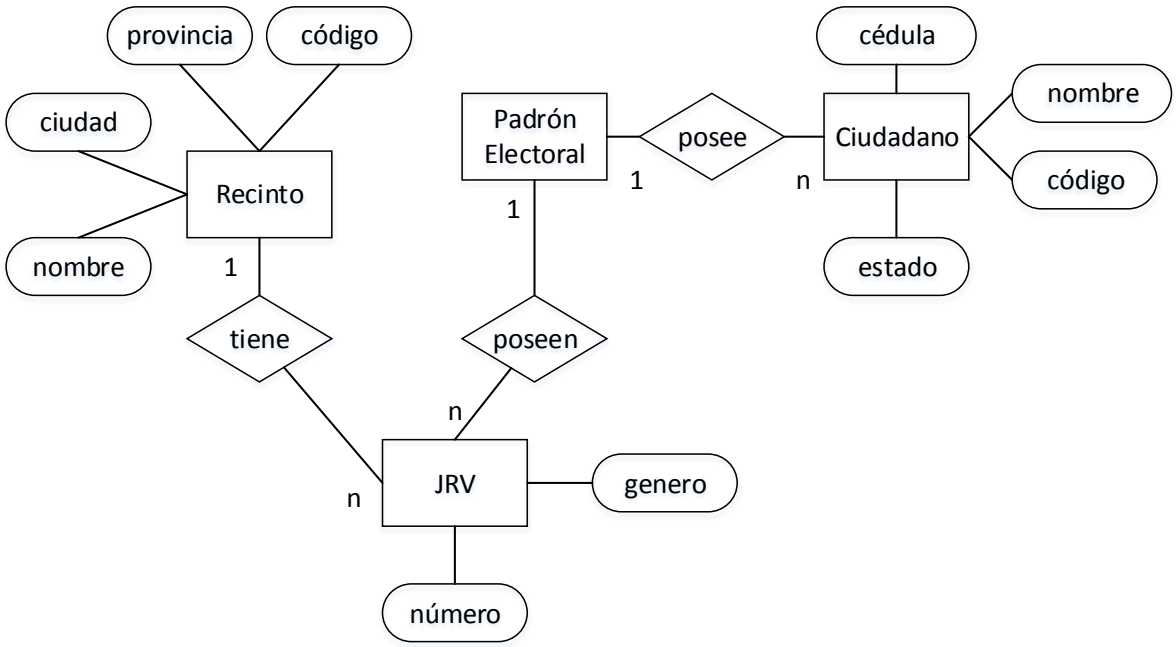


Figura 3-2. Diagrama Entidad Relación del Padrón Electoral.

En la figura 3-3 se muestra el diagrama entidad-relación de la Papeleta de Votación.

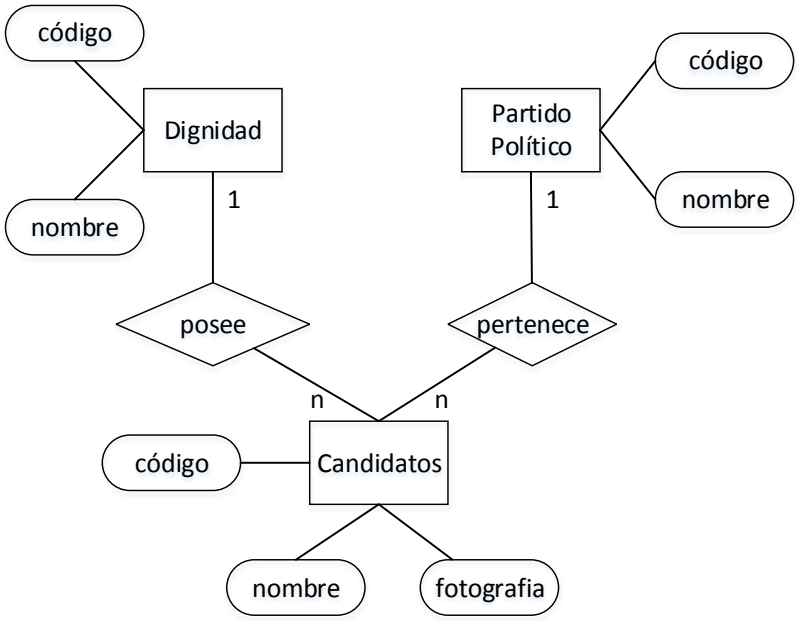


Figura 3-3. Diagrama Entidad Relación de la Papeleta de Votación

En la figura 3-4 se muestra el diagrama entidad-relación del Voto.

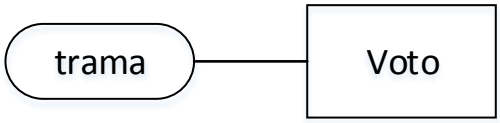


Figura 3-4. Diagrama Entidad Relación del Voto

3.2.2 DISEÑO ARQUITECTÓNICO

La arquitectura de software seleccionado para el software de votación es cliente servidor de 3 capas. Esta arquitectura es seleccionada por las siguientes razones:

- Debido a que el número de usuarios continuamente va creciendo, esta arquitectura permite aumentar la capacidad de procesamiento añadiendo nuevos servidores.
- El número de usuarios actualmente es 40763. Si se realiza cambios en el software no es necesario realizar cambios en los 40763 terminales clientes, basta con realizarlos en los servidores de aplicaciones.
- Protección de la base de datos. En esta arquitectura los usuarios no se conectan directamente a la base de datos.

La arquitectura cliente servidor de 3 capas modela la aplicación como un conjunto de servicios proporcionados por los servidores y un conjunto de clientes que usan estos servicios. Esta arquitectura se compone de 3 capas lógicas:

- Capa de presentación.
- Capa de procesamiento de la aplicación.
- Capa de gestión de datos.

Cada capa son procesos lógicamente separados que se ejecutan sobre servidores diferentes. En la tabla 3-2 se presenta las funciones de cada capa y el componente físico sobre el cual se ejecutan.

Capa	Funciones	Componente físico
Capa de presentación.	• Presenta la información al usuario y maneja toda la interacción con él. • Solicita los servicios de la capa de procesamiento de la aplicación.	Esta capa se ejecuta en la terminal del cliente a través de navegador web.
Capa de procesamiento de la aplicación	• Implementa la lógica del negocio. • Proporcionan los servicios que implementan la lógica del negocio a la capa de presentación. • Evita que el usuario tenga acceso directo a la base de datos.	Esta capa se ejecuta sobre el servidor de base de aplicaciones.
Capa de gestión de datos.	• Maneja todas las operaciones sobre la base de datos. • Proporciona al servidor de aplicaciones los datos que solicita.	Esta capa se ejecuta sobre el servidor de base de datos.

Tabla 3-2. Capas lógicas de la arquitectura cliente servidor de 3 capas

En la figura 3-5 se muestra el diseño arquitectónico del software de votación detallado en esta sección.

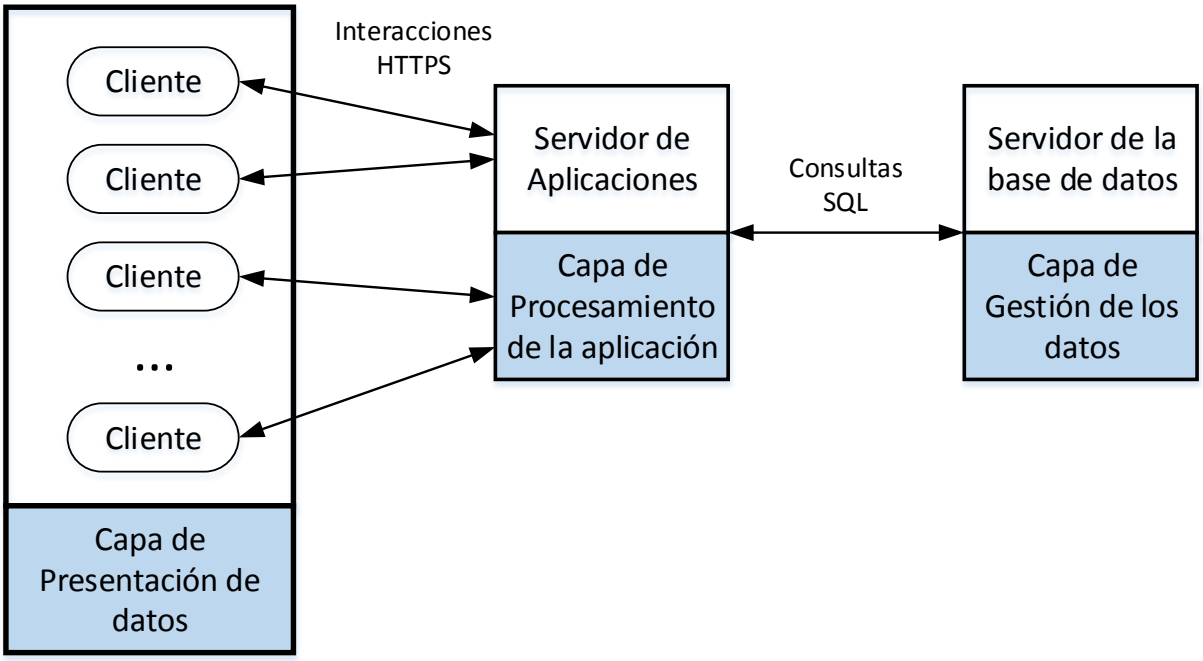


Figura 3-5. Diseño Arquitectónico del software de votación

La capa de Presentación de datos está conformada por los terminales clientes de cada JRV.

La capa de Procesamiento de la aplicación está conformada por los siguientes servidores de aplicaciones:

- Servidor de Aplicación JRV.
- Servidor de Aplicación de Firma del Voto.
- Servidor de Aplicación de Validación de la Firma del Voto.
- Servidores de Aplicaciones Mix.
- Servidor de Aplicación de Conteo.
- Servidor de Aplicaciones de Resultados.

La capa de Gestión de Datos está conformada por los siguientes servidores de base de datos:

- Servidor de Base de datos del Padrón Electoral.
- Servidor de Base de datos de la Papeleta Digital.

- Servidor de Base de datos Voto.

3.2.3 DISEÑO A NIVEL DE COMPONENTES

En esta sección se describe la interacción entre los componentes del diseño arquitectónico del software de votación para cada escenario identificado en las historias de usuario.

3.2.3.1 Módulo de Autenticación

3.2.3.1.1 Escenario principal JRV

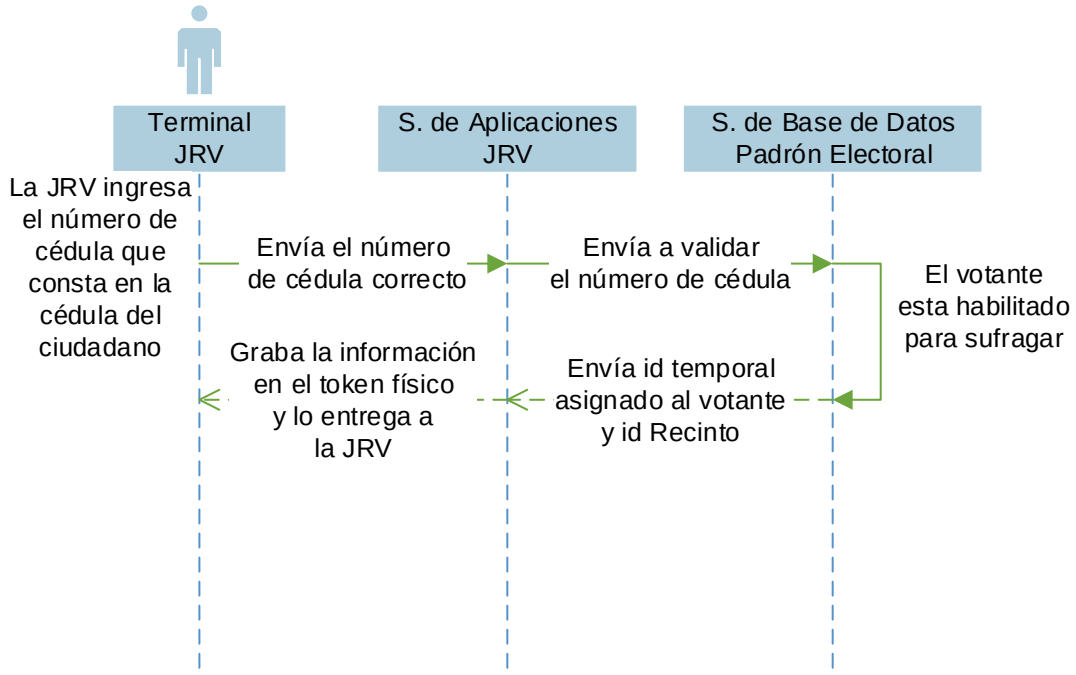


Figura 3-6. Autenticación. Escenario Principal JRV

3.2.3.1.2 Escenario Alterno 1: LA JRV ingresa el número de cédula incorrecta

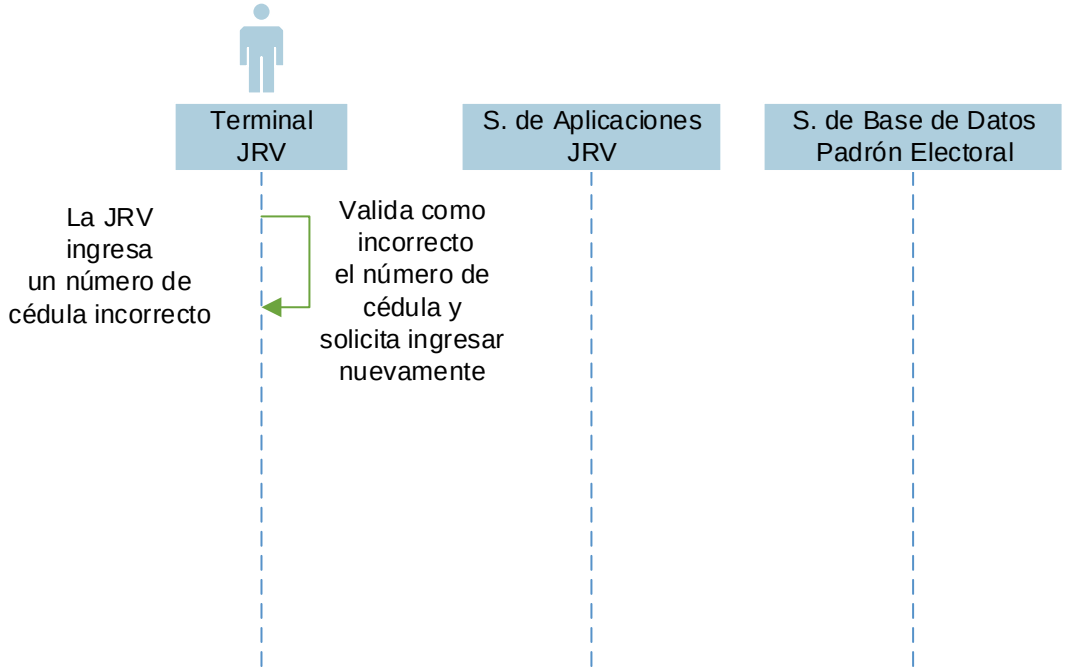


Figura 3-7. Autenticación. Escenario Alterno 1 de la JRV

3.2.3.1.3 Escenario Alterno 2: La JRV valida que el votante no se encuentra en el Padrón Electoral de la JRV

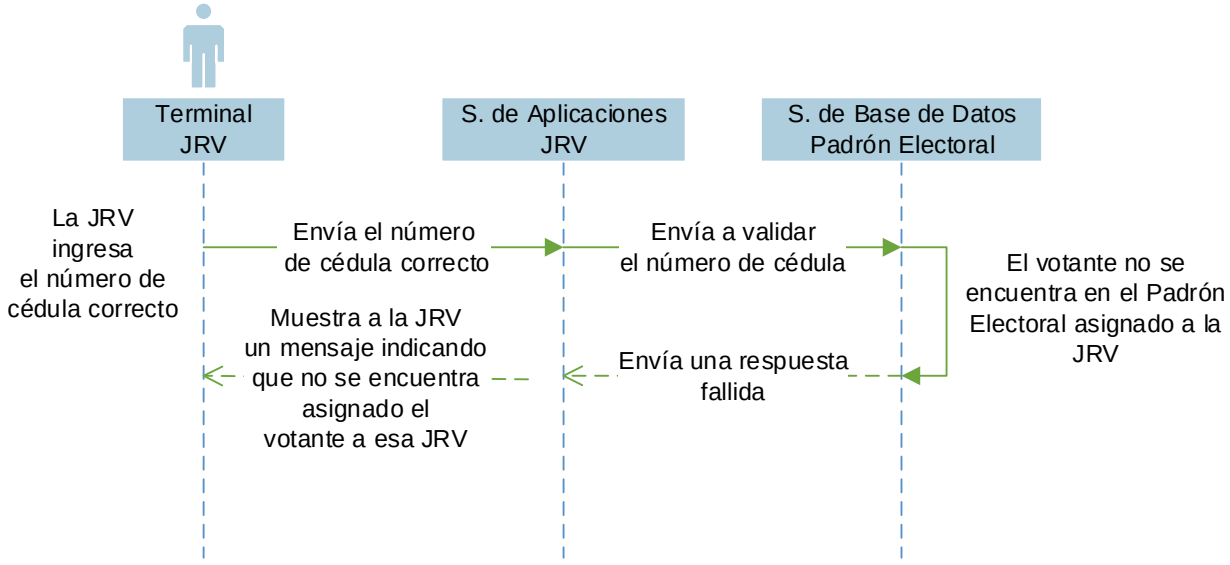


Figura 3-8. Autenticación. Escenario Alterno 2 de la JRV

3.2.3.1.4 Escenario Alterno 3: La JRV valida que el votante ya sufragó

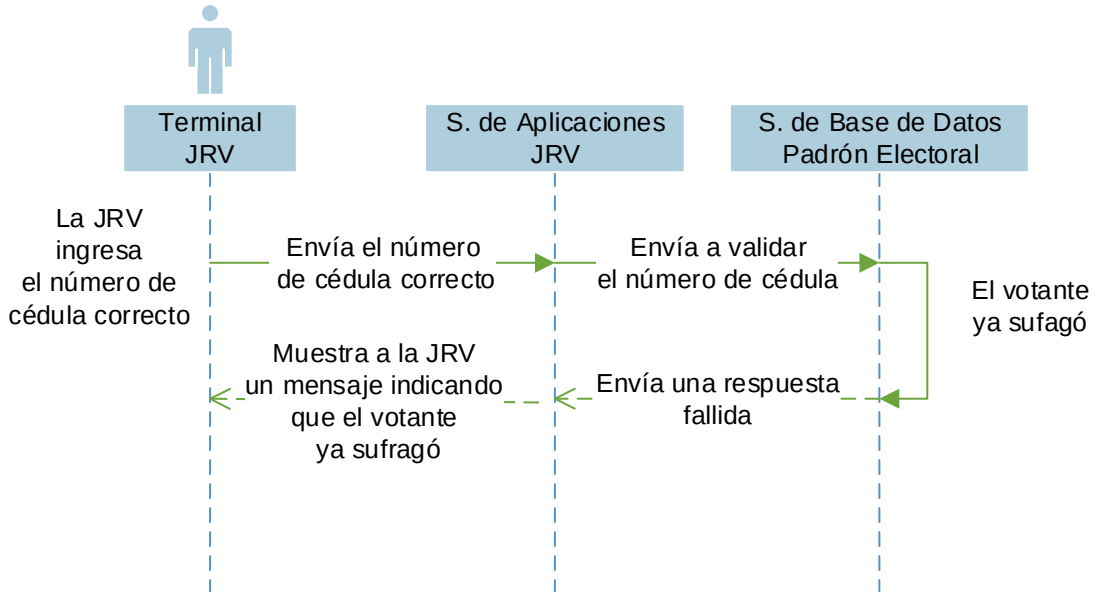


Figura 3-9. . Autenticación. Escenario Alterno 3 de la JRV

3.2.3.1.5 Escenario principal Votante

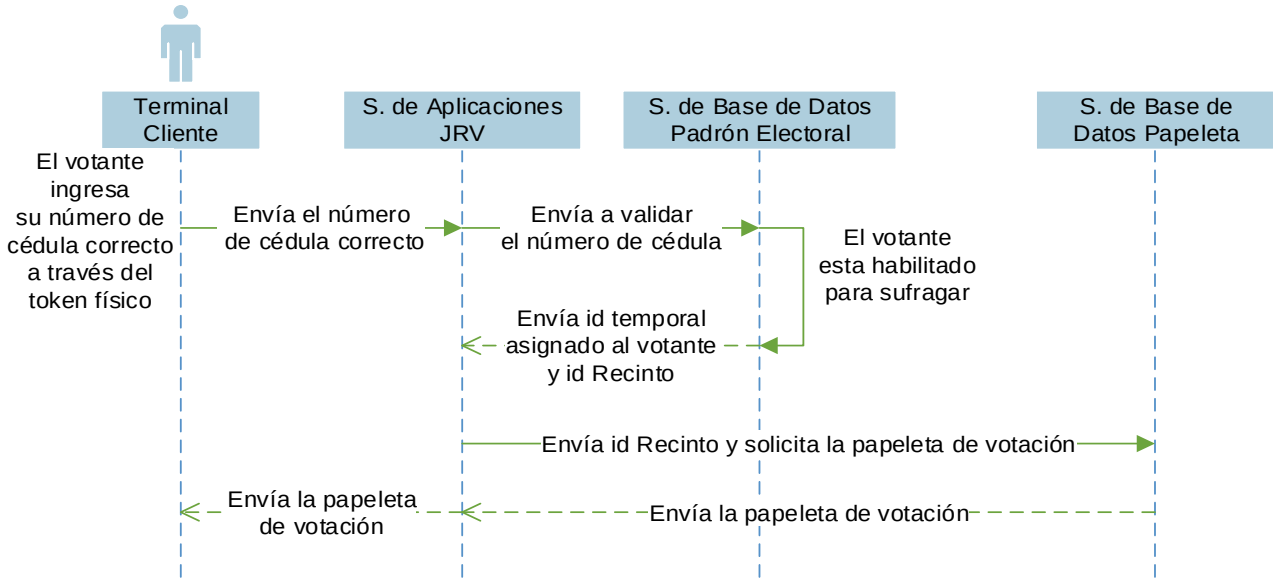


Figura 3-10. Autenticación. Escenario Principal del Votante

3.2.3.1.6 Escenario Alterno 1: El votante ingresa su número de cédula incorrecta

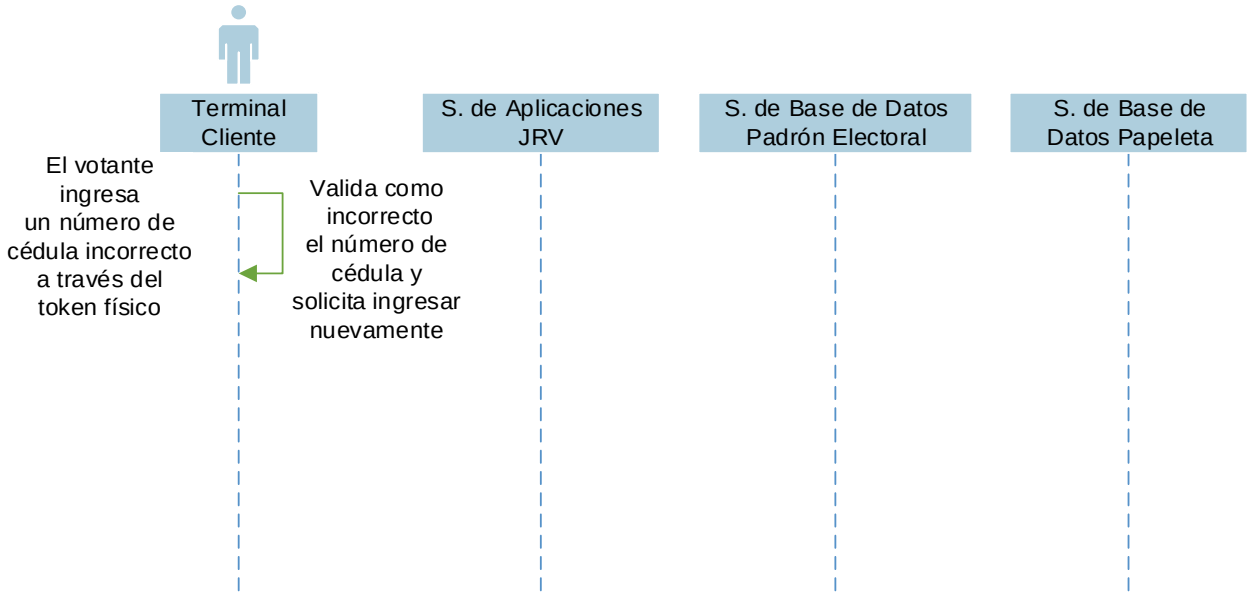


Figura 3-11. Autenticación. Escenario Alterno 1 del Votante

3.2.3.1.7 Escenario Alterno 2: El votante no se encuentra en el Padrón Electoral de la JRV

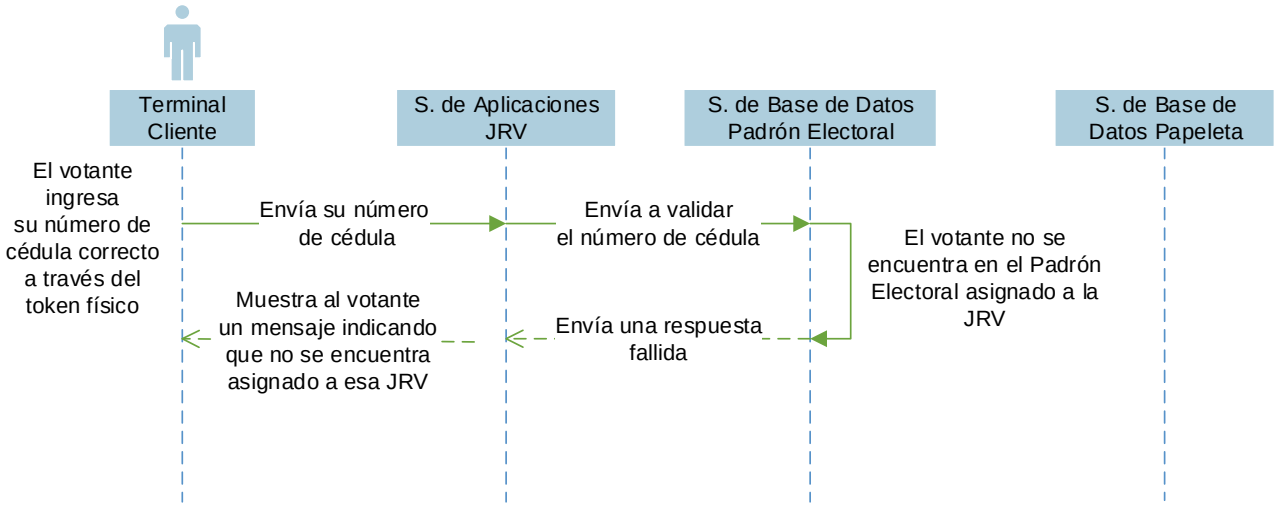


Figura 3-12. Autenticación. Escenario Alterno 2 del Votante

3.2.3.1.8 Escenario Alterno 3: El votante ya sufragó

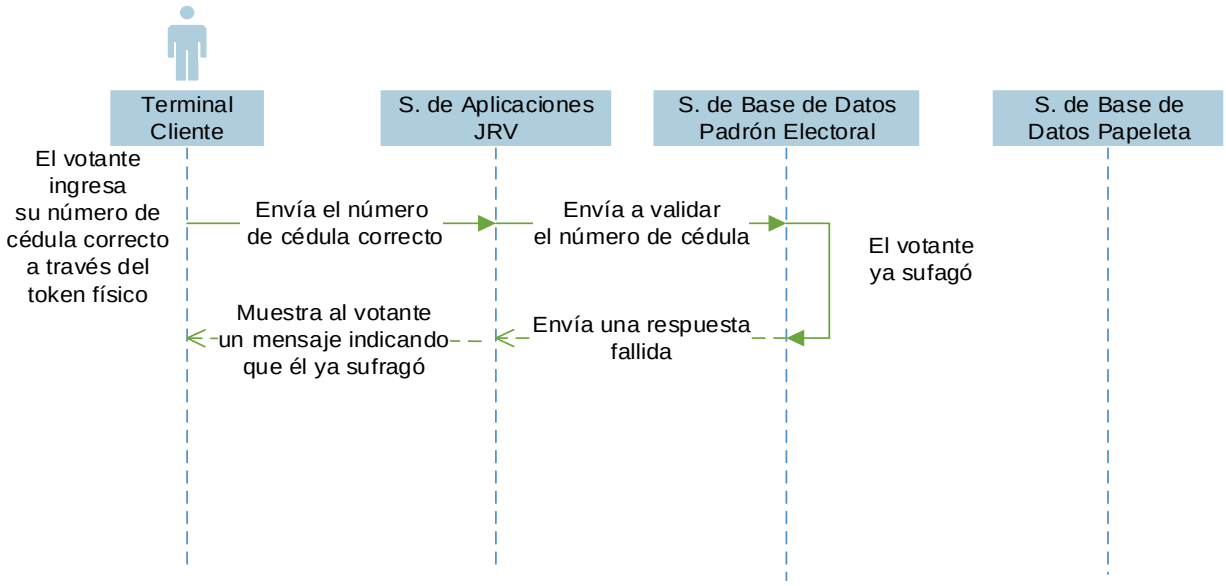


Figura 3-13. . Autenticación. Escenario Alterno 3 del Votante

3.2.3.2 Módulo de Votación

3.2.3.2.1 Escenario Principal

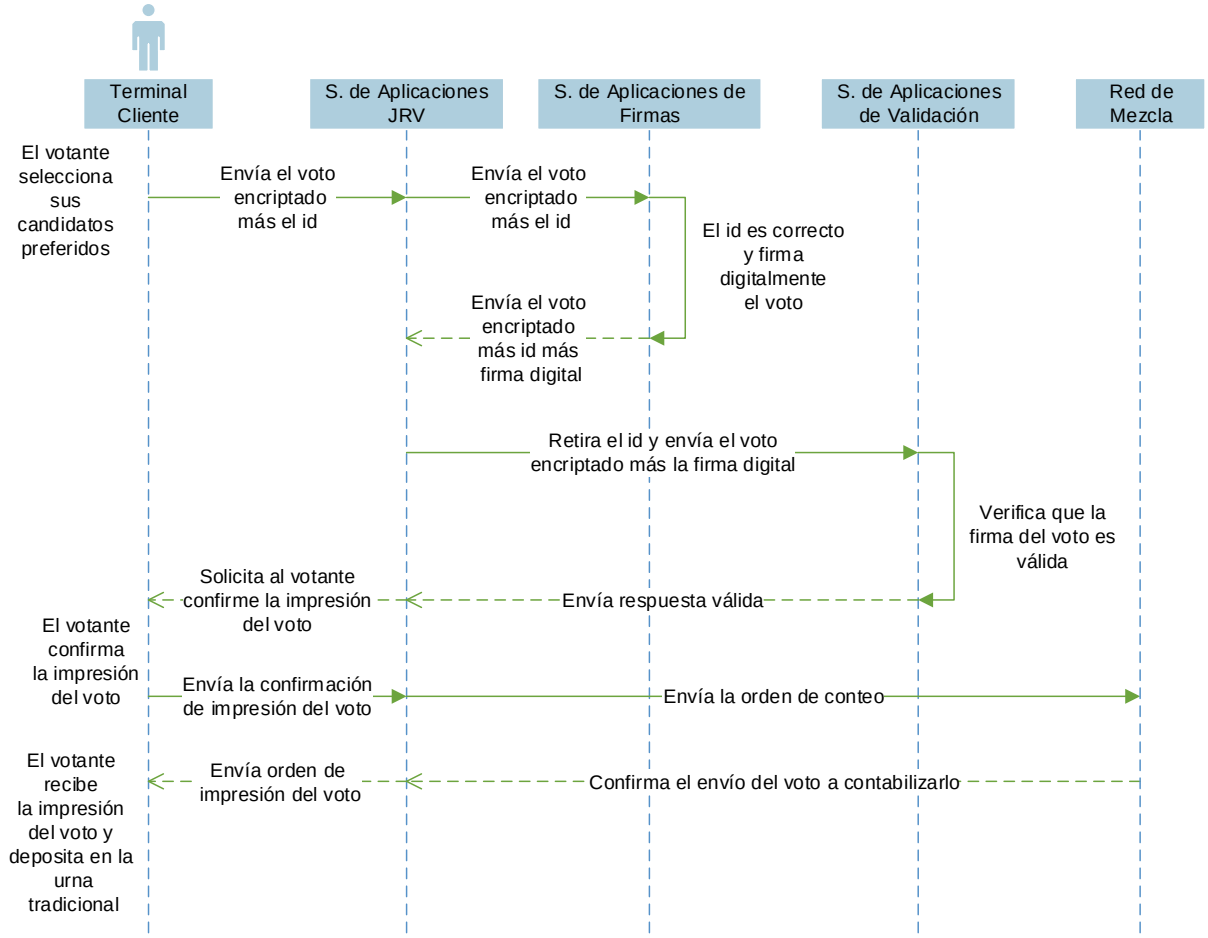


Figura 3-14. Votación. Escenario Principal

El voto en blanco y el voto nulo serán presentados en la papeleta como otras opciones que pueden ser seleccionadas.

3.2.3.2.2 Escenario Alterno 1: El votante envía un voto en blanco

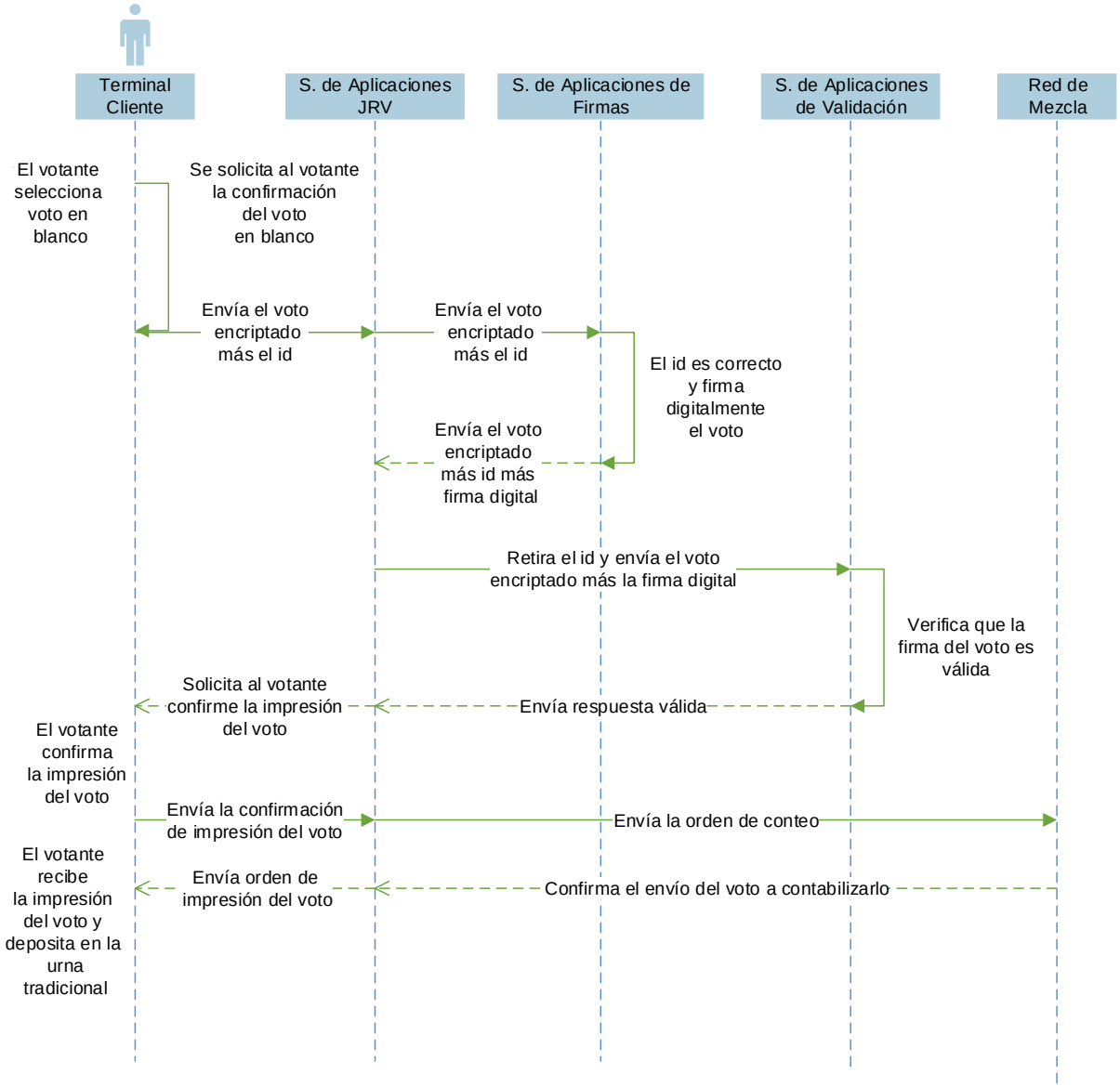


Figura 3-15. Votación. Escenario Alterno 1

3.2.3.2.3 Escenario Alterno 2: El votante envía un voto nulo

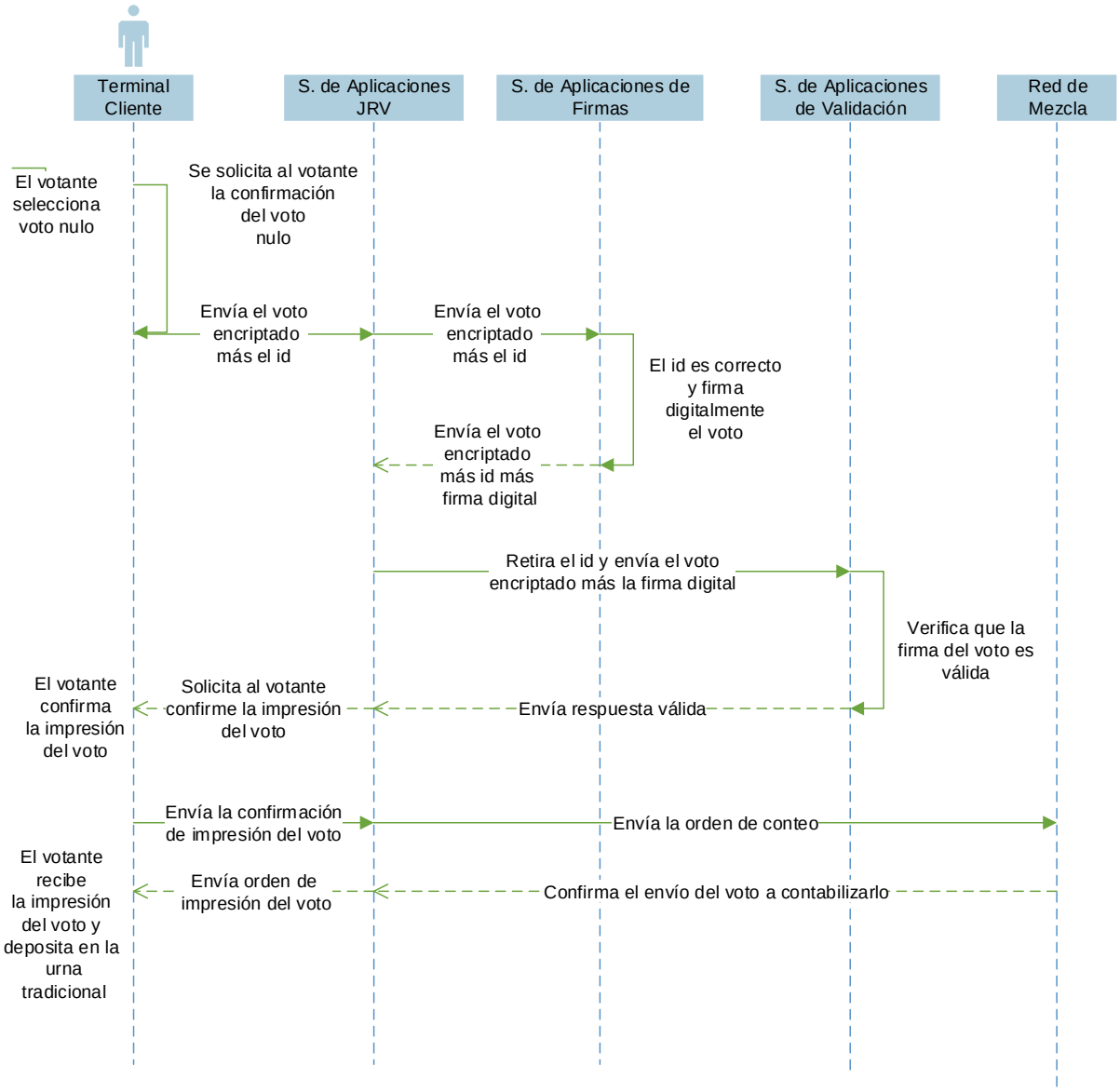


Figura 3-16. Votación. Escenario Alterno 2

3.2.3.2.4 Escenario Alterno 3: El votante intenta elegir más candidatos de los permitidos

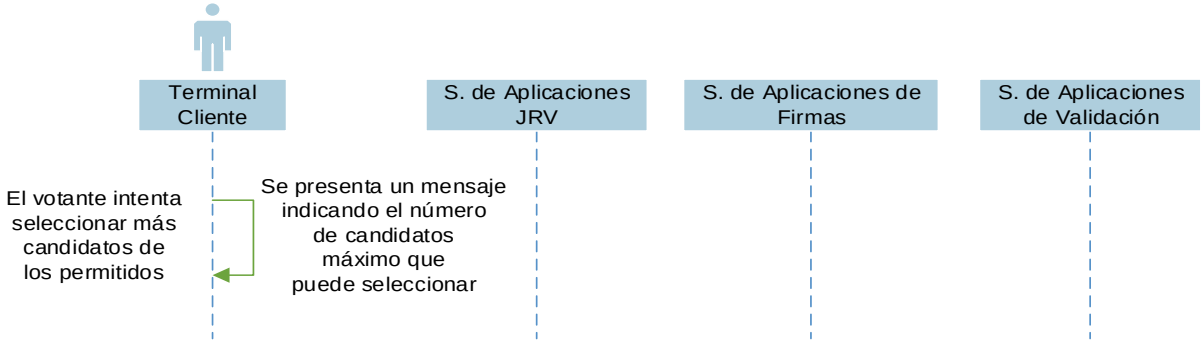


Figura 3-17. Votación. Escenario Alterno 3

3.2.3.2.5 Escenario Alterno 4: El votante rechaza la impresión del voto

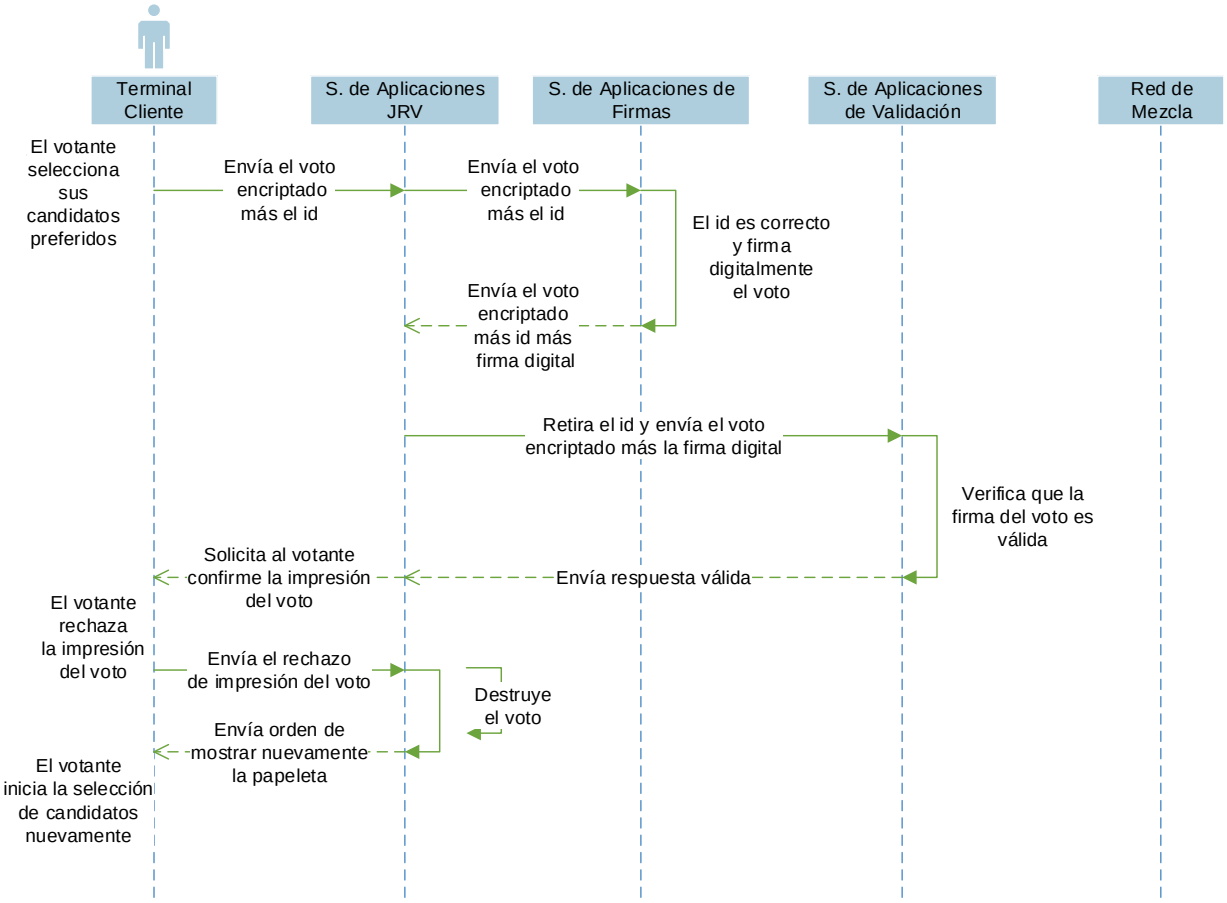


Figura 3-18. Votación. Escenario Alterno 4

3.2.3.2.6 Escenario Alterno 5: La firma del voto no es válida

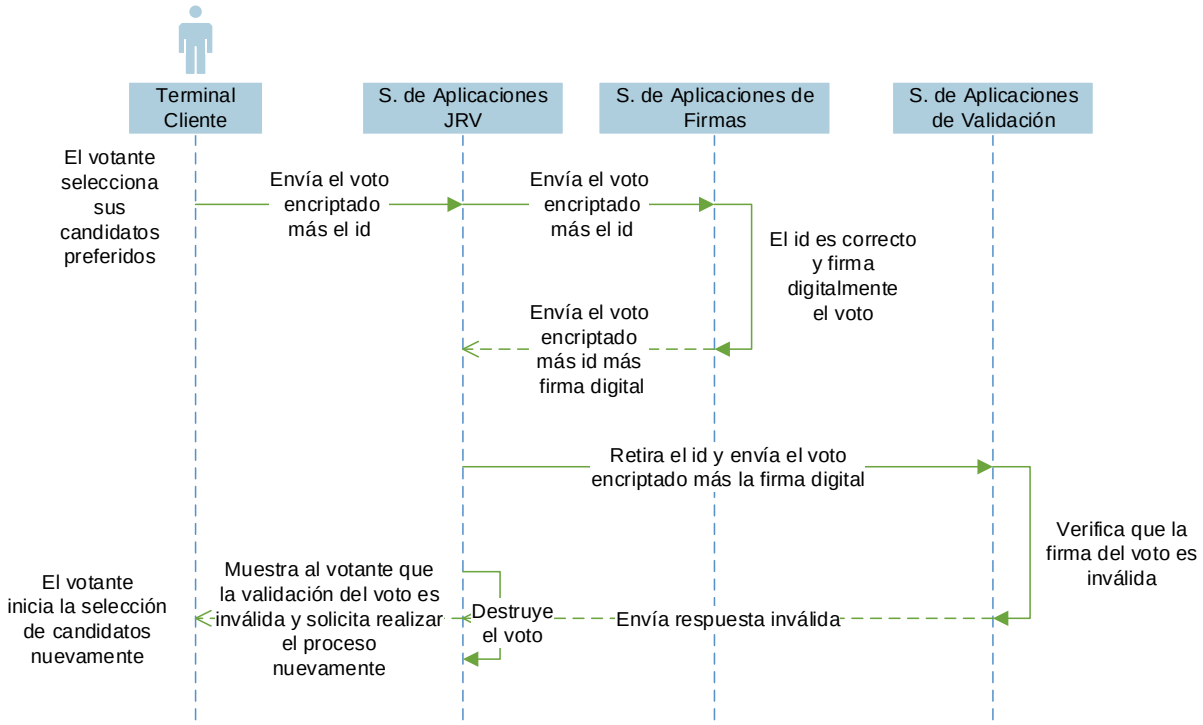


Figura 3-19. Votación. Escenario Alterno 5

3.2.3.3 Módulo de Conteo

Escenario Principal

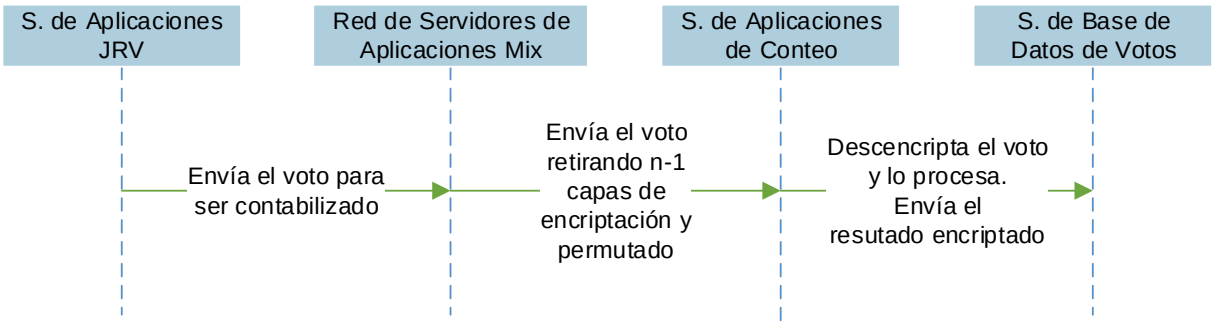


Figura 3-20. Conteo. Escenario Principal

3.2.3.4 Módulo de Resultados

Escenario Principal

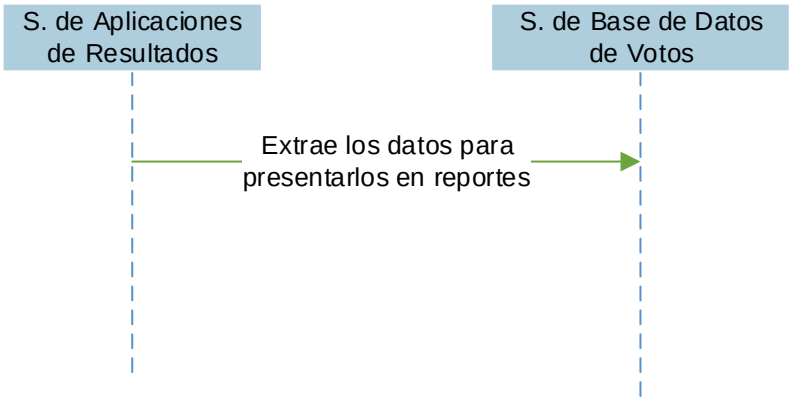


Figura 3-21. Resultados. Escenario Principal

3.3 DISEÑO DEL SISTEMA DE SEGURIDAD

El diseño del sistema de seguridad se basa en los esquemas criptográficos de firmas ciegas [43] y redes de mezcla [44]. El cifrado RSA se usará para encriptar la identificación del votante y el voto. Este diseño se basa en los requerimientos de software y de seguridad descritos en las secciones 2.2.1 y 2.2.3 respectivamente. El diseño de seguridad se divide en 3 fases: fase de Autenticación, fase de Votación y fase de Conteo. [45]

3.3.1 DISEÑO DE SEGURIDAD DURANTE LA FASE DE AUTENTICACIÓN DEL VOTANTE

La fase de Autenticación del votante tiene como objetivo asegurar que la identificación del votante se mantenga en secreto y que solo puedo emitir un voto. Para lo cual:

1. El votante ingresa su número de cédula al software de votación.
2. El software encripta el número de identificación con la llave pública del servidor de base de datos del Padrón Electoral.
3. El software de votación envía el número de cédula encriptado al servidor JRV. El envío se realiza a través del explorador que usa certificado SSL y la VPN IPSEC.
4. El servidor JRV solicita el número de identificación temporal del sistema al servidor de base de datos del Padrón Electoral.
5. El servidor de base de datos realiza verifica que el votante se encuentre habilitado para sufragar y envía el identificador temporal al servidor JRV.
6. El servidor de aplicaciones solicita la papeleta digital al servidor de base de datos Papeleta y envía el identificador encriptado y la papeleta digital al votante. El envío se lo realiza utilizando certificado SSL y por medio de la VPN IPSEC. [46] [47]

3.3.2 DISEÑO DE SEGURIDAD DURANTE LA FASE DE VOTACIÓN

La fase de Votación tiene como objetivo realizar el envío del voto en secreto y que llegue íntegro a su destino. Para lo cual:

1. El votante al momento de aceptar el envío del voto:
    a. El voto se encripta con las llaves públicas de los servidores Mix.
    b. El voto encriptado es enmascarado con un coeficiente de ocultamiento y una función. El proceso de ocultamiento del voto se especifica en el Anexo N.
    c. La identificación del votante se encripta con la llave pública del servidor de base de datos del Padrón Electoral.
2. El voto e identificador encriptado se envían cifrados con a través del explorador que usa certificado SSL y la VPN IPSEC.
3. El voto y el identificador son recibidos por el servidor JRV, y este los envía al servidor de firmas del voto.

4. El servidor de firmas del voto verifica que el identificador recibido conste en el Padrón Electoral y entonces procede a firmar el voto.
    a. El voto es firmado usando el esquema de firmas ciegas. Este esquema emplea el cifrado RSA. El proceso de firma del voto se especifica en el Anexo N.
5. El voto encriptado y firmado viaja junto al identificador del votante encriptado (con la llave pública del servidor de base de datos del Padrón Electoral) al servidor JRV.
6. El servidor JRV retira la identificación del votante y envía el voto firmado al servidor Validador de Firmas.
7. El servidor Validador de firmas verifica la autenticidad de la firma del voto. Para esto emplea un algoritmo de verificación detallado en el Anexo N.
8. El servidor Validador de firmas envía al servidor JRV el voto encriptado y la confirmación de que la firma es auténtica.
9. El servidor JRV envía la solicitud de confirmación del conteo del voto al votante.
10. El votante confirma su voto al servidor JRV.
11. El servidor JRV retira la firma del voto y envía el voto a la red de mezcla.

3.3.3 DISEÑO DE SEGURIDAD DURANTE LA FASE DE CONTEO DEL VOTO

La fase de Conteo del Voto tiene como objetivo anonimizar y contabilizar el voto. Para lo cual:

1. El servidor JRV envía el voto encriptado a la red de mezcla. La red de mezcla está conformada por 3 servidores mix.
2. El primer servidor de la red de mezcla S1 usará su llave privada para quitar la primera capa de encriptación del voto. Luego S1 envía el servidor mix S2 el voto permutado con el algoritmo de permutación descrito en el anexo P. La permutación consiste en no enviar los votos en el mismo orden que fueron recibidos.

3. S2 usará su llave privada para quitar la segunda capa de encriptación del voto. Luego S2 envía el voto permutado el servidor mix 3 o también llamado servidor de conteo el voto.
4. El servidor de conteo quitar la tercera y última capa de encriptación del voto. Luego, este servidor procesa el voto en claro. Este servidor permuta el resultado del voto y lo almacena encriptado al servidor de base de datos Votos. El resultado del voto es encriptado con la llave pública del servidor de base de datos Votos.

3.3.4 DISEÑO DE SEGURIDAD DURANTE LA FASE DE PRESENTACIÓN DE RESULTADOS

La fase de Presentación de Resultados tiene como objetivo permitir la publicación de los resultados del proceso electoral y proteger los votos emitidos de modificación o destrucción. Para lo cual:

5. El servidor de Conteo mantendrá una conexión con el servidor Publicación de Resultados para replicación de datos.
6. La estrategia de replicación será Maestro-Esclavo Unidireccional la cual se explica en el Anexo U. El servidor de Conteo tomará el papel de Maestro y el servidor Publicación de Resultados será el Esclavo.
7. Al finalizar el proceso de votación y tener una replicación del 100% en el Esclavo, la conexión entre los servidores será desactivada.
8. Se dispondrá de un terminal para acceder al Esclavo y el acceso será autorizado luego de desactivar la conexión entre los servidores Maestro-Esclavo.

CAPÍTULO IV

4 CONCLUSIONES Y RECOMENDACIONES

En este capítulo se presentan las conclusiones y recomendaciones que se obtuvieron como resultado del análisis y el desarrollo del diseño de la infraestructura tecnológica para realizar votación digital en Ecuador.

4.1 CONCLUSIONES

- Con base al análisis de las experiencias en implementación de votación digital de otros países se concluye que los problemas presentados se debieron por falta de control sobre los sistemas a usarse, antes de su despliegue el día de las elecciones. Esto demuestra que aunque existan leyes que normen los procesos electorales y los sistemas de votación a emplearse es necesario realizar control de cumplimento de estas normas desde la convocatoria a elecciones hasta la publicación de los resultados oficiales.
- Se realizó el análisis de riesgos de la infraestructura tecnológica para votación digital y se determinó que las amenazas que representan mayor riesgo son las de tipo humano. A pesar que los controles para mitigar el riesgo de las amenazas humanas existen, las personas son proclives a cometer errores o incumplir con las políticas de seguridad, ya sea deliberadamente o no.
- Se realizó un análisis de los problemas que se presentan en el proceso electoral manual. Se determinó que el factor que desata estos problemas es el humano y un sistema de votación digital no está exento de estos problemas. Sin embargo la diferencia entre la automatización del proceso y un proceso manual estriba en se puede generar registros que permitan identificar la o las personas que cometieron acciones ilícitas para sancionarlas y también determinar cuándo en un proceso electoral se ha cometido fraude.

- Los requerimientos del sistema de votación digital fueron abordados desde 3 perspectivas; software, red y seguridad. Los tres tipos de requerimientos permiten cumplir con la normativa del proceso electoral del Ecuador. Los objetivos son permitir al ciudadano emitir su voto directo y secreto.
- Para el análisis de los riesgos de la infraestructura de votación digital se utilizó Guía de Gestión de Riesgos para Sistemas de Tecnología de la Información NIST SP 800-30. El análisis de riesgos permitió: conocer las vulnerabilidades y los tipos de amenazas a las que está expuesta este tipo de infraestructuras. El riesgo más alto es cuando una amenaza de tipo humana explota vulnerabilidades de los recursos tecnológicos y humanos. Esta información fue la base para proponer un conjunto de controles que permitan operar la infraestructura de votación digital de manera segura.
- El diseño de la infraestructura de votación digital presentada en este proyecto de titulación propone de solución para realizar votación digital en el Ecuador. La infraestructura está compuesta por: esquemas criptográficos que aseguren al votante que su voto es contabilizado y ha sido emitido de manera anónima; una red de datos que permita la transferencia de la información de manera segura e implemente controles para contrarrestar ataques; y un software que implemente los procesos electorales del día de votación y controles para mitigar ataques.

4.2 RECOMENDACIONES

- Los requerimientos de software, de red y de seguridad fueron obtenidos con base en los datos actuales del proceso de votación como: definición de los procesos del día de votación, tamaño del Padrón Electoral y número de Recintos Electorales. Estos requisitos deben ser revisados y actualizados al menos cada año debido a los cambios en la tecnología, crecimiento del Padrón Electoral o cambios en los procesos electorales
- Implementar un ambiente de pruebas de la infraestructura tecnológica previo a la implementación del diseño propuesto en este documento. Esto permitirá verificar el funcionamiento del diseño propuesto de la infraestructura tecnológica para votación digital con el fin de identificar debilidades del diseño y realizar mejoras.
- El CNE debería establecer un Sistema de Gestión de la Seguridad de la información y el proceso electoral automatizado sea certificado con la norma ISO 27001. Esta certificación permite avalar que el CNE se encuentra apto para actuar en el caso de producirse un incidente de seguridad.
- Los certificados digitales utilizados en la infraestructura tecnológica para votación digital deberían ser otorgados por entidades certificadoras independientes al gobierno para asegurar que estos certificados no hayan sido manipulados por alguna entidad del gobierno antes, durante y al final del proceso electoral.
- Asignar un administrador para el monitoreo de cada servidor de la infraestructura tecnológica para votación digital durante el tiempo que tome el proceso electoral. Esto permitirá que en el caso de producirse un incidente de seguridad el administrador conozca de este hecho he inmediatamente tome medidas correctivas al respecto.

REFERENCIAS BIBLIOGRÁFICAS

[1] Consejo Nacional Electoral, "Guía de Procedimientos de la Juntas Receptoras del Voto," [Online]. Available: Guía de Procedimientos de la Juntas Receptoras del Voto.

[2] *Constitución de la República del Ecuador. Artículo 220,* 2008.

[3] *Constitución de la República del Ecuador. Artículo 47,* 2008.

[4] *Constitución de la República del Ecuador. Artículo 48,* 2008.

[5] *Constitución de la República del Ecuador. Artículo 65,* 2008.

[6] "Naciones Unidas," [Online]. Available: http://www.un.org/esa/socdev/enable/documents/tccconvs.pdf.

[7] "Consejo Nacional Electoral," [Online]. Available: http://cne.gob.ec/es/secretaria/resoluciones/download/file?fid=8.110.

[8] C. N. Electoral, "Guía de Procedimientos de las Juntas Receptoras del Voto Votación," [Online]. Available: http://capacitacionelectoral.cne.gob.ec/mod/resource/view.php?id=61.

[9] R. Rivera, "Comparison of the OCTAVE and NIST's Special Publication 800-30 Methodologies," 02 Diciembre 2004. [Online]. Available: http://www.angelfire.com/tx5/techpc/Octave.html.

[10] T. Mark and M. Jason, TALABIS, Mark, MARTIN, Jason, “Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis”, Syngress, 2012.

[11] C. Wilmer, "Metodologías para el análisis de riesgos en Seguridad Informática," 02 Marzo 2011. [Online]. Available:

http://wilmer09.blogspot.com/2011/03/metodologias-para-el-analisis-de.html.

[12] IBM, "IBM Passport Advantage Express," [Online]. Available: http://goo.gl/v5nByK.

[13] ORACLE, "Oracle Store," [Online]. Available: http://goo.gl/c2JW6g.

[14] F. B. d. Monte, "SelectedWorks," [Online]. Available: http://works.bepress.com/cgi/viewcontent.cgi?article=1025&context=fernando_barrientos.

[15] Smartmatic, "BusinessWire," 31 Enero 2012. [Online]. Available: http://www.businesswire.com/news/home/20120131005851/es/#.U-.

[16] Smartmatic, "Smartmatic," 03 Marzo 2014. [Online]. Available: http://elecciones.smartmatic.com/prueba-publica-de-voto-electronico-en-faribault-estados-unidos-el-6-de-marzo/.

[17] Carter Center, "CarterCenter," [Online]. Available: http://www.cartercenter.org/resources/pdfs/peace/americas/EstudioElectoralVenezuela1%20CarterCenter.pdf.

[18] VOTO DIGITAL, "Voto Digital," 4 Marzo 2014. [Online]. Available: https://votodigital.wordpress.com/tag/elecciones-provinciales-2014-ecuador/.

[19] VOTO DIGITAL, "Voto Digital," 4 Octubre 2013. [Online]. Available: https://votodigital.wordpress.com/2013/10/04/ecuador-una-eleccion-dos-modelos-de-voto-electronico/.

[20] VOTO DIGITAL, "Voto Digital," 14 Septiembre 2013. [Online]. Available: https://votodigital.wordpress.com/2013/09/14/ecuador-se-prepara-para-cambiar-con-la-ayuda-de-la-tecnologia/.

[21] EL TELÉGRAFO, "El telégrafo," 23 Enero 2014. [Online]. Available: http://www.telegrafo.com.ec/politica/item/la-morita-conocio-sobre-el-voto-electronico.html.

[22] RADIO HUANCAVILCA, "radiohuancavilca," 20 Diciembre 2013. [Online]. Available: http://radiohuancavilca.com.ec/politica/2013/12/20/tecnologia-rusa-para-voto-electronico-en-pichincha/.

[23] VOTO DIGITAL, "Voto Digital," 25 Enero 2014. [Online]. Available: https://votodigital.wordpress.com/2014/01/25/1902/.

[24] VOTO DIGITAL, "Voto Digital," 20 Diciembre 2013. [Online]. Available: https://votodigital.wordpress.com/2013/12/20/ecuador-avanza-seguro-hacia-el-voto-electronico/.

[25] VOTO DIGITAL, "Voto Digital," 24 Febrero 2014. [Online]. Available: https://votodigital.wordpress.com/2014/02/24/el-voto-electronico-se-estreno-con-exito-en-ecuador/.

[26] VOTO DIGITAL, "Voto Digital," 16 Febrero 2014. [Online]. Available: https://votodigital.wordpress.com/2014/02/16/simulacros-dejaron-a-punto-el-voto-electronico-en-ecuador/.

[27] CISCO, "Scribd," 04 Diciembre 2013. [Online]. Available: http://es.scribd.com/doc/189303257/70894041-Son-A.

[28] M. Evelio, "Eveliux," 2007, 21 Julio. [Online]. Available: http://www.eveliux.com/mx/Diseno-de-una-red.html.

[29] UNELINK, "Unelink," [Online]. Available: https://www.unelink.es/procesador-cpu/velocidad-194-c.html.

[30] CULTURACIÓN, "Culturación," [Online]. Available:

http://culturacion.com/como-mejorar-el-desempeno-de-una-red-ii/.

[31] ALBY, "Microsiervos," 2005, 15 Septiembre. [Online]. Available: http://www.microsiervos.com/archivo/seguridad/rsa-1024-no-es-suficiente.html.

[32] OAS, "Organization of American States," [Online]. Available: https://www.oas.org/dsd/publications/Unit/oea32s/ch71.htm.

[33] A. Martinez, "La Información," 25 Junio 2013. [Online]. Available: http://goo.gl/Hq7uF.

[34] CONELEC, "Conelec," [Online]. Available: http://www.conelec.gob.ec/enlaces_externos.php?l=1&cd_menu=4247.

[35] CISCO SYSTEM INC., Designing for Cisco Internetwork Solutions, Student Guide, 2007.

[36] CISCO SYSTEM INC., “CISCO SAFE Implementation”, Student Guide, 2004.

[37] K. Vasquez, "Scribd," 17 Junio 2012. [Online]. Available: http://es.scribd.com/doc/97362933/Arquitectura-Sona-Cisco-Framework.

[38] Anónimo, "Etimosoft," 10 Febrero 2012. [Online]. Available: http://timosoft.wordpress.com/2012/02/10/cisco-safe/.

[39] H. Reyes, "SlideShare," 12 Julio 2013. [Online]. Available: http://es.slideshare.net/hugoreyes79/conexiones-vpn.

[40] CISCO, "CISCO," [Online]. Available: http://www.cisco.com/web/ES/solutions/es/vpn/index.html.

[41] Jolman, "Scribd," 07 Abril 2007. [Online]. Available: http://es.scribd.com/doc/14025162/Manual-Infraestructura-VPN-Segura.

[42] EKONTSULTA, "ekontsulta," 11 Junio 2009. [Online]. Available: http://www.ekontsulta.net/ekontsulta/wiki/index.php/VPN.

[43] C. P. y. e. al, "Universidad de Sevilla," 28 Septiembre 2007. [Online]. Available: http://congreso.us.es/cedya2007/actas/textos/144.pdf.

[44] P. Seguel, "Universidad de Chile," Agosto 2009. [Online]. Available: http://users.dcc.uchile.cl/~ahevia/proyectos/mixnets/pseguel/memoria.pdf.

[45] C. García, "Cinvestav," Septiembre 2005. [Online]. Available: http://delta.cs.cinvestav.mx/~francisco/Repository/tesisCPGZ.pdf.

[46] E. Arias, Implantación de una Red Privada Virtual, 2007.

[47] J. Tomás, Servicio VPN de acceso remoto basado en SSL mediante OpenVPN, 2008.

[48] R. Silva, "SlideShare," 26 Febrero 2014. [Online]. Available: http://es.slideshare.net/roxanasilvach/presentacion-inclusion-19-022014.

[49] Wikipedia, "Wikipedia," 11 Marzo 2014. [Online]. Available: http://es.wikipedia.org/wiki/Tarjeta_de_banda_magn%C3%A9tica.

[50] Wikipedia, "Wikipedia," 11 Septiembre 2014. [Online]. Available: http://es.wikipedia.org/wiki/Tarjeta_inteligente.

[51] Wikipedia, "Wikipedia," 8 Marzo 2013. [Online]. Available: http://es.wikipedia.org/wiki/Tarjeta_de_proximidad.

[52] M. Bellare, "École Normale Supérieure," 2003. [Online]. Available: http://www.di.ens.fr/~pointche/Documents/Papers/2003_joc.pdf.

[53] M. López, "Cinvestav," Junio 2011. [Online]. Available: http://www.cs.cinvestav.mx/TesisGraduados/2011/TesisLourdesLopez.pdf.

[54] C. Jiménez, "Archivo Digital UPM," Septiembre 2010. [Online]. Available: http://oa.upm.es/4803/1/PFC_CARLOS_CASELLES_JIMENEZ.pdf.

[55] IBM, "Tivoli Software," [Online]. Available: https://publib.boulder.ibm.com/tividd/td/TRM/SC23-4822-00/es_ES/HTML/user277.htm.

[56] J. Spichiger, "Redes Cisco," [Online]. Available: http://www.redescisco.net/archivos/clases_online/Clase1_ACL.pdf.

[57] Securay, "Scribd," 9 Agosto 2012. [Online]. Available: http://es.scribd.com/doc/102406804/Replicacion-asincrona-unidireccional-Maestro-Linux.

[58] V. R. Buchillón, "Monografías," [Online]. Available: http://www.monografias.com/trabajos82/replicaciondatos/replicaciondatos2.shtml#ixzz3LNWvO2hE.

GLOSARIO

Algoritmo de Euclides extendido: el algoritmo de Euclides extendido permite, además de encontrar un máximo común divisor de dos números enteros a y b, expresarlo como la mínima combinación lineal de esos números, es decir, encontrar números enteros s y t tales que mcd(a,b)=a s+b t.

Ancho de banda: es la longitud, medida en Hz, del rango de frecuencias en el que se concentra la mayor parte de la potencia de la señal.

Amenaza: es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño ya sea material o inmaterial, sobre los elementos de un sistema

Aritmética modular: es un sistema aritmético para clases de equivalencia de números enteros llamadas clases de congruencia

Aplicación Web: es un tipo de aplicación en la que los usuarios utilizan un programa de escritorio conocido como “browser” o navegador, para conectarse con un servidor web.

Aplicación: es un programa de computador destinado a realizar una tarea específica.

Audiencia Pública: “constituye una instancia de participación en el proceso de toma de decisión administrativa o legislativa en el cual la autoridad responsable de la misma habilita un espacio institucional para que todos aquellos que puedan verse afectados o tengan un interés particular expresen su opinión respecto de ella. El objetivo de esta instancia es que la autoridad responsable de tomar la decisión

acceda a las distintas opiniones sobre el tema en forma simultánea y en pie de igualdad a través del contacto directo con los interesados."[21]

Autenticación: es un proceso mediante el cual una persona o entidad se identifica dentro de un sistema.

Coprimo: también conocido como primos entre sí o primos relativos, si dos números enteros a y b no tienen ningún factor primo en común, o, dicho de otra manera, si no tienen otro divisor común más que 1 y -1.

Desempeño de red: es una medida concreta y de fácil cálculo, que permite saber si una red está funcionando en forma óptima.

Discapacidad psíquica: se considera que una persona tiene discapacidad psíquica cuando presenta "trastornos en el comportamiento adaptativo, previsiblemente permanentes".

Discapacidad intelectual o mental: se considera discapacidad intelectual al funcionamiento intelectual inferior a la media, que coexiste junto a limitaciones en dos ó más de las siguientes áreas de habilidades de adaptación: comunicación, cuidado propio, vida en el hogar, habilidades sociales, uso de la comunidad, autodirección, salud y seguridad, contenidos escolares funcionales, ocio y trabajo

Discapacidad física: la diversidad funcional motora se puede definir como la disminución o ausencia de las funciones motoras o físicas (ausencia de una mano, pierna, pie, entre otros), disminuyendo su desenvolvimiento normal diario

[21] http://residuoszarate.wordpress.com/programa-de-contrataciones-publicas-transparentes/audiencias-publicas/que-es-una-audiencia-publica/

Discapacidad sensorial: la discapacidad sensorial corresponde a las personas con deficiencias visuales, a los sordos y a quienes presentan problemas en la comunicación y el lenguaje.

Escrutinio: computo de los votos emitidos durante un proceso de votación.

Esquemas de Relleno: mecanismos de llenado que introducen información irrelevante para mantener cierta seguridad sobre la privacidad del contenido y así ocultar la estructura de los datos estructura.

Firma ciega: es un protocolo de firma digital que permite a una persona obtener un mensaje firmado por otra entidad, sin revelarle información del contenido del mensaje.

Firma Digital: mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente determinar la entidad originadora de dicho mensaje y confirmar que el mensaje no ha sido alterado desde que fue firmado por el originador.

Framework: conocido también como marco de trabajo, es un conjunto de prácticas, criterios y conceptos que se utilizan como referencia para resolver problemas de índole similar.

Función φ de Euler: si n es un número entero positivo, entonces φ(n) se define como el número de enteros positivos menores o iguales a n y coprimos con n.

IBM WebSphere Application Server: es un servidor de aplicaciones de la familia WebSphere, construido con estándares de libre acceso y distribuido por la empresa IBM.

Impacto: conjunto de consecuencias provocadas por un hecho o actuación que afecta a un entorno.

ISO 27005: es una parte de la familiar de estándares internacionales, publicada por la Organización Internacional de Estandarización (ISO por sus siglas en inglés), y se enfoca en técnicas para manejo de riesgos de seguridad de la información.

JBoss: es un servidor de aplicaciones de código abierto que está avalado por la empresa Red Hat.

Junta receptora del voto: son organismos de gestión electoral con carácter temporal que se encargarán de instalar las mesas para la recepción del voto, harán el conteo y llenarán las actas de escrutinio.

Multiplicador modular inverso: el multiplicador modular inverso de un entero n módulo p es un entero m tal que $n^{-1} \equiv m \pmod{p}$

NIST SP 800-30: es una guía de gestión de riesgos de los sistemas de tecnología de la información.

Octave: es un conjunto de herramientas, técnicas y métodos para la evaluación de seguridad basada en los riesgos.

Oracle WebLogic: es un servidor de aplicaciones y servidor HTTP distribuido por la empresa Oracle.

Padrón electoral: es un registro en el que se detalla un listado de las personas que poseen el derecho del sufragio.

Requerimientos funcionales: son determinadas funciones o características que debe poseer un producto de software.

Riesgo: es un r problema potencial que puede ocurrir en cuando una amenaza explota una vulnerabilidad.

SCRUM: es una metodología de desarrollo ágil iterativo e incremental.

Servidor de Aplicaciones: es un tipo de servidor interconectado a una red que tiene la función de ejecutar determinadas aplicaciones.

Test de primalidad: es un algoritmo que dado un número de entrada n, no consigue verificar la hipótesis de un teorema cuya conclusión es que n es compuesto, entonces por lo tanto el número es primo.

Tolerancia a fallos: es la capacidad de un sistema de acceder a la información, aun en caso de producirse algún fallo o anomalía.

Trama: unidad de envio de datos.

Voto Digital: es un tipo de votación en el que se automatizan ciertos procesos, como la emisión de los votos y/o el escrutinio.

Vulnerabilidad: es la capacidad, las condiciones y características del sistema mismo que lo hace susceptible a amenazas, con el resultado de sufrir algún daño.

xP: es una metodología de desarrollo ágil iterativo e incremental.

ACRÓNIMOS

- AH: Authentication Protocol.
- CNE: Consejo Nacional Electoral.
- DER: Diagrama Entidad Relación.
- DRE: Direct-recording electronic.
- ESP: Encapsulated Security Payload.
- HAVA: Help America Vote Act
- HIDS: Host-based Intrusion Detection System.
- HTTP: Protocolo de Transferencia de Hipertexto.
- HTTPS:Protocolo de Transferencia de Hipertexto Segura.
- IDE: Ambiente integrado de desarrollo.
- IDS: Sistema de detección de intrusos.
- IP: Internet Protocol.
- ISO: Organización Internacional de Estandarización.
- ISP: Internet Service Provider.
- ITAA: Information Technology Association of America.
- JRV: Junta receptora del Voto.
- LAN: Red de Área Local.
- MSA: Magic Software Argentina.
- NIST SP: National Institute of Standards and Technology Special Publications.
- NOS: Sistema Operativo de Red.
- RSA: Ron Rivest, Adi Shamir y Leonard Adleman.
- SOAP: Simple Object Access Protocol.
- SSL: Secure Socktes Layer.
- TCP: Protocolo de Control de Transmisión.
- UI: Interfaz de Usuario.
- VIVA: Voting Integrity and Verification Act.

- VPN: Red Virtual Privada.
- WAS: WebSphere Application Server.
- WSDL: Web Service Definition Language.
- XP: eXtreme Programming.

ANEXOS

ANEXO A: Artículos de la Constitución de la República de Ecuador

Art. 425. “La Constitución es la norma suprema y prevalece sobre cualquier otra del ordenamiento jurídico. Las normas y actos del poder público deberán mantener conformidad con las disposiciones constitucionales; en caso contrario carecerán de eficacia jurídica.

La Constitución y los tratados internacionales de derechos humanos ratificados por el Estado que reconozcan derechos más favorables a los contenidos en la Constitución, prevalecerán sobre cualquier otra norma o acto del poder jurídico.”

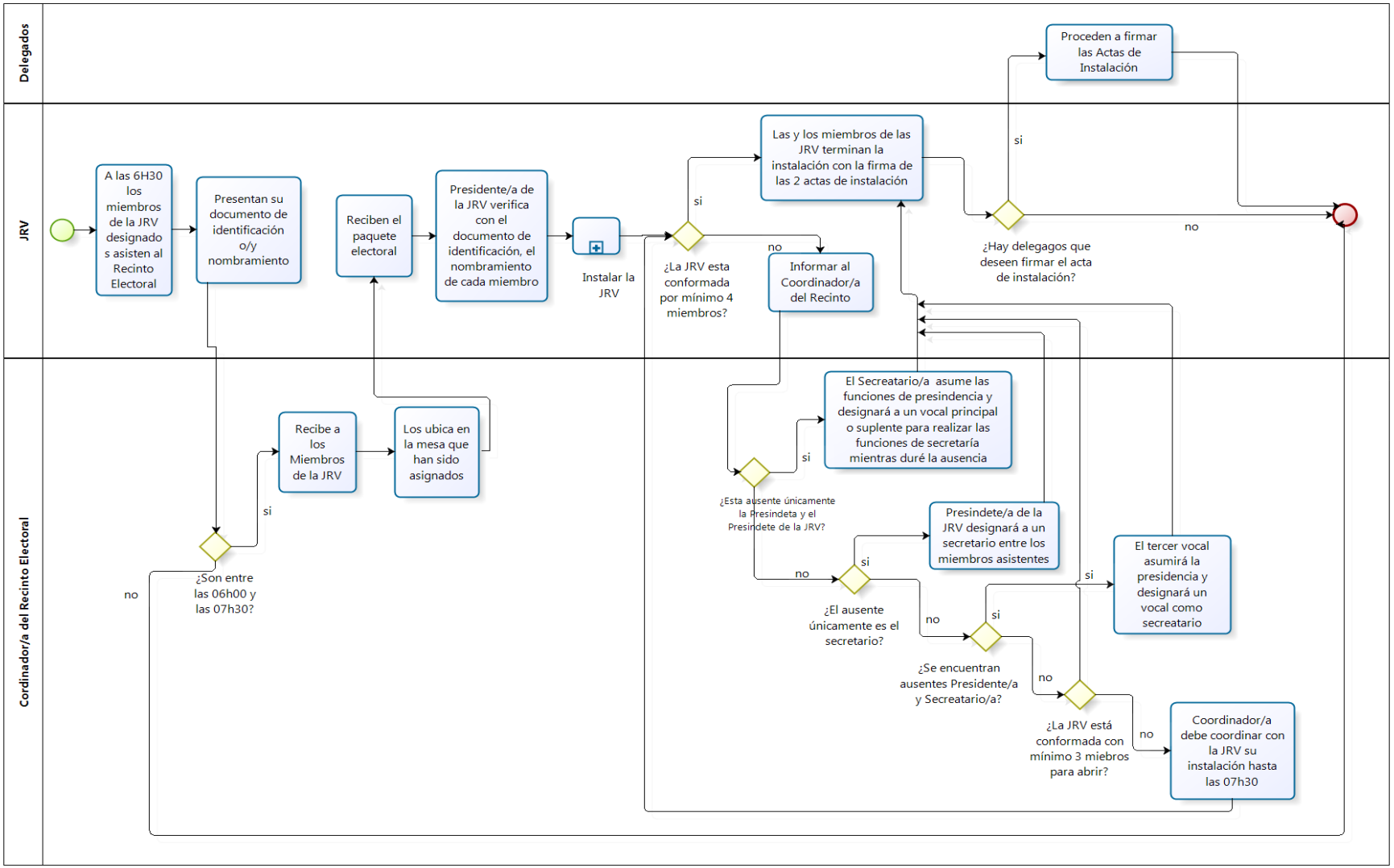
Art. 426. “El orden jurídico de aplicación de las normas será el siguiente: La Constitución; los tratados y convenios internacionales; las leyes orgánicas; las leyes ordinarias; las normas regionales y las ordenanzas distritales; los decretos y reglamentos; las ordenanzas; los acuerdos y las resoluciones; y los demás actos y decisiones de los poderes públicos.

En caso de conflicto entre normas de distinta jerarquía, la Corte Constitucional, las juezas y jueces, autoridades administrativas y servidoras y servidores públicos, lo resolverán mediante la aplicación de la norma jerárquica superior.”

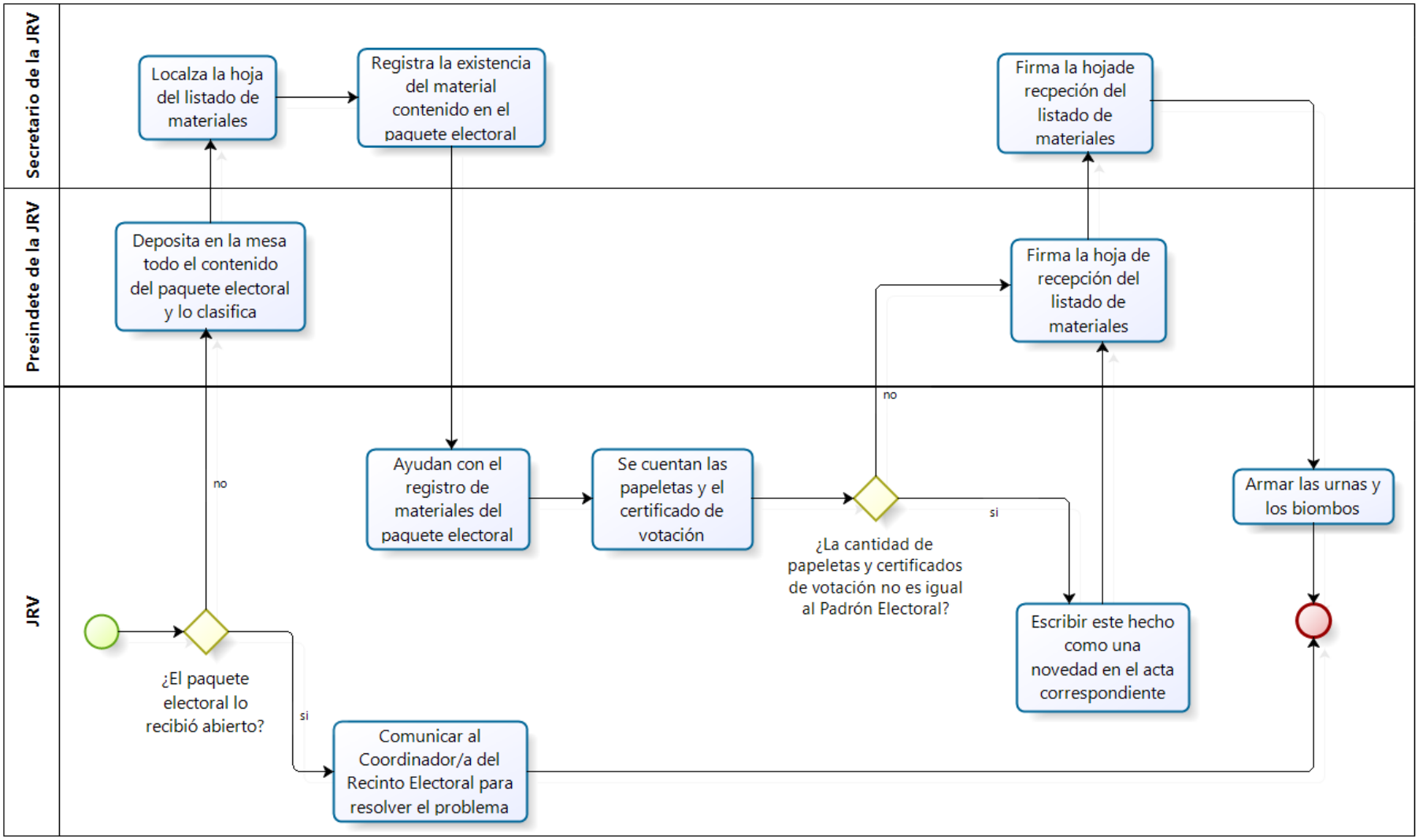
Art. 217. “La Función Electoral garantizará el ejercicio de los derechos políticos que se expresan a través del sufragio, así como los referentes a la organización política de la ciudadanía.

La Función Electoral estará conformada por el Consejo Nacional Electoral y el Tribunal Contencioso Electoral. Ambos órganos tendrán sede en Quito, jurisdicción nacional, autonomías administrativa, financiera y organizativa, y personalidad jurídica propia. Se regirán por principios de autonomía, independencia, publicidad, transparencia, equidad, interculturalidad, paridad de género, celeridad y probidad.”

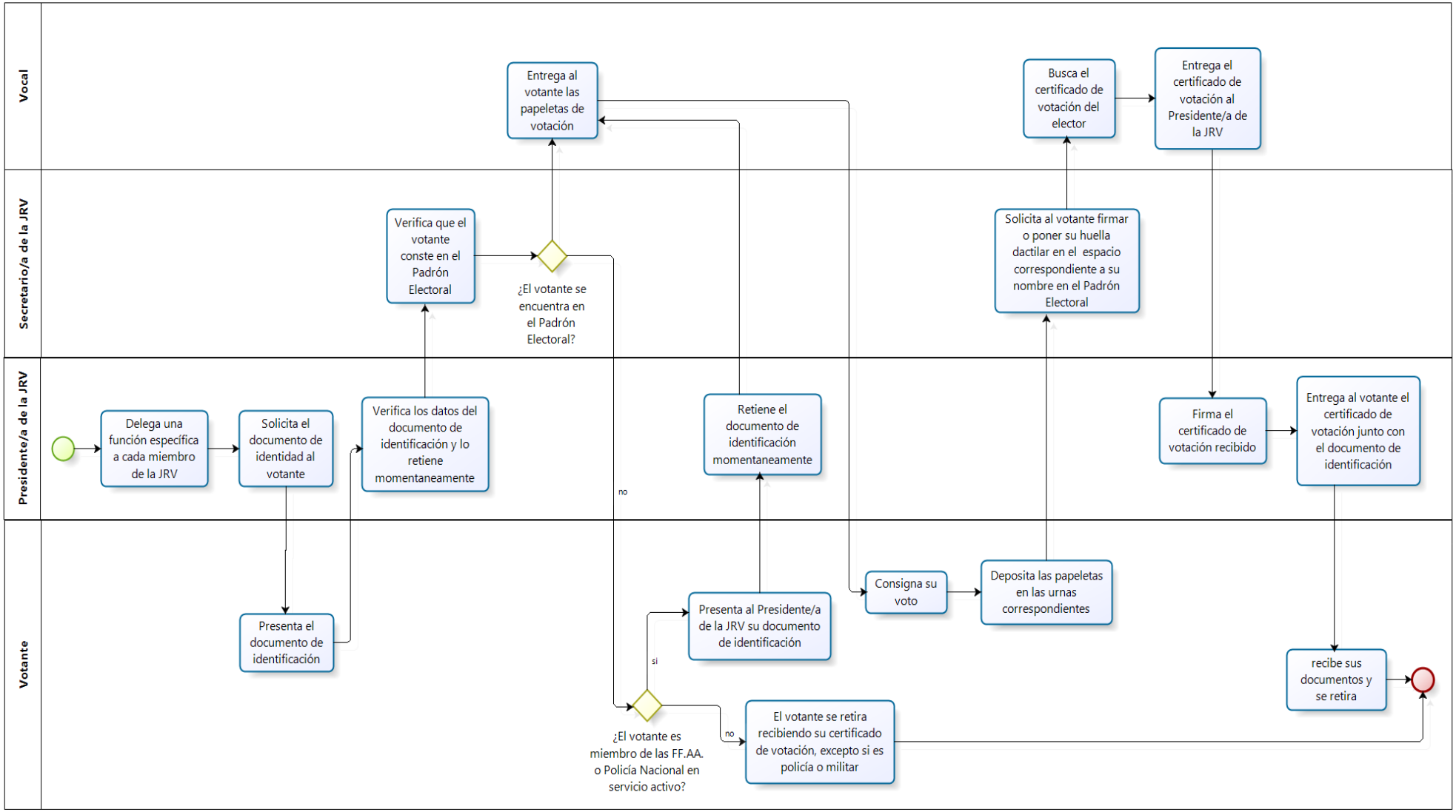
ANEXO B: Diagrama de Procesos de la Fase de Instalación



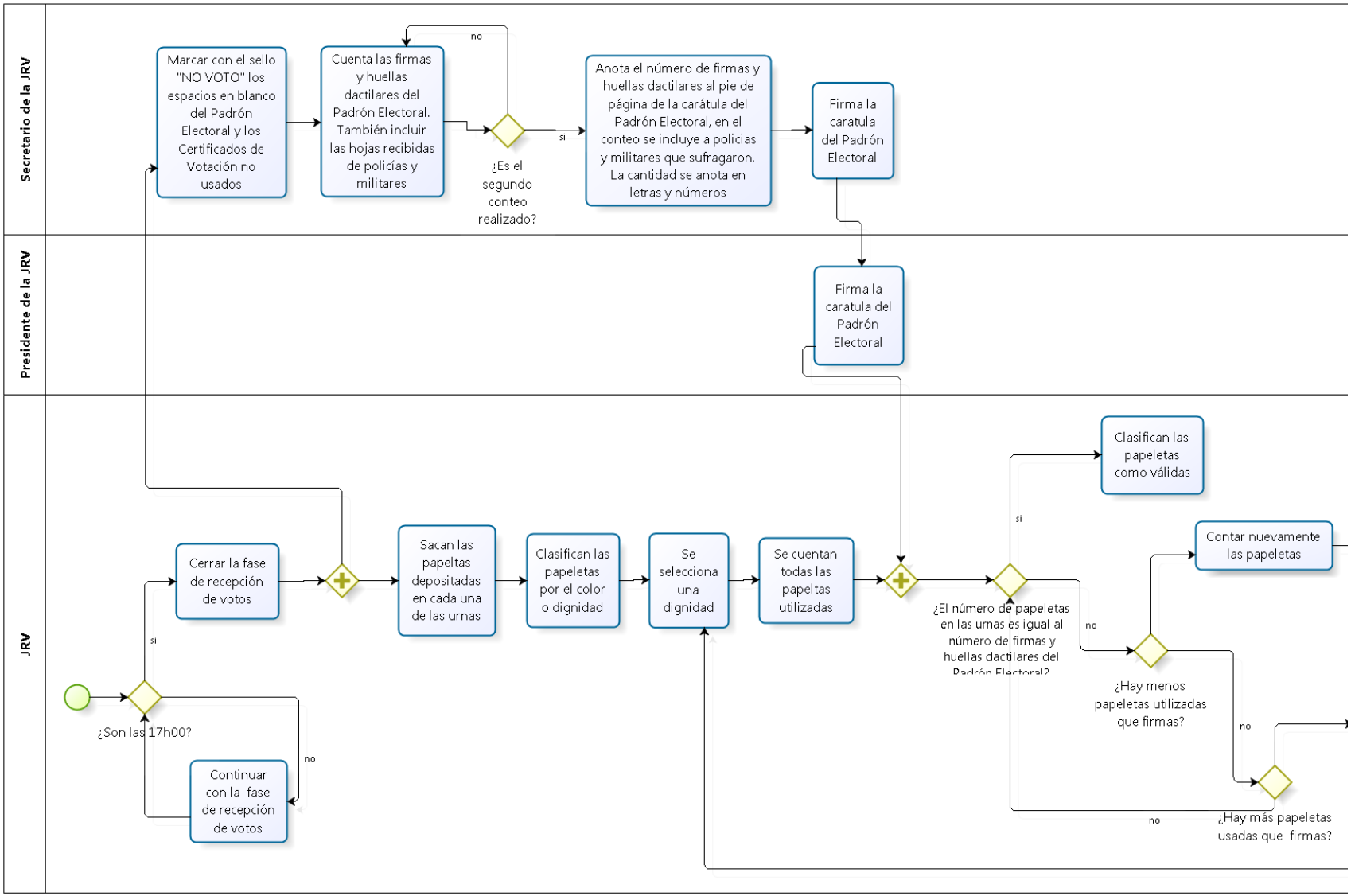
ANEXO C: Diagrama de Procesos de la Fase de Instalación.



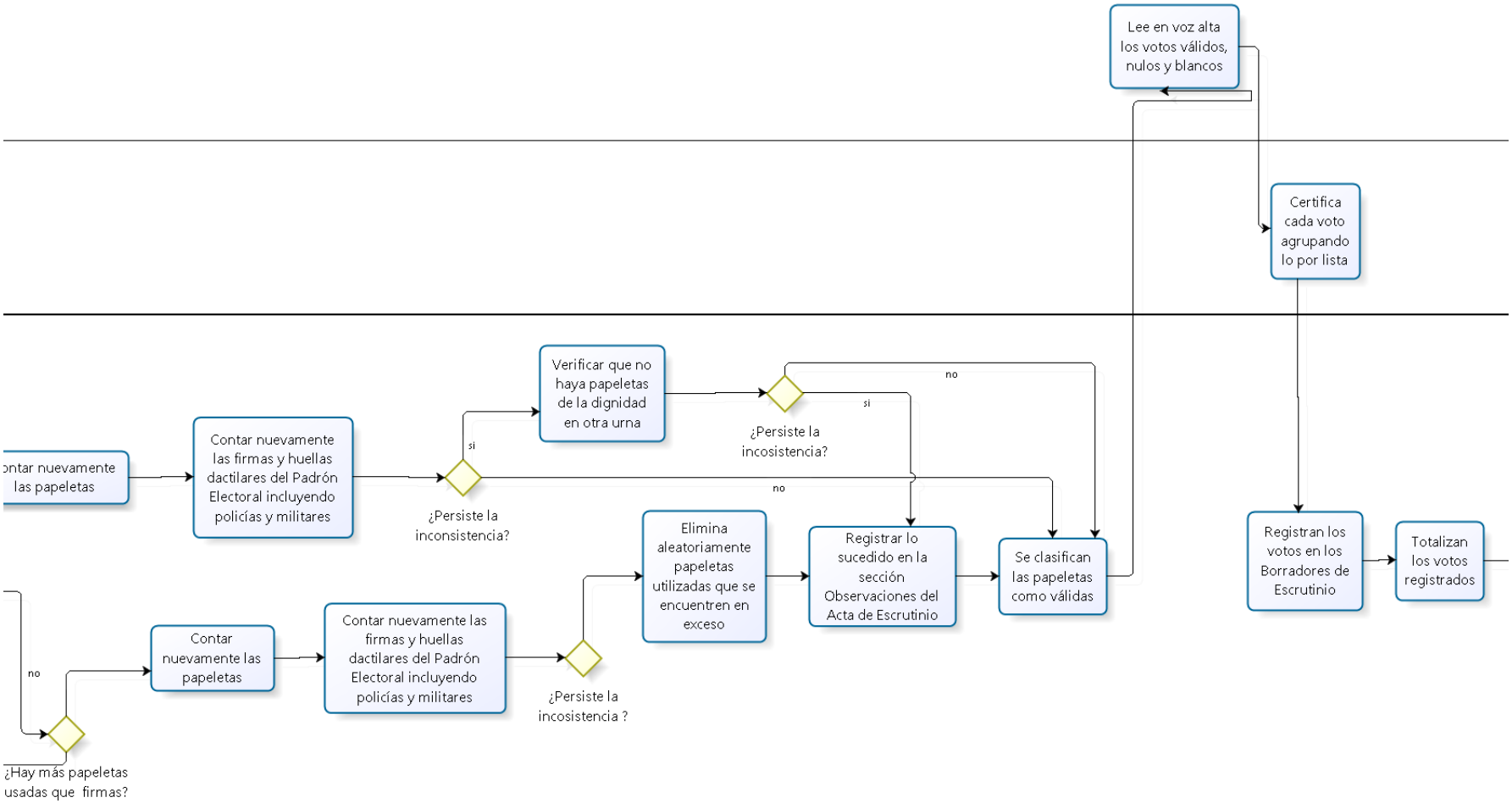
ANEXO D: Diagrama de Procesos de la Fase de Votación



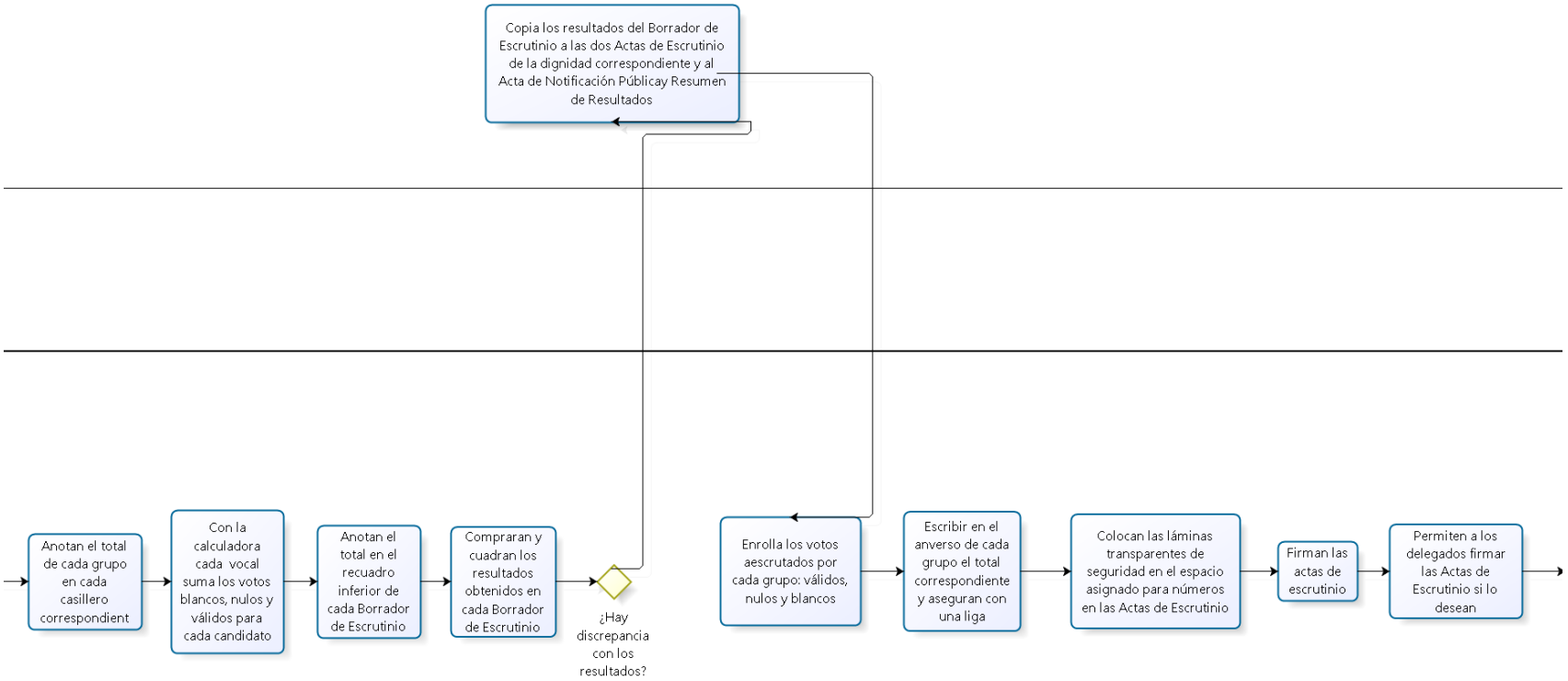
ANEXO E: Diagrama de Procesos de la Fase de Escrutinio en la JRV.



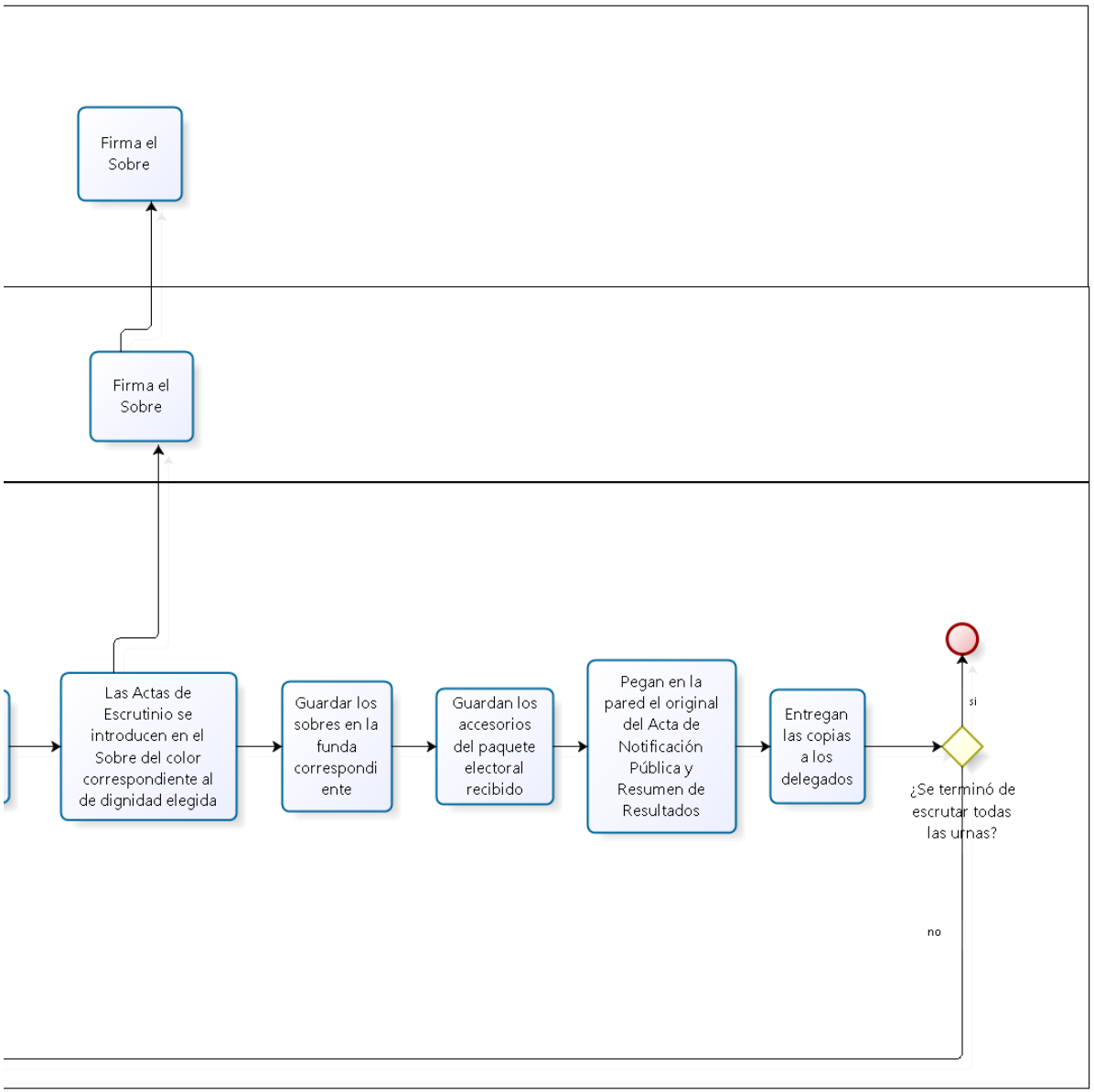
Continúa en la siguiente página



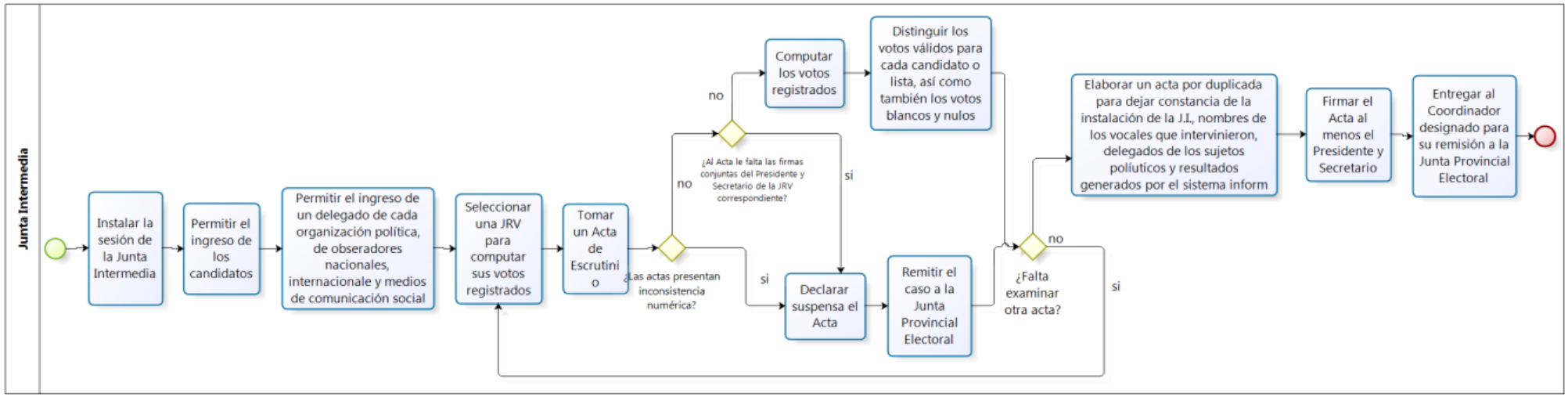
Continúa en la siguiente página



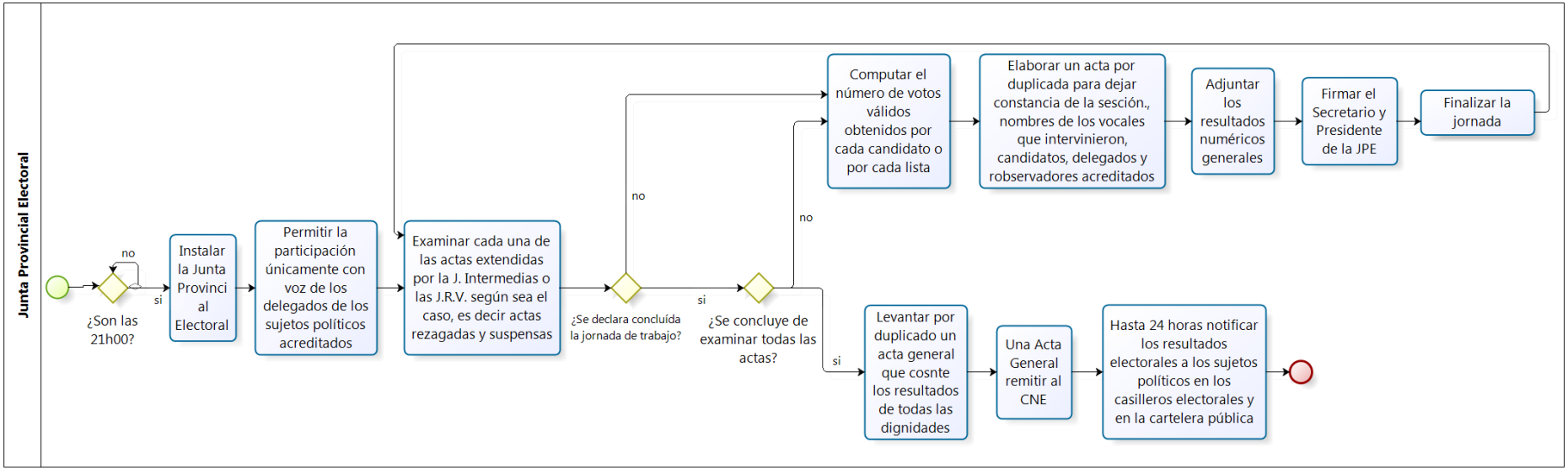
Continúa en la siguiente página


Firma el Sobre
Firma el Sobre
Las Actas de Escrutinio se introducen en el Sobre del color correspondiente al de dignidad elegida
Guardar los sobres en la funda correspondi ente
Guardan los accesorios del paquete electoral recibido
Pegan en la pared el original del Acta de Notificación Pública y Resumen de Resultados
Entregan las copias a los delegados
¿Se terminó de escrutar todas las urnas?
si
no

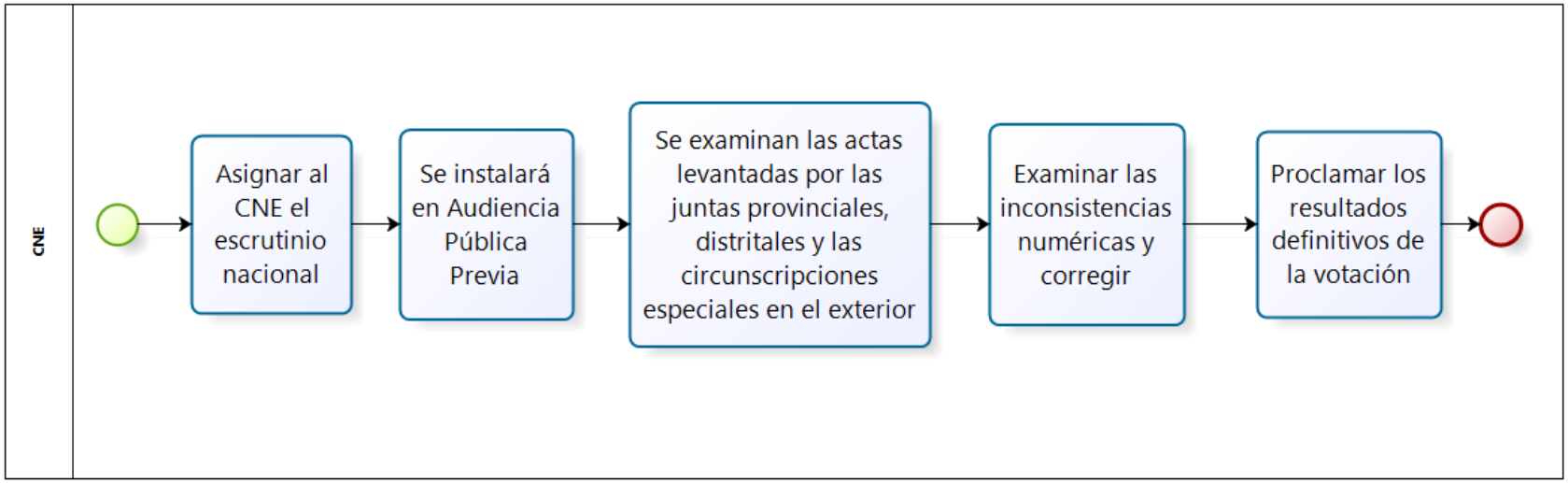
ANEXO F: Diagrama de Procesos de la Fase de Escrutinio en la JI



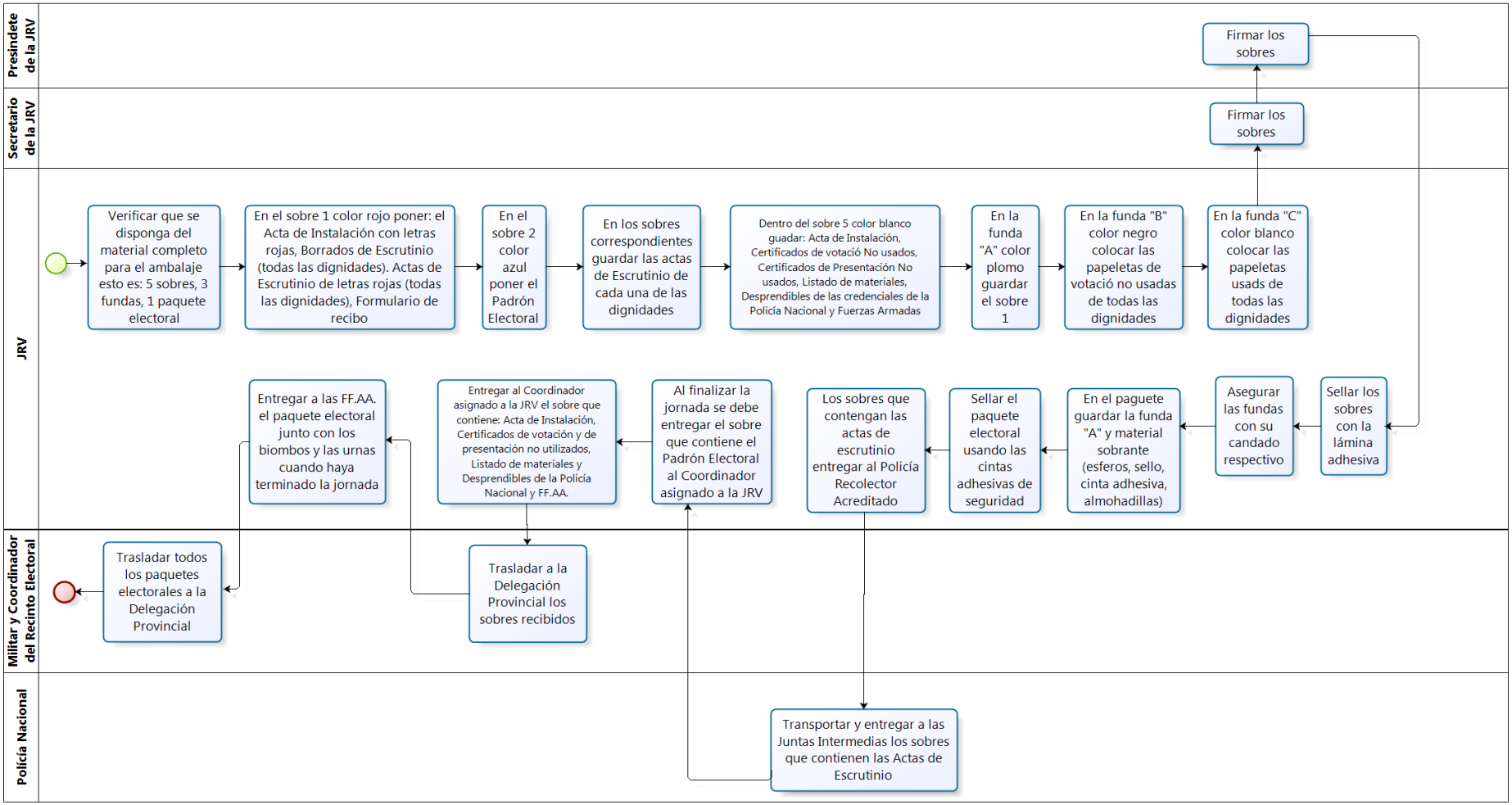
ANEXO H: Diagrama de Procesos de la Fase de Escrutinio en la JEP.



ANEXO I: Diagrama de Procesos de la Fase de Escrutinio Nacional.

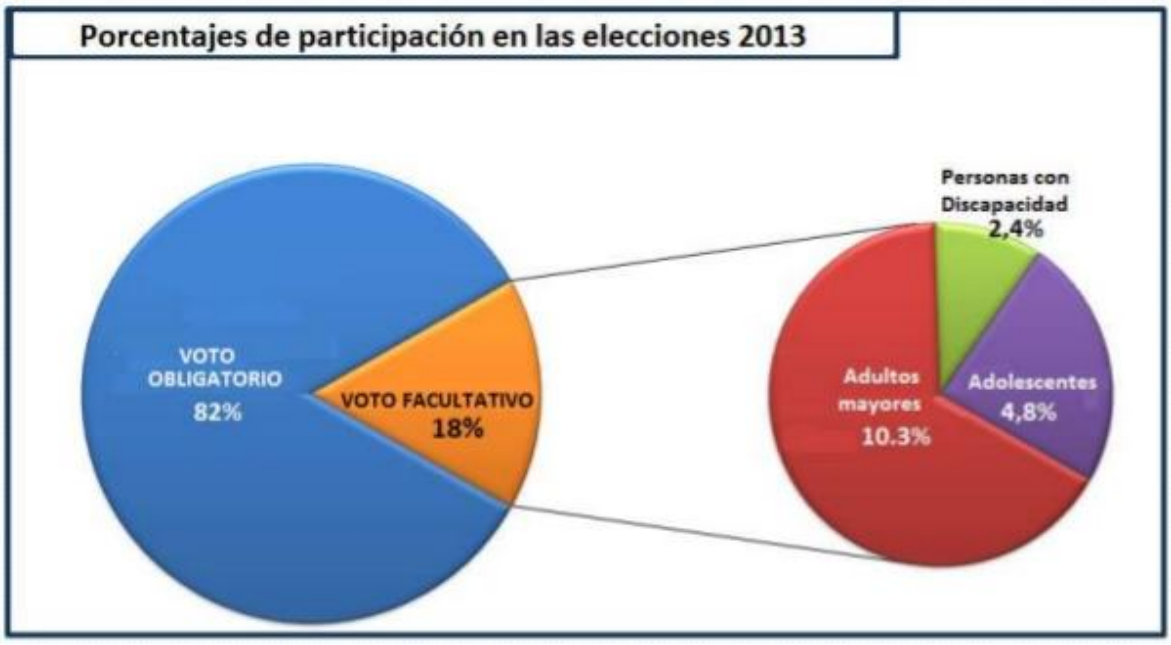


ANEXO J: Diagrama de Procesos de Envío y Embalaje del material electoral



ANEXO K: Estadísticas de Electores con Discapacidad en Ecuador en el 2014

El número de personas con discapacidad empadronadas para las elecciones de febrero de 2014 en Ecuador fueron 304.108 [48] votantes. Los 304.108 votantes constituyen el 2.4% del Padrón Electoral.

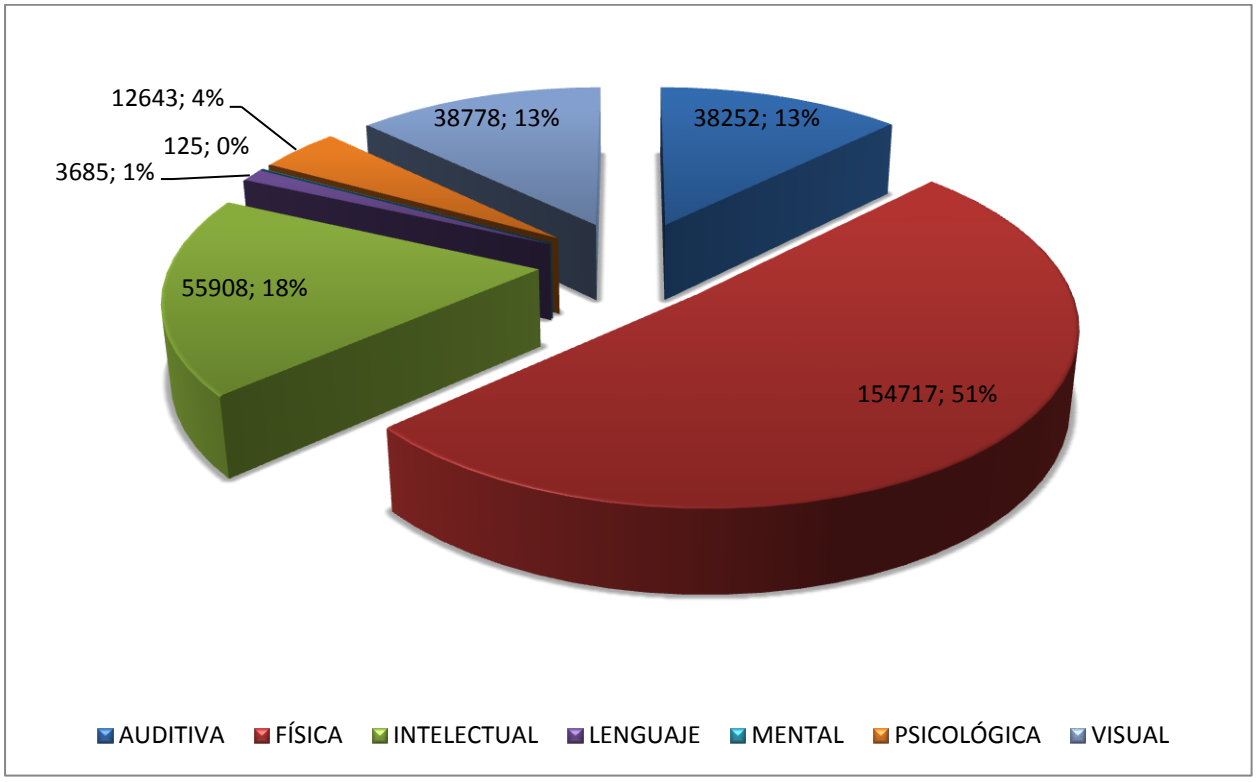


Representación del Voto Facultativo en Ecuador. Fuente: http://es.slideshare.net/roxanasilvach/presentacion-inclusion-19-022014

La distribución de votantes con discapacidad empadronados según el tipo de discapacidad es la siguiente:

PROVINCIA	PERSONAS CON DISCAPACIDAD	AUDITIVA	FÍSICA	INTELECTUAL	LENGUAJE	MENTAL	PSICOLÓGICA	VISUAL
AZUAY	21657	2218	12759	3261	245	7	560	2607
BOLÍVAR	5279	994	2192	965	130	3	165	830
CAÑAR	5802	766	2835	1115	152	4	263	667
CARCHI	4578	947	2112	718	57	2	211	531
CHIMBORAZO	11318	2429	5030	2362	123	1	163	1210
COTOPAXI	8290	1344	3768	1606	235	7	189	1141
EL ORO	14785	1370	7221	3678	133	9	697	1677
ESMERALDAS	9438	729	4929	1946	115	1	254	1464
GALÁPAGOS	268	34	140	43	1	0	13	37
GUAYAS	66274	7146	33987	13666	682	25	2633	8135
IMBABURA	8457	2075	3641	1359	108	2	317	955
LOJA	11229	1380	4749	2974	96	2	574	1454
LOS RÍOS	15231	1115	9047	2737	190	4	391	1747
MANABÍ	37258	3198	21018	4669	251	6	2795	5321
MORONA SANTIAGO	3219	283	1619	536	70	2	127	582
NAPO	2660	384	1285	463	58	1	59	410
ORELLANA	3390	351	1687	399	55	0	137	761
PASTAZA	1814	271	870	314	17	1	68	273
PICHINCHA	42342	6815	20409	7145	561	35	1993	5384
SANTA ELENA	6719	795	3759	1239	70	2	150	704
STO DGO TSÁCHILAS	8407	870	4630	1404	103	1	353	1046
SUCUMBÍOS	3701	411	1794	701	64	2	148	581
TUNGURAHUA	9398	1983	3990	2052	129	7	297	940
ZAMORA CHINCHIPE	2594	344	1246	556	40	1	86	321
TOTAL NACIONAL	**304108**	**38252**	**154717**	**55908**	**3685**	**125**	**12643**	**38778**

Personas con discapacidad a nivel provincial según tipo de discapacidad. Fuente: http://es.slideshare.net/roxanasilvach/estadisticas-del-registro-electoral-2014



Distribución de personas empadronadas con discapacidad para las elecciones de febrero de 2014.

De acuerdo a la figura anterior:

- La discapacidad física representa el 51%, las personas con esta discapacidad en el caso de no contar con sus extremidades superiores tendrán que ser asistidas por una persona de su confianza, dispuesto así con la Convención de los Derechos de las personas con Discapacidad y en el Reglamento para la participación de personas con discapacidad.
- El segundo tipo de discapacidad es la intelectual. Para los votantes con este tipo de discapacidad los tendrá que ser asistidas por una persona de su confianza.
- El tercer tipo de discapacidad es la auditiva, en este caso, el votante con esta condición puede realizar el proceso de sufragio solo, ya que esta discapacidad no le impide navegar por el software de votación.

- La cuarta discapacidad es la visual. Para votante con esta discapacidad se tendrán en cuenta en los requisitos y diseño, el uso de la comunicación por medio de braile y mensajes de audio para la interacción con el software de votación.
- Los 3 últimos tipos de discapacidades son la psicológica, de lenguaje y mental. En este tipo de discapacidades dependerá de la severidad, para que el votante si es su decisión realizar el proceso de votación asistido por alguien de su confianza.

ANEXO L: Historias de Usuario del Sistema de Votación Autenticación

<table>
<tr><th colspan="2">Historia de Usuario</th></tr>
<tr><td>Número: 1</td><td>Usuario: Votante</td></tr>
<tr><td colspan="2">Nombre historia: Autenticación del votante</td></tr>
<tr><td>Prioridad en negocio:
Alta</td><td>Riesgo en desarrollo:
Medio</td></tr>
<tr><td>Puntos estimados: 8</td><td>Iteración asignada: 1</td></tr>
<tr><td colspan="2">Responsables: Andrea Santacruz-Fernando Valenzuela</td></tr>
<tr><td colspan="2">Descripción:
Como votante necesito autenticarme en el software de votación con la finalidad de visualizar la papeleta de votación digital.

Criterios de Aceptación
• Escenario 1: Autenticación exitosa
Dado que el votante presenta su identificación y es validada en el sistema de autenticación en la JRV y no ha sufragado cuando ingresa el token físico a continuación se presenta la papeleta de votación digital y su nuevo número de identificación temporal.

• Escenario 2: Autenticación fallida
Dado que el votante presenta su identificación y es validada en el sistema de autenticación en la JRV y no ha sufragado cuando ingresa el token físico a continuación se presenta un mensaje indicando que ya emitió su voto.
• Escenario 3: Autenticación fallida
Dado que la JRV ingresa un número de cédula incorrecto cuando da clic en el botón “Validar” a continuación se presenta un mensaje indicando el número de cédula es incorrecto.
• Escenario 4: Autenticación fallida
Dado que el votante ingresa su número de cédula correcto y no pertenece a la JRV desde la cual está intentando autenticarse cuando da clic en el botón “Ingresar” a continuación se presenta un mensaje indicando que no pertenece a la JRV y le muestra el nombre del Recinto Electoral y el número de JRV correcta.</td></tr>
<tr><td colspan="2">Observaciones:
El número de identificación temporal dura 1 día.</td></tr>
</table>

El número de cédula tiene que ser validado al momento de dar clic en el botón “Ingresar” Durante esta actividad la interacción entre el sistema y el usuario tiene que ser visual y sonora.

Historia de Usuario	
Número: 2	**Usuario:** Votante
Nombre historia: Sufragio	
Prioridad en negocio: Alta	**Riesgo en desarrollo:** Medio
Puntos estimados: 8	**Iteración asignada: 1**
Responsables: Andrea Santacruz-Fernando Valenzuela	

Descripción:
Como votante *necesito* seleccionar los candidatos de mi preferencia en la papeleta de votación digital *con la finalidad de* para emitir mi voto.

Criterios de Aceptación

- ***Escenario 1: Voto válido***

Dado que el votante selecciona el número de candidatos permitidos *cuando* da clic en el botón “Enviar el voto” *a continuación* se presenta un mensaje solicitando confirmación para imprimir el voto.

- ***Escenario 2: Voto en blanco***

Dado que el votante selecciona el voto en blanco *cuando* da clic en el botón “Enviar el voto” *a continuación* se presenta un mensaje solicitando confirmación para imprimir el voto en blanco.

- ***Escenario 3: Voto nulo***

Dado que el votante selecciona el voto nulo *cuando* da clic en el botón “Enviar el voto” *a continuación* se presenta un mensaje solicitando confirmación para imprimir el voto nulo.

Observaciones:
El número de candidatos seleccionados debe ser menor o igual que el número de candidatos permitidos.
Durante esta actividad la interacción entre el sistema y el usuario tiene que ser visual y sonora.

<table>
<tr><th colspan="3">Historia de Usuario</th></tr>
<tr><td>Número: 3</td><td colspan="2">Usuario: Votante</td></tr>
<tr><td colspan="3">Nombre historia: Escrutinio del voto</td></tr>
<tr><td colspan="2">Prioridad en negocio:
Alta</td><td>Riesgo en desarrollo:
Medio</td></tr>
<tr><td colspan="2">Puntos estimados: 8</td><td>Iteración asignada: 1</td></tr>
<tr><td colspan="3">Responsables: Andrea Santacruz-Fernando Valenzuela</td></tr>
<tr><td colspan="3">Descripción:
Como votante necesito imprimir mi voto con la finalidad que sea contabilizado.

Criterios de Aceptación
• Escenario 1: Aceptación de la impresión del voto
Dado que el votante necesita confirmar el conteo de su voto cuando da clic en el botón “Aceptar la impresión” a continuación se imprime el voto y se presenta un mensaje indicando que el voto ha sido contado.
• Escenario 2: Rechazo de la impresión del voto
Dado que el votante necesita rechazar el conteo de su voto cuando da clic en el botón “Rechazar la impresión” a continuación se presenta un mensaje indicando que el voto ha sido destruido, permitiéndole repetir su voto.</td></tr>
<tr><td colspan="3">Observaciones:
El comprobante impreso del voto debe ser depositado en una urna tradicional.
Durante esta actividad la interacción entre el sistema y el usuario tiene que ser visual y sonora.</td></tr>
</table>

<table>
<tr><th colspan="3">Historia de Usuario</th></tr>
<tr><td>Número: 4</td><td colspan="2">Usuario: Publicador de resultados</td></tr>
<tr><td colspan="3">Nombre historia: Publicación de los resultados finales</td></tr>
<tr><td colspan="2">Prioridad en negocio:
Alta</td><td>Riesgo en desarrollo:
Medio</td></tr>
<tr><td colspan="2">Puntos estimados: 8</td><td>Iteración asignada: 1</td></tr>
<tr><td colspan="3">Responsables: Andrea Santacruz-Fernando Valenzuela</td></tr>
<tr><td colspan="3">Descripción:
Como publicador de los resultados necesito publicar los resultados finales del sufragio con la finalidad de dar a conocer los resultados a los votantes.

Criterios de Aceptación
• Escenario 1: Publicación de resultados
Dado que el publicador de resultados necesita presentar los resultados del sufragio cuando da clic en el botón “Generar resultados” a continuación los reportes de resultados son generados.</td></tr>
<tr><td colspan="3">Observaciones:</td></tr>
</table>

ANEXO M: Token Físico

Para sistemas de autenticación en los que se utilizan tokens físicos se puede optar por varias opciones, por ejemplo:

Tarjetas de banda magnética llamada a veces magstripe como abreviación de magnetic stripe es toda aquella banda oscura presente en tarjetas de crédito, abonos de transporte público o carnés personales que está compuesta por partículas ferromagnéticas incrustadas en una matriz de resina (generalmente epoxi) y que almacenan cierta cantidad de información mediante una codificación determinada que polariza dichas partículas. La banda magnética es grabada o leída mediante contacto físico pasándola a través de una cabeza lectora/escritora gracias al fenómeno de la inducción magnética. Fue inventada por IBM en 1960. [49]

Tarjetas con chip, tarjeta inteligente,smart card o tarjeta con circuito integrado (TCI), es cualquier tarjeta del tamaño del bolsillo con circuitos integrados, que permite la ejecución de cierta lógica programada. Aunque existe un diverso rango de aplicaciones, hay dos categorías principales de TCI. Las tarjetas de memoria contienen sólo componentes de memoria no volátil y posiblemente alguna lógica de seguridad. Las tarjetas microprocesadoras contienen memoria y microprocesadores. [50]

Tarjetas de proximidad magnética es el nombre genérico dado a la tarjeta inteligente "sin contacto" que se utiliza para el acceso seguro o como un sistema de pago. Se puede referir tanto a las viejas tarjetas de 125 kHz RFID como las nuevas tarjetas sin contacto que funcionan a 13,56 MHz, comúnmente conocidas como tarjeta inteligente sin contacto. Las tarjetas modernas de proximidad responden a la norma ISO 14443. Existe también el estándar ISO 15693 relativo a la llamada "tarjeta de vecindad". [51]

ANEXO N: Product Backlog

No. HDU	Id. Tarea	Tarea	Responsable	Prioridad	Estimación de Esfuerzo	Sprint
1	1	Diseñar los modelos de datos del Padrón Electoral, Papeleta Digital y Votos	Andrea Santacruz - Fernando Valenzuela	1	3	1
1	2	Definir las validaciones que deben ser aplicadas al votante.	Andrea Santacruz - Fernando Valenzuela	1	5	1
1	3	Diseñar las interfaces de usuario	Andrea Santacruz - Fernando Valenzuela	1	4	1
2	5	Definir las validaciones de cuándo un voto es válido, nulo y blanco.	Andrea Santacruz - Fernando Valenzuela	2	2	2
2	6	Definir el algoritmo de encriptación del voto.	Andrea Santacruz - Fernando Valenzuela	2	3	2
2	7	Diseñar las interfaces de usuario	Andrea Santacruz - Fernando Valenzuela	2	3	2
2	8	Definir las reglas	Andrea	2	3	2

		para determinar la validez del voto emitido para contabilizarlo.	Santacruz - Fernando Valenzuela			
3	9	Definir los algoritmos de desencriptación del voto.	Andrea Santacruz - Fernando Valenzuela	3	3	3
3	10	Definir los algoritmos para permutar el voto.	Andrea Santacruz - Fernando Valenzuela	3	5	3
3	11	Definir las reglas del procesamiento del voto para contabilizarlo.	Andrea Santacruz - Fernando Valenzuela	3	5	3
4	12	Definir los reportes necesarios para publicar los resultados del conteo de votos.	Andrea Santacruz - Fernando Valenzuela	4	5	4
4	13	Implementar los reportes de resultados del conteo de votos.	Andrea Santacruz - Fernando Valenzuela	4	5	4

ANEXO O: Cifrado RSA

RSA es un sistema criptográfico de cifrado de llave pública. [52] RSA es usado para encriptar y para firmar digitalmente. Este sistema se fundamenta en el producto de dos números primos grandes, elegidos al azar y protegidos en secreto.

La comunicación cifrada con RSA consiste en establecer una llave pública y otra privada. El emisor para a enviar un mensaje usa la llave pública del receptor para encriptar su mensaje. El receptor recibe el mensaje encriptado y lo desencripta usando su llave o clave privada. Los mensajes enviados se representan mediante números.

El certificado digital usado para la comunicación con RSA debe ser otorgado por una Autoridad de Certificación.

Funcionamiento de RSA

El votante envía su voto **M** en forma de un número **m.** La transformación del mensaje **M en m** se lo hace mediante un protocolo reversible conocido como padding scheme[22] o esquema de relleno. Y **m** tiene que ser menor que el número **n.** Posterior, se genera el mensaje cifrado c mediante la siguiente operación:

$c \equiv m^e \pmod n$, donde ***e*** es la clave pública del Servidor Mix.

Ahora el servidor receptor desencripta el mensaje en clave –**c-** mediante la siguiente operación inversa:

$m \equiv c^d \pmod n$, donde ***d*** es la clave privada que solo el Servidor Mix conoce.

El algoritmo de RSA se compone de tres fases: generación de llaves, cifrado y descifrado

Generación de llaves

[22] Mecanismos de llenado que introducen información irrelevante para mantener cierta seguridad sobre la privacidad del contenido y así ocultar la estructura de los datos estructura.

1. Cada participante de la comunicación elige dos números primos diferentes p y q. Los números p y q deben:
    - Ser elegidos de forma aleatoria por motivos de seguridad.
    - Tener una longitud similar en bits.
    - Se pueden hallar primos fácilmente mediante test de primalidad[23].
2. Se determina n = pq. Donde n es el módulo tanto para la llave pública como privada.
3. Se calcula φ(n) = (p-1) (q-1). Donde φ es la función de Euler[24].
4. Se selecciona un entero positivo **e** menor que φ(n) y que sean coprimos[25].

    - **e** es el exponente de la clave pública.
    - Al seleccionar **e** mediante una suma encadenada corta, el encriptado será más efectivo. Un exponente e muy pequeño -por ejemplo de un digito- puede ir en detrimento de la seguridad y así convertirse en una vulnerabilidad.

5. Se calcula un **d** a través de aritmética modular[26] y debe satisfacer la congruencia **e • d ≡ 1 (mod φ(n)).** Esto significa que **d** sea el multiplicador modular inverso[27] de **e mod φ(n)**.

    - Si φ(n) = (p-1) (q-1), entonces el multiplicador modular inverso es $\frac{1}{\mathrm{p}-1\ (q-1)}$. El cálculo se lo realiza empleando el algoritmo de Euclides extendido[28].
    - Finalmente **d** es el exponente de la llave privada.

[23] Dado un número de entrada n, no se puede verificar la hipótesis de un teorema. La conclusión de este teorema es que n es compuesto, entonces por lo tanto el número es primo.
[24] Si n es un número entero positivo, entonces φ(n) se define como el número de enteros positivos menores o iguales a n y coprimos con n.
[25]Si dos números enteros r y s no poseen ningún factor primo en común, es decir si únicamente tienen como divisor común 1 y -1
[26] Es un sistema aritmético para clases de equivalencia de números enteros llamadas clases de congruencia
[27] El multiplicador modular inverso de un entero n módulo p es un entero m tal que n-1 ≡ m (mod p)
[28] Permite hallar un máximo común divisor de dos números enteros a y b, y expresarlo como la mínima combinación lineal de esos números, es decir, hallar dos números enteros t y v tales que mcd(a,b)=a t+b v.

La llave pública es establecida por **(n, e)**, donde n es el módulo y e el exponente de encriptación. La llave privada es definida por **(n, d**), donde n es el módulo y d es el exponente de desencriptación.

Cifrado

Los servidores mix comunican su llave pública (n, e) al votante y guarda su llave privada en secreto.

Si el votante va a enviar un mensaje ***M*** al Servidor Mix, entonces debe transformar ***M*** en un número entero ***m*** menor que ***n.*** La transformación se realiza a través el protocolo de relleno reversible convenido previamente. Inmediatamente, el cálculo del texto cifrado ***c*** se computa mediante la operación:

$$c \equiv m^e (mod\ n)$$

Donde **n = p*q** y **e** es coprimo con **(p-1) (q-1)**.

Ahora el votante transmite el mensaje cifrado ***c*** a los servidores mix.

Descifrado

Los servidores mix pueden recuperar el número ***m*** usando ***c*** y el exponente ***d*** de su llave privada a través del cálculo:

$$m = c^d (mod\ n)$$

Donde **d** es un inverso de **e** módulo **(p-1) (q-1)**.

Cuando el servidor tiene **m**, puede obtener el mensaje original, es decir **M** invirtiendo el esquema de relleno.

Justificación:

$$c \equiv m^e (mod\ n)$$

Entonces:

$c^d \ mod\, n \ = (m^e)^d \ mod\, n \ = \ m^{1+k\ p-1\ \ q-1} \ \ mod\, n \ = \ \ m^{\ p-1\ \ q-1\ \ \ k}.m\ (mod\ n)$

Y se tiene:

$m^{\ p-1\ \ \ k\ q-1} \ = \ m\ (mod\ p)$ y $\ m^{\ q-1\ \ \ k\ p-1} \ = \ m\ (mod\ q)$

Considerando la función de Euler **φ(n) = (p-1) (q-1)** y como se ha elegido ***d*** y ***e*** se tiene **ed = 1 + k φ(n) = 1 + k (p-1) (1-q)**

Por tanto la función de Euler-Fermat

$m^{\varphi(n)} = \ 1 \ \ mod\, n \ \ \rightarrow \ \ m^{\ p-1\ \ q-1\ \ \ k} \equiv 1\, mod\, n$

Entonces se obtiene.

$$c^d \ mod\, n \ = 1 * mod\ (n) = m$$

Donde 0 <= M <= n.

Este cálculo demuestra que se obtiene el mensaje original:

$$m \equiv c^d (mod\ n)$$

Se recomienda que en la implementación de RSA usar un esquema de relleno con el fin de producir textos encriptados seguros a partir del valor de ***M***.

ANEXO P: Firmas Ciegas [53]

El esquema de Firmas Ciegas es un tipo especial de firma digital debido a que no se conoce el contenido a firmar.

La firma a ciega se caracteriza porque la entidad firmante no puede obtener conocimiento alguno sobre el documento que está firmando. Posteriormente, la firma obtenida podrá ser verificada como válida por el propio firmante o por cualquier entidad que disponga de la información pertinente para ello. Sin embargo, el firmante no puede establecer ninguna relación con las circunstancias en que realizó la firma

El funcionamiento de este esquema está compuesto por tres pasos:

1. Proceso de Ocultación: el votante envía su voto dentro de un sobre cerrado de papel carbón y junto con su identificador a la autoridad. Esta autoridad comprueba la identidad del votante y en función de esto, decidirá firmar o no el voto. La autoridad firma en la superficie del sobre sin conocer su contenido. Esta firma faculta al votante para emitir o no su voto.
2. Proceso de Firma: la autoridad coloca su rúbrica en la superficie del sobre sin abrirlo. El papel carbón aplica la firma de la autoridad al voto contenido en el sobre. El sobre firmado es devuelto al votante.
3. Proceso de Desocultación: el votante extrae su voto del sobre en privado. El voto se encuentra firmado por la autoridad, aunque esta no conoce su contenido, únicamente vio el sobre que lo contenía.

De manera técnica, el sistema de firma ciega con RSA funciona de la siguiente manera:

Sean:

- (n_{sfc}, e_{sfc}) la clave pública del servidor de firmas ciegas y d_{sfc} su clave privada.
- M el voto encriptado con las claves públicas de los servidores mix.
- k coeficiente de ocultamiento.

Proceso:

1. El votante conoce las claves públicas del Servidor de Firma Ciega. (SFC: n_{sfc}, e_{sfc})
2. El votante crea un mensaje ***M***.
3. El votante elige un coeficiente de ocultamiento ***k***, de forma que se cumpla: $mcd\ (k, n_{sfc}) = 1$.
4. El votante calcula $k^{-1} = inv\ (k, n_{sfc})$.
5. El votante enmascara su mensaje aplicando la siguiente operación: $t_{votante} = M * k^{e}_{sfc}\ mod\ n_{sfc}$ y lo envía al servidor de firma ciega.
6. El servidor de firma ciega valida la identidad del votante y en caso de verificarla con éxito, firma de la siguiente manera el mensaje recibido: $T_{SFC} = t_{votante}{}^{d}_{sfc}\ mod\ n_{sfc}$ y lo envía al votante.
7. El votante quita la máscara haciendo $s = T_{SFC} * inv\ (k, n_{sfc})\ mod\ n_{sfc}$. Y el votante obtiene $M^{d}_{sfc}\ mod\ n_{sfc}$, es decir, la firma de SFC sobre el voto ***M***.

La autoridad no puede conocer el contenido del mensaje ***M*** a partir de M_{ciego}. [29] [30]

Una vez recibido el voto firmado, la firma del voto es verificada por un servidor Validador. El servidor Validador para realizar la verificación emplea el siguiente algoritmo.

Este algoritmo tiene como entrada m, s, k_v y como salida el valor ***verdadero*** o ***falso***.

v(s) = { Válida / Rechazada }

Sea:

m es el mensaje firmado,

s la firma ciega para el mensaje m,

[29] http://blogs.politicadigital.com.mx/firma-electronica/?p=130
[30] http://congreso.us.es/cedya2007/actas/textos/144.pdf

$\mathbf{k_v}$ la llave pública de la entidad firmante.

La verificación de la firma ciega se realiza de la siguiente manera:

Entrada:

- firma **s**,
- mensaje **m**,
- llave pública del signatario o firmante ($\mathbf{n_{sfc}}$, $\mathbf{e_{sfc}}$).

Algoritmo:

1. h = H(m)
2. h' = s^e mod $\mathbf{e_{sfc}}$
3. **Si** h = h' **entonces**

    Retorna Válida **ó** Retorna Rechazada

Salida:

- {Válida / Rechazada}.

La firma ciega puede ser verificada por cualquier entidad ya que este algoritmo es público. La firma ciega es válida únicamente si la llave pública del signatario es usada en el proceso de verificación.

Respecto a la seguridad:

- La verificación de la firma ciega utiliza una función Hash para evitar la falsificación del mensaje por parte del usuario.
- La entidad firmante no puede obtener el mensaje original a partir del mensaje oculto debido al factor de opacidad.

EL votante al obtener la firma ciega retira el factor de opacidad, la entidad firmante no tiene forma de relacionar el mensaje oculto con el mensaje original

ANEXO Q: Redes de mezcla de Chaum [54]

La red de mezcla de Chaum está formada por varios servidores de mezla y cada uno posee su propio par de llaves (kn, kd) en algún esquema de cifrado de llave pública. Las llaves públicas de cada servidor son conocidas por todos los remitentes. Entonces, el remitente genera su mensaje encriptado con las llaves públicas de los servidores de mezcla y envía el mensaje a S1:

$$c_{i1} = Enc \;\; k_{e1}, Enc \;\; k_{e2}, \dots Enc \;\; k_{en}, Enc \;\; k_e, m_i \quad \dots \quad ,$$

El primer servidor de la red de mezcla de Chaum S1 recibe el conjunto de mensajes. S1 descifra cada mensaje con su propia llave privada, permuta aleatoriamente el conjunto y pasa el resultado al siguiente servidor Sj+1. Este proceso se lo repite hasta llegar al servidor Sn-1. El último servidor de mezcla Sn transmite su salida a D, este último descifra cada mensaje con su llave privada obteniendo los mensajes del conjunto en orden aleatorio.

Este esquema funciona cifrando el mensaje original por capas. Cada capa corresponde a cada servidor de mezcla más el destinatario final. Y cada capa de encriptación debe aplicarse en orden inverso.

La consecuencia de este esquema es que cada mensaje deberá pasar por todos los servidores de mezcla antes de ser leído por el destinatario. Un mensaje no puede saltarse un servidor de mezcla.

ANEXO R: Algoritmo de Permutación

El algoritmo de permutación consiste en:

El servidor mix n recolecta 10 votos en un orden específico.

El servidor genera 10 números aleatorios y asigna un número a cada voto.

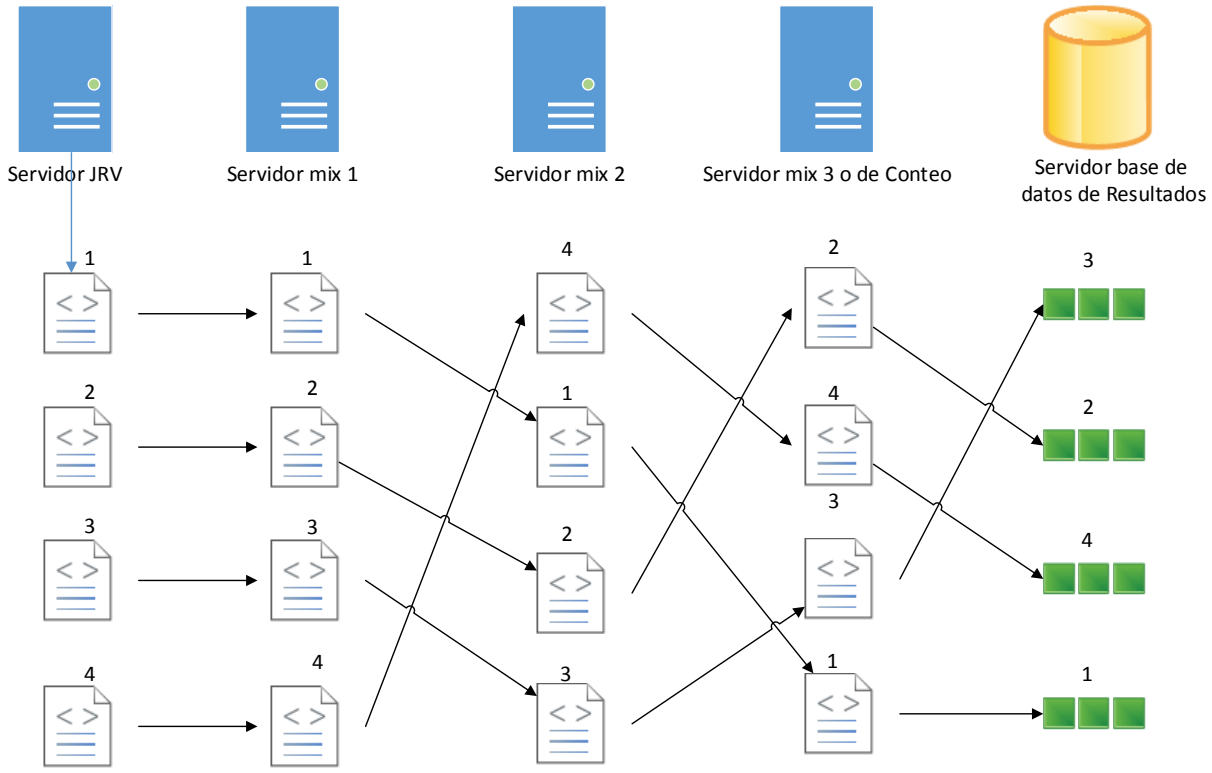
El servidor ordena los votos en una lista de acuerdo a los números asignados.

El servidor genera dos nuevos número aleatorio a y b. Estos números no pueden ser iguales

Si a es mayor que b, entonces el servidor mix n envía los votos al siguiente servidor iniciando por el último voto de la lista.

Si a es menor que b, entonces el servidor mix n envía los votos al siguiente servidor iniciando por el primer voto de la lista.

En la siguiente figura se representa el orden de envío de los votos.



ANEXO S: Protocolo SSL/TLS [55]

La arquitectura de SSL/TLS está compuesta por dos niveles de protocolos:

Primer nivel:

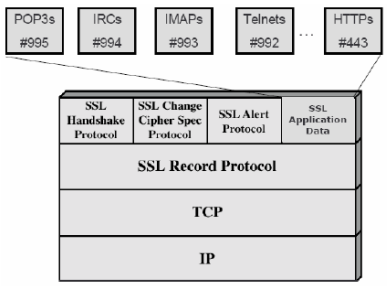
Este nivel está compuesto por un protocolo que se encarga de construir el canal seguro.

- Record Protocol: encapsula los protocolos de alto nivel y proporciona a aplicaciones http, ftp, telnet, entre otros, servicios de seguridad básicos para formar un canal de comunicación seguro.

Segundo nivel:

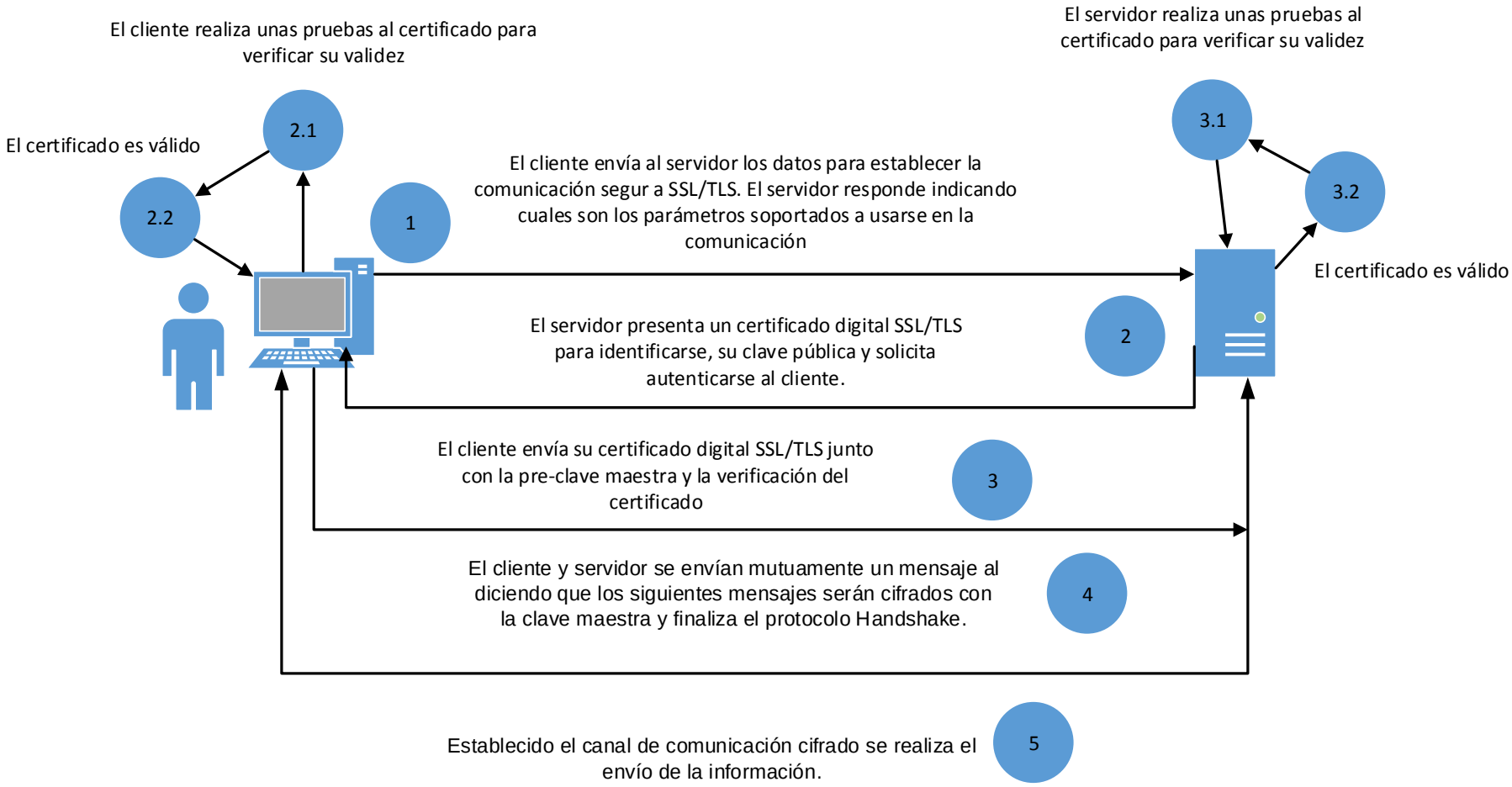
Este nivel está compuesto por tres protocolos de gestión de intercambios SSL.

- Handshake Protocol: administra el establecimiento de los algoritmos de cifrado y la autenticación entre cliente y servidor. Define las claves de sesión utilizadas para encriptar.
- Change Cipher Spec Protocol: es un mensaje de un byte para informar cambios en la estrategia de encriptación.
- Alert Protocol: señaliza alertas y errores en la sesión establecida.



Protocolos SSL/TSL. Fuente: http://goo.gl/fTghFg pág. 14

Estos 4 protocolos interactúan para establecer un canal de comunicación encriptado, tal como se muestra en la siguiente figura:



Funcionamiento general de una VPN SSL/TLS.

El protocolo SSL/TLS consta de cuatro fases para negociar los parámetros de una sesión:

Fase 1

Esta fase establece las siguientes capacidades de seguridad, como: versión de protocolo, identificador de sesión, suite de cifrado, método de compresión y números aleatorios iniciales.

La fase inicia cuando el cliente envía al servidor los parámetros para establecer una comunicación segura con SSL/TLS. La información es enviada a través del protocolo Handshake. El servidor decide si soporta esos parámetros que el cliente le ha enviado y se lo comunica.

El cliente envía los parámetros al servidor empleando el mensaje “Client_hello”. Este mensaje contiene los siguientes parámetros a negociar entre cliente y servidor:

- Versión: número de la versión más alta de SSL/TLS que el cliente soporta.
- Valor Aleatorio: número aleatorio inicial del cliente.
- Identificador de Sesión: número de identificación de la sesión. Si el valor del identificador es diferente de cero, entonces se creará una nueva conexión dentro de esa sesión y se actualizará los parámetros de la conexión existente. Si el valor del identificador es cero, entonces se creará una nueva conexión en una nueva sesión y se actualizarán los valores tanto de la sesión como de la conexión.
- Suite de Cifrado: este campo contiene una lista de suites de cifrado soportados por el cliente. Esta suite de cifrado debe contener el algoritmo de intercambio de claves, el algoritmo de cifrado, el tipo de cifrado, el tamaño del Hash, parámetros para calcular claves, tamaño de vector de inicialización.
- Método de Compresión: el método o métodos que soporta el cliente para comprimir los datos de aplicación.

El servidor envía la respuesta al cliente empleando el mensaje “Server_Hello”. Este mensaje contiene los parámetros seleccionados por el servidor para establecer una comunicación segura con SSL/TLS, estos son:

- Versión: versión del protocolo SSL/TLS elegida por el servidor. Esta versión debe ser soportada por el cliente y por el servidor.
- Valor aleatorio: número aleatorio inicial del servidor.
- Identificador de Sesión: número de identificación de la sesión. Si el identificador de sesión del cliente recibido por el servidor es igual a cero, entonces el identificador de sesión del servidor contendrá un valor distinto de cero, para indicar que se ha creado una nueva sesión. Si el identificador de sesión del cliente recibido por el servidor es diferente de cero, entonces el servidor comprobará en su caché si guarda información sobre esa conexión, y si es así y se puede crear una nueva conexión responde con el mismo identificador de sesión que el del cliente.
- Suite de Cifrado: este campo contiene la suite de cifrado soportada por el cliente y seleccionada por el servidor. Esta suite de cifrado deberán contener el algoritmo de intercambio de claves, el algoritmo de cifrado, el tipo de cifrado, el tamaño del Hash, parámetros para calcular claves, tamaño de vector de inicialización.
- Método de Compresión: el método seleccionado por el servidor que soporta el cliente para comprimir los datos de aplicación.

Fase 2

Esta fase estable el certificado de autenticación del servidor, intercambio de clave y solicitud de certificado de autenticación al cliente. Los mensajes enviados por el servidor en esta fase son “Certificate”, Server_Key_Exchange”, “Certificate_Request” y “Server_Hello_Done”, siendo este último el único mensaje que el servidor está obligado a enviar al cliente. A continuación se describe cada uno de estos mensajes:

- “Certificate”: contiene el certificado X.509 del servidor firmado por la Autoridad Certificadora (CA). El certificado permite autenticarse ante el cliente y contiene la clave pública del servidor. La clave pública será utilizada para intercambiar las claves de sesión.
- “Server_Key_Exchange”: contiene la clave pública del servidor para el intercambio de claves. Este mensaje no se utilizará debido a que el intercambio de claves se realiza mediante RSA.
- “Certficate_Request”: solicita al cliente autenticarse. El servidor solicita al cliente un determinado tipo de certificado y una lista de CA aceptables.
- “Server_Hello_Done”: pone fin a los mensajes de la fase 2 asociados al servidor. Este mensaje no envía ningún parámetro.

La clave pública del servidor es enviada al cliente mediante el protocolo RSA. El cliente usa esta clave para cifrar la información necesaria para generar una clave secreta común y la devuelva al servidor. De este modo, el servidor la descifrará con la clave privada y podrá generar la misma clave común.

Fase 3

Esta fase permite al cliente autenticarse ante el servidor. El cliente envía su certificado, el intercambio de clave y la verificación del certificado del servidor. El cliente debe responder con su certificado X.509 o con un mensaje de alerta “No_Certificate” indicando que no lo tiene.

Los mensajes enviados en esta fase del protocolo Handshake por el cliente son: “Certificate”, “Client_Key_Exchange” y “Certificate_Verify”. A continuación una breve descripción de cada mensaje:

- “Certificate”: envía el certificado X.509 del cliente para autenticarse al servidor.
- “Cliente_Key_Exchange”: el cliente envía al servidor una clave secreta o número aleatorio generado, llamada clave pre-master. La pre-clave es de 48 bytes y es cifrada con la clave pública del servidor.

- “Certificate_Verify”: verifica que el cliente posee la clave privada en concordancia con el certificado del cliente. Este mensaje se envía junto al anterior y consta de una firma Hash que abarca los mensajes anteriores. El cifrado se realiza con la clave privada del cliente.

El servidor usa su clave privada para obtener la clave pre-master. El cliente y el servidor utilizan la clave pre-master para calcular la clave maestra, las claves de sesión y las claves MAC.

Fase 4

Esta fase permite que un cliente envíe un mensaje al servidor para señalar que los siguientes mensajes serán cifrados con la clave maestra. El cliente también envía un mensaje encriptado al servidor para comunicar que la parte del cliente del protocolo Handshake ha finalizado.

El servidor responde con un mensaje al cliente diciendo que los mensajes serán cifrados con la clave maestra. Por último, el servidor envía un mensaje encriptado al cliente indicando que su parte del protocolo Handshake ha finalizado.

Esta fase consta de dos mensajes y son iguales tanto para el cliente como para el servidor:

- “Change_Cipher_Spec”: sirve para dar como concluido el intercambio, pasando del estado pendiente al estado operativo.
- “Finished”: sirve para finalizar el protocolo Handshake y para comenzar a transmitir los datos de aplicación protegidos con las claves y algoritmos negociados.

Fase 5

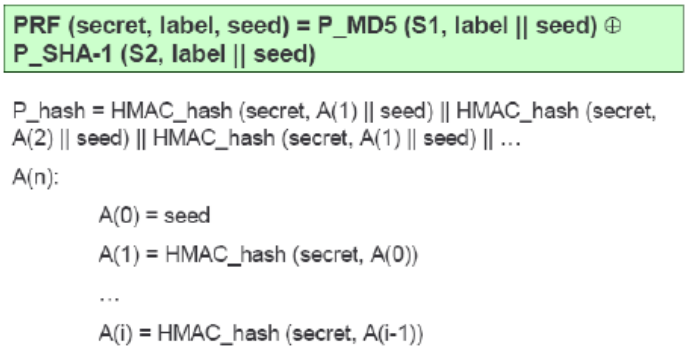
En esta fase se inicia el intercambio de mensajes encriptados entre el servidor y cliente.

Cálculo de la clave maestra

El tamaño de esta clave maestra es de 48 bytes y el uso de esta clave es válido para una única sesión. El cálculo de esta clave maestra se realiza en dos pasos:

1. Cliente genera la clave pre-master –Kprevia- y se la envía cifrada al servidor mediante el algoritmo de intercambio de claves RSA.
2. Se realiza el cálculo de la clave maestra por parte del cliente y del servidor. Para el cálculo de dicha clave se emplea una función pseudo aleatoria o función PRF[31] que tiene como función la expansión de dicha clave maestra.

La clave maestra se genera a partir de una clave pre-master. Para el cálculo de dicha clave maestra en TLS versión 1 se realizan las siguientes operaciones:



Cálculo de la clave maestra en TLS versión 1. Fuente: http://goo.gl/OxLVTh Pág. 24

La clave maestra también es reutilizada para calcular:

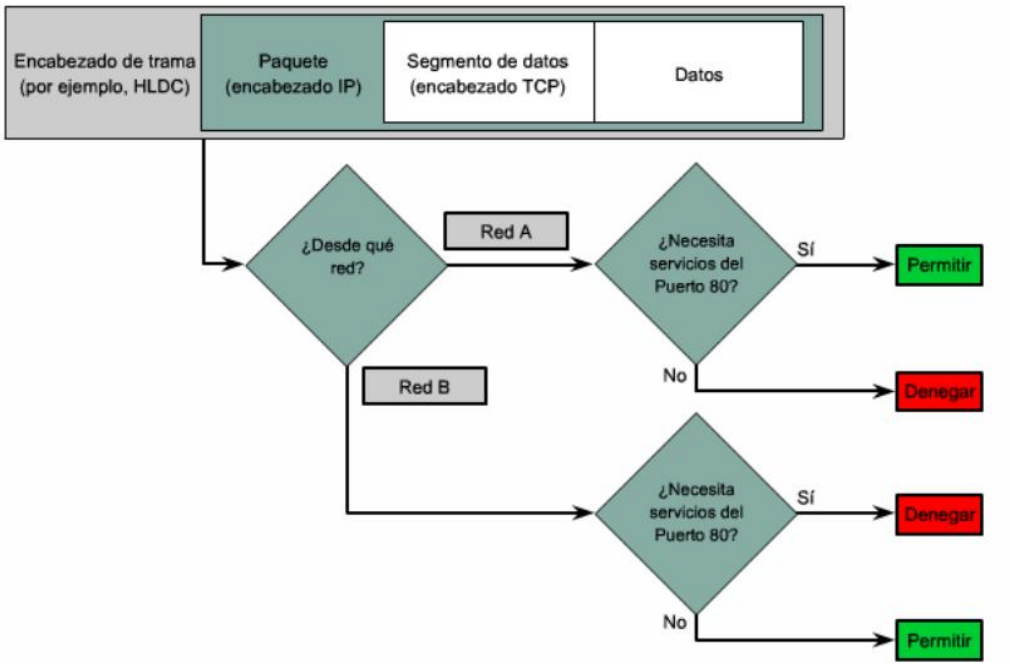
- Llave secreta MAC de Escritura del Servidor.
- Llave secreta MAC de Escritura del Cliente.
- Llave de escritura del Servidor.
- Llave de escritura del Cliente.
- Vector de Inicialización (IV) del Cliente y Servidor.

[31] Pseudos Random Function

ANEXO T: ACLs [56]

Una ACL es una lista secuencial de sentencias de permiso o denegación que se aplican a direcciones o protocolos de capa superior. Las ACL controlan el tráfico de entrada o de salida de la red a través de estas sentencias. La sentencia del ACL verifica el origen del paquete de datos y si está permitido acceder al puerto que solicita. Si la sentencia determina que puede acceder, entonces el paquete es enviado al puerto que solicitó caso contrario se rechaza.

El funcionamiento de una ACL se visualiza en la siguiente figura.



Esquema de funcionamiento de ACLs. Fuente: http://goo.gl/1ukk5K

ANEXO U: Replicación Asíncrona Unidireccional

La replicación unidireccional consiste en disponer de dos servidores. Servidor maestro o primario, este acepta todas las operaciones de escritura provenientes del sistema cliente. El servidor esclavo o secundario ejecuta las mismas operaciones sobre su conjunto de datos. Esta estrategia permite tener la misma información en los diferentes servidores.

Funcionamiento:

- El servidor maestro escribe todas las actualizaciones en un fichero de log binario. Este servidor mantiene un índice de los ficheros para rastrear las rotaciones de logs.
- El servidor esclavo detecta cuando sucede algún cambio en el log binario del maestro, y ejecutan estos cambios en sus tablas. [57] Para ejecutar los cambios se basa en el log binario.

La principal ventaja de esta estrategia de replicación es que los datos viajan en un solo sentido: Maestro-Esclavo. Por lo que las operaciones de escritura son aceptadas sólo en un lugar, el servidor maestro; y las operaciones de consulta se hacen sobre el servidor esclavo. De esta manera las modificaciones sobre las réplicas fluyan de una sola manera. [58]