UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

MODELACIÓN Y ANÁLISIS DEL SISTEMA CHILENO DE VOTACIÓN

TESIS PARA OPTAR AL GRADO DE
MAGÍSTER EN CIENCIAS, MENCIÓN COMPUTACIÓN

MEMORIA PARA OPTAR AL TÍTULO DE INGENIERO CIVIL EN COMPUTACIÓN

JUAN ANTONIO ROJAS ESPEJO

PROFESOR GUÍA:
ALEJANDRO HEVIA ANGULO

MIEMBROS DE LA COMISIÓN:
TOMAS BARROS ARANCIBIA
PATRICIO POBLETE OLIVARES
PEDRO PINACHO DAVIDSON

Este trabajo ha sido parcialmente financiado por CONICYT y NIST

SANTIAGO DE CHILE
2020

Resumen

Este trabajo se centra en el sistema de votación chileno, un proceso complejo con el que se eligen los representantes políticos del país. En particular el trabajo se centra en los distintos procesos que conforman las elecciones y cómo éstos permiten obtener una elección correcta, es decir, que sus resultados muestren correctamente las intenciones de que los votantes tenían al momento de votar.

La motivación para realizar este análisis viene de las últimas elecciones y la contingencia social, en donde se ha sugerido implementar sistemas de votación electrónica para aumentar la participación social. Sin embargo, en muchos otros países se han implementado de forma abrupta sistemas electrónicos sin haberlos probado antes adecuadamente, y sin haber estudiado sus ventajas y desventajas, llevando a cuestionamientos a la pertinencia del cambio e incluso a la legitimidad de las elecciones hechas con el nuevo sistema.

Esta tesis realiza un estudio del proceso actual de votación, para evaluar su seguridad y posibles mejoras a éste, para ver qué partes podrían mejorarse con tecnología, antes de dar un salto a sistemas de votación electrónica.

En particular, este trabajo incluye un modelo distribuido de tres subsistemas de la votación chilena. El primero corresponde a la elección de los vocales de mesa (los funcionarios que velan por la correcta realización de las votaciones el día de las elecciones), el segundo al proceso de manejo de información durante el día de las elecciones, el cual considera desde la captura de las intenciones de los votantes a los votos al conteo público, a las actas de votación y los sistemas de envío de información; y el tercero al conjunto de los procesos de escrutinio finales, donde se verifica la correctitud de los resultados reportados el día de la elección.

Mediante un análisis global de distintos ataques a las distintas fases de las votaciones estudiadas, y de una simulación realizada para evaluar el efecto cuantitativo de distintos tipos de ataque a las votaciones, logramos tener una visión constructiva de las distintas amenazas a las que se ve expuesto el actual sistema de votación chileno, lo cual permite evaluar las fortalezas y debilidades del actual sistema de votación chileno, requisito indispensable antes de considerar la implementación de cualquier forma de voto electrónico.

Finalmente se propone el uso de nuevas tecnologías para mitigar los posibles ataques encontrados a las votaciones, con medidas como el uso del Faro de Aleatoriedad de Random UChile para la elección de vocales de mesa, y el uso de una auditoría estadística posterior a las elecciones en el país.

Agradecimientos

Quiero agradecer a todas las personas que me apoyaron en este proceso: a mi pareja Jessica, a mis amigos, en especial al grupo "1306": Garo, Ignacio, Javier, Joaquín, José Carlos, Leopoldo, Sebastián, y Vicente; y al grupo "Los Cracks": Américo, Belisario, Gabriel, Javier, Joaquín, Nicolás, Rodrigo, y Sergio; a mis padres María Antonieta y Juan, a mi abuela María Antonieta y finalmente a don Juan Gálvez.

También agradezco los financiamentos de NIST con el proyecto 60NANB18D21, y a CONICYT con la beca CONICYT-PFCHA/MagísterNacional/2018-22181865.

Tabla de Contenido

Índice de Tablas

Índice de Ilustraciones

Capítulo 1

Introducción

1.1. Contexto

Las elecciones populares son el pilar fundamental de la democracia moderna, con ellas se eligen a los representantes de un país y es por esto que es necesario que los votantes puedan ejercer el derecho a voto sin problemas y que los resultados reflejen sus intenciones. En particular, la seguridad de las elecciones es importante puesto que el resultado pudiera ser imposible de corregir en caso de ser alterado. De hecho, comprobar cuál era la intención original de los votantes es difícil o, en muchos casos, imposible. Por lo tanto se debe asegurar en la mayor medida posible que el sistema sea resistente a ataques.

Tras las últimas elecciones en Chile y la contingencia social de fines del 2019, han surgido voces a favor de implementar un sistema de votación electrónica en el país para reemplazar el actual sistema de voto en papel, principalmente para aumentar los niveles de participación de la población, ya sea mediante sistemas de votación remotos para que la gente no deba salir de sus casas, o con sistemas electrónicos presenciales, que traen otros beneficios como mayor disponibilidad de idiomas, poder agregar preguntas complejas y permitir a la población votar en cualquier local de votación, en vez del que se le asigna con anterioridad.

Otros países ya han hecho la transición desde votación con papel y lápiz a votación electrónica. En Estados Unidos, luego de un escándalo en las votaciones presidenciales del año 2000 atribuido al tipo de papeletas usadas, tarjetas perforables, múltiples sistemas usados por décadas se desecharon para ser reemplazados por sistemas electrónicos que sustituyeron rápidamente al procedimiento en papel. Sin embargo, estos sistemas no fueron probados correctamente antes de usarse, lo que llevó a fallas, cuestionamientos y muchos años de investigación tanto de análisis de seguridad de los sistemas existentes, como de planteamientos de nuevos sistemas de votación en reemplazo de los ya en funcionamiento. Finalmente, se demostró que la seguridad de varios de estos sistemas era frecuentemente deficiente [15] y, en casos, irreparable sin un cambio en la arquitectura de la solución [12].

Los problemas que tuvieron tanto el método de votación en papel de Estados Unidos como muchos de los métodos de votación electrónica implementados posteriormente se pueden sintetizar con una frase: no eran capaces de garantizar una votación correcta, es decir, una

votación cuyos resultados coinciden con las preferencias de la población.

Un resultado de este proceso fue que los sistemas de votación electrónica fueron analizados cuidadosa y profundamente en términos de seguridad. Nada impide realizar este tipo de análisis para el sistema chileno *en papel*. El sistema de votación chileno actual corresponde a un sistema complejo, con muchos participantes que podrían tomar el papel de adversarios en el sistema, intentando alterar el flujo de información a lo largo del proceso.

Es posible que el día de mañana busquemos cambiar parte del sistema de votación actual chileno por una variante electrónica. Antes de eso, es deseable tener un análisis constructivo que evalúe cualitativa y cuantitativamente la seguridad de cada etapa del proceso de votación en uso, para así saber qué componentes son seguras y cuáles podrían tener potenciales cambios, para lograr mejorar efectivamente el sistema y evitar reemplazar partes que ya funcionan perfectamente sólo por querer usar más tecnología.

1.2. Problema a Resolver

Se pretende investigar el funcionamiento del sistema de votación chileno, enfocándose principalmente en:

- La selección de vocales de mesa, proceso que se realiza con sorteos a lo largo del país.
- El desarrollo de la votación durante el día de las elecciones, focalizado principalmente en la operación de toda la arquitectura computacional para la transmisión de datos y la replicación de información.
- El escrutinio posterior a las elecciones, donde se comprueba que la información entregada en el conteo preliminar sea correcta.

Para modelar todo el proceso se propone usar técnicas de sistemas distribuidos [28]. En particular analizaremos la seguridad de cada una de las partes para determinar qué componentes operan correctamente y cuáles podrían mejorarse mediante el uso de sistemas computacionales. Entre las principales preguntas a resolver están:

- ¿Es este proceso de votación modelable como un modelo distribuido? En particular, ¿es posible modelar el sistema en términos de un conjunto de participantes (algunos posiblemente maliciosos) conectados por líneas de comunicación como en un sistema distribuido?
- ¿Qué tan seguras son las partes electrónicas del proceso?
- ¿Son algunas partes del proceso mejorables con sistemas computacionales?
- ¿Qué tan fácil es tener un actor malicioso en el sistema?
- ¿Qué consecuencias puede provocar un actor malicioso, o un grupo organizado de éstos, en el resultado?
- ¿Es posible encontrar rastros de la presencia de un actor malicioso una vez que ya alteró los resultados?

Además se pretende identificar los supuestos bajo los cuales el sistema actual opera, y los supuestos necesarios para que el sistema de votación sea robusto y seguro.

1.3. Hipótesis

Es factible usar técnicas de sistemas distribuidos para modelar el proceso de votación chileno, y este modelo permite analizar las características de seguridad de las distintas partes involucradas en el sistema.

1.4. Objetivos

Objetivos generales

Crear un modelo de las distintas partes del proceso de votación chilena y usar este modelo para analizarlo en busca de posibles mejoras.

Objetivos específicos

- Modelar el proceso de selección de vocales de mesa, transmisión de datos y recuento de votos.
- Identificar las distintas fases de los procesos.
- Identificar actores involucrados en cada fase.
- Modelar el flujo de información de cada proceso.
- Encontrar los supuestos de comunicación de cada etapa.
- Analizar cada una de las partes descritas anteriormente.
- Explorar mejoras para el sistema actual a partir del análisis anterior.

1.5. Metodología

La metodología usada en este trabajo fue la siguiente:

1. Realizar un estudio de bibliografía pertinente a las técnicas a utilizar para el análisis.
2. Realizar un estudio de información públicamente disponible sobre el proceso de selección de vocales de mesa, el proceso de transmisión de resultados en las elecciones y el proceso de recuento posterior a las elecciones.
3. Realizar entrevistas con personal del Servicio Electoral para saber detalles del procedimiento mencionado en los puntos anteriores.
4. Realizar un modelo de los tres procesos anteriormente señalados.
5. Usando los modelos anteriores, analizar los procesos para encontrar posibles fallas.
6. De acuerdo a lo anterior, explorar posibles nuevos sistemas o procesos que solucionen o mitiguen las falencias potencialmente encontradas.

1.6. Resultados Esperados

Los resultados esperados como producto de este trabajo son:

- Modelo de elecciones chilenas que pueda ser potencialmente aplicado a otros países con votaciones en papel para evaluar posibles ataques.
- Informe a entregar al Servicio Electoral, con evaluación final de la seguridad de las elecciones y posibles mejoras al modelo actual.

1.7. Estructura de la Tesis

El resto del trabajo está estructurado como sigue:

1. **Capítulo 2: Marco Teórico**: Aquí se exploran trabajos relacionados al contenido de la tesis. Luego se explican conceptos básicos de las elecciones en Chile, y conceptos relevantes para este trabajo como lo son los sistemas distribuidos.
2. **Capítulo 3: Elección de Vocales de Mesa**: En este capítulo se describen en detalle como se realiza la selección de vocales de mesa a lo largo del país. También se describen posibles ataques al proceso de selección de vocales.
3. **Capítulo 4: Día de Votación**: Aquí se describe todo el proceso de cómo se realizan las votaciones, y los procesos asociados que se realizan el mismo día, junto a posibles ataques a todos estos procesos.
4. **Capítulo 5: Simulación de una Elección**: En este capítulo se describe una simulación realizada para evaluar el efecto que tienen distintos ataques y actores maliciosos en los procesos descritos en los dos capítulos anteriores. Posteriormente se muestran los resultados de esta simulación y un análisis de los resultados obtenidos.
5. **Capítulo 6: Escrutinio Posterior**: Aquí se describe el proceso realizado el día posterior a las elecciones, donde se comprueba la correctitud de los resultados obtenidos el día anterior. También se describen posibles ataques a este proceso.
6. **Capítulo 7: Tribunal Calificador de Elecciones**: Este capítulo describe el proceso final de las elecciones, donde se califica la correctitud de los resultados de las elecciones, revisando el proceso del capítulo anterior, junto a los reclamos realizados por los candidatos. Se describen posibles ataques a este proceso.
7. **Capítulo 8: Análisis Global**: Aquí se analizan todos los ataques descritos en los capítulos anteriores, evaluando la capacidad que tiene el mismo proceso de elecciones para evitar o detectar los ataques descritos, y proponiendo nuevas medidas cuando el sistema actual no permite detectar algunos ataques.
8. **Capítulo 9: Nuevas Mitigaciones a Ataques**: En este capítulo se describe el uso del Faro de Aleatoriedad para la selección de vocales, junto a una simulación y su análisis. También se describe la Auditoría Estadística, que permite comprobar la correctitud de un conteo de votos.

1.8. Contribuciones de este Trabajo

A través del estudio de las distintas etapas del proceso de elecciones en Chile, este trabajo logra identificar posibles ataques en cada una de las etapas de las elecciones.

Luego, con la ayuda de una simulación de las elecciones, se cuantifica el efecto de estos ataques, para poder evaluar el riesgo que posee cada parte del proceso. Además se simula

con datos reales de una elección, para poder encontrar el efecto real que hubiera tenido dicho ataque en una elección anterior.

Finalmente, mediante el análisis de los ataques descritos y sus efectos, se proponen distintas medidas para mitigar los efectos de los ataques estudiados, estudiando con mayor profundidad dos de las medidas propuestas: el Faro de Aleatoriedad y la Auditoría Estadística.

Capítulo 2

Marco Teórico

2.1. Estado del Arte

En esta sección presentamos la situación previa en términos de investigación en modelos para sistemas de votación de escala nacional.

En las últimas décadas, la comunidad científica se ha centrado en analizar los sistemas de votación electrónica creados para distintos países del mundo, encontrando variados problemas de seguridad en éstos. Por ejemplo, el análisis de la máquina AccuVote-TS de DieBold [12, 15], utilizado en las elecciones de 2006 en USA, evidenció problemas de seguridad que permitían a un actor malicioso inyectarle software para cambiar votos de una máquina en segundos. Otro caso es el de Estonia, donde múltiples vulnerabilidades fueron expuestas [26], incluyendo contraseñas expuestas en oficinas que fueron capturadas por videos oficiales. Estas deficiencias, han motivado el desarrollo de nuevos sistemas de votación electrónica utilizando técnicas criptográficas, como *Code Voting*, *Homomorphic Cryptosystems* y *Shuffles* [18]. Lamentablente éstos no sólo fallan en modelar el sistema de votación en su totalidad y modelan sólo una parte específica (la componente criptográfica), sino que no cubren el caso de votaciones clásicas hechas en papel. Una excepción es el análisis del sistema de Israel explicado a continuación.

2.1.1. Análisis al sistema de Israel

A diferencia de los sistemas electrónicos mencionados anteriormente, el sistema de votación de Israel es realizado completamente en base al papel. Sin embargo, Ashur et al. [5] mostraron que es posible averiguar el voto de una persona simplemente sabiendo cuando votó y teniendo acceso a su mesa de votación. Este tipo de ataque supone el uso de un tipo de papeleta de votación específica única de Israel, donde las distintas preferencias ya están pre-impresas en distintas opciones de voto y sólo se tiene que elegir uno de distintas pilas. El análisis está basado en el hecho de que era posible saber por quién había votado un grupo específico de personas durante una ventana de tiempo analizando qué papeletas era necesario reponer en medio de la elección, proceso que se realiza múltiples veces al día.

2.1.2. Análisis de propiedades físicas de seguridad

Un caso de estudio sobre las propiedades de seguridad asociadas a elementos físicos se realizó para unas elecciones en Holanda [34]. Ahí se asignó riesgos a cada uno de los elementos asociados a un día de votación, pero sólo focalizándose en la votación misma y el conteo, pero no en todos los procesos asociados a ésta.

2.1.3. Modelación de riesgo para votaciones

El estudio de la sección anterior está basado en un trabajo previo, en donde se usan *threat trees* [4] y simulación de Montecarlo para modelar los distintos factores de riesgo de una amenaza a un sistema de votación [20]. En particular el trabajo analiza la probabilidad de que una elección sea atacada, el grado de motivación de un atacante cualquiera, la dificultad de atacar al sistema y el impacto de un posible ataque exitoso al sistema. Si bien este modelo busca calcular el riesgo de un sistema de votación, el enfoque utilizado es demasiado general respecto a las partes de una elección. Nuestro enfoque es más especializado respecto a las etapas de las elecciones, asignando riesgos a partes específicas de ésta y no a procesos enteros.

2.2. Elecciones en Chile

Las elecciones son el proceso democrático con el que se eligen a los representantes políticos del país. Realizadas en un tiempo acotado (durante un sólo día), durante el proceso se habilitan locales de votación públicos, generalmente escuelas, en donde los ciudadanos habilitados para sufragar (personas con al menos 18 años) se acercan a este recinto, van a su mesa asignada atendida por los vocales de mesa (ciudadanos elegidos aleatoriamente para asistir el proceso), marcan su preferencia de candidatos en una hoja de papel en secreto, y depositan el voto sellado en una urna de votación. Los votos son posteriormente contados el mismo día y los candidatos elegidos son anunciados.

El proceso anteriormente descrito, correspondiente al día de las elecciones, es acompañado por otros que ocurren antes y después del día de la elección que serán descritos en más detalle en capítulos posteriores. Un mes antes de las elecciones, las juntas electorales (organismos autónomos a lo largo del país) proceden a elegir candidatos para el papel de vocales de mesa, seleccionando candidatos por mesa y luego haciendo un sorteo público para elegir a los designados entre los candidatos que eligieron.

El día siguiente a las elecciones, el Colegio Escrutador (elegido de la misma forma que los vocales de mesa) se reúne y comprueba la correctitud de los resultados de las elecciones, mediante la revisión de las actas de resultados del día de la elección.

Estos procesos son organizados por el Servicio Electoral (SERVEL), el cual es un organismo autónomo, encargado de la administración, supervigilancia y fiscalización de procesos electorales y plebiscitos. También se encarga del cumplimiento de normas sobre transparencia, límite y control de gasto electoral, de las normas sobre la organización de los partidos políticos, y de mantener el sistema de inscripciones electorales y registro de partidos políticos, entre otras funciones [25].

Entre los cargos a elegir están, por ejemplo:

- Presidente de la República: es el jefe de Estado y gobierno, máxima autoridad política. Encargado de la administración y el gobierno del Estado de Chile.
- Senadores y Diputados: la principal función de ambos cargos es participar en la elaboración de leyes junto al Presidente de la República. En la actualidad hay 43 senadores y 155 diputados.

También se realizan elecciones para elegir cargos como alcaldes, concejales y consejeros regionales.

2.2.1. División Electoral de Chile

Las elecciones de Presidente de la República son cada 4 años y son comunes a lo largo de todo el país, pero los Diputados y Senadores no son elegidos por todos los votantes, sino que se separan en circunscripciones y distritos:

- Circunscripciones senatoriales: Se elige una cantidad de senadores por cada una de éstas, dependiendo de la población que vive dentro de la circunscripción. Actualmente se tiene una circunscripción por región en Chile, llegando a 16. El cargo de senador dura 8 años y hay elecciones cada 4, alternando circunscripciones pares e impares en sus elecciones.
- Distritos: Cada distrito posee una cantidad de diputados determinada por la población de la zona geográfica. En la actualidad hay 28 distritos y se realizan elecciones en todos ellos cada 4 años.

2.3. Sistemas Distribuidos

Un sistema distribuido es una colección de computadores independientes que se comunican entre sí, el cual para sus usuarios aparenta ser un solo sistema coherente [28]. Esta definición implica que los computadores que trabajan independientemente deben poder colaborar para lograr trabajar como un sólo organismo. Para esto los sistemas se dividen en dos partes importantes, las entidades, que corresponden a los computadores que forman parte del sistema, y el medio, la forma en que se conectan entre sí.

Entre los conceptos importantes asociados a los sistemas distribuidos, y que son relevantes para este trabajo, están:

- Tolerancia a fallas: Debido a que el sistema está compuesto de muchos computadores operando al mismo tiempo, es posible que uno o más de éstos dejen de funcionar en cualquier momento. Hay distintos tipos de fallas, entre ellas que un componente no envíe los mensajes que debe enviar, que no los reciba, que envíe mensajes incorrectos o que deje de funcionar completamente. Un buen sistema distribuido tiene medidas para evitar que todo el sistema deje de funcionar si es que algunas de las partes fallan.
- Replicación de información: Corresponde a almacenar información en más de un lugar a la vez, principalmente por dos motivos: tener respaldos en caso de que una de las

componentes que almacena la información falle, y para mejorar el rendimiento cuando más de una componente del sistema requiere la misma información.

2.3.1. Relevancia para este trabajo

Uno de los principales objetivos de este trabajo es modelar el sistema de votación como un modelo distribuido, en donde hay distintas entidades, las cuales en vez de computadores son principalmente personas, registros físicos, y computadores; y el medio de comunicación es ya sea el mismo texto escrito de las actas, las redes locales (o Internet) o la comunicación humana.

En particular, distintos conceptos equivalentes entre sistemas distribuidos y el sistema de votación serían, por ejemplo, que personas involucradas den información errónea en los documentos oficiales de resultados, que personas se ausenten en los procesos a los que deben concurrir, que personas se nieguen a enviar mensajes, que fuentes de información (actas de votación) tengan más copias para agilizar el proceso y repetir información, etc.

Por simplicidad, el caso particular de que una persona se niegue a enviar mensajes no se considerará en el trabajo, ya que esto involucraría represalias a la persona en forma de multas o cárcel, y supondremos que las personas siempre querrán evitar este tipo de sanciones.

Capítulo 3

Elección de Vocales de Mesa

3.1. Personal Involucrado

3.1.1. Vocales de Mesa

Los vocales de mesa son ciudadanos comunes y corrientes, habilitados para votar, que son escogidos para trabajar en roles específicos del proceso eleccionario, principalmente en el día de las elecciones [2]. Entre sus tareas están, principalmente:

- Permanecer durante todo el día en el local de votación en su mesa asignada.
- Asistir a los votantes pertenecientes a la mesa, entregándoles los materiales necesarios para votar.
- Registrar en los libros oficiales las personas que ya asistieron a votar a la mesa.
- Posteriormente al plazo oficial de votación, abrir las urnas con las papeletas y contar el resultado final de la mesa.
- Registrar los resultados en las actas oficiales que provee el Servicio Electoral.

Estas personas reciben un bono en dinero de dos tercios de unidad de fomento por sus labores en un día de votación.

En cada mesa deben haber cinco vocales, diferenciados en los roles de Presidente, Secretario y Comisario, elegidos por votación entre los mismos vocales de la mesa.

A diferencia de otros países donde estos empleados son seleccionados y contratados por las autoridades, en Chile son ciudadanos comunes y corrientes elegidos de forma aleatoria por las denominadas Juntas Electorales. Para las elecciones presidenciales del año 2017, se contó con 214.450 vocales de mesa para un total de 42.890 mesas de votación.

3.1.2. Junta Electoral

Las juntas electorales [2] son organismos independientes del Servicio Electoral que cumplen las siguientes funciones:

- Elegir a los vocales de mesa y miembros del Colegio Escrutador de su zona,
- Elegir a los reemplazantes de los cargos anteriores, en caso de que éstos deban excusarse,
- Recibir las excusas de los vocales de mesa y miembros del Colegio Escrutador que no puedan ejercer su labor por razones específicas, y
- Nombrar a los Delegados de la Junta Electoral junto a sus asesores, que se encargan de supervisar un local de votación designado en el día de las elecciones.

Cada Junta Electoral está asignada a una región geográfica específica, debe haber al menos una por provincia y el Servicio Electoral puede crear más Juntas Electorales si lo cree necesario. Al momento de escribir este trabajo, se cuenta con 116 Juntas Electorales en Chile.

A diferencia de los vocales de mesa, las personas que componen la Junta Electoral están determinadas por la ley, y corresponden a personas con cargos públicos específicos:

- En las provincias en las que haya una Corte de Apelaciones, la junta será integrada por el Fiscal Judicial de esta corte, el Defensor Público de la capital de la provincia y el Conservador de Bienes Raíces.
- En las demás capitales de provincia, las Juntas se integrarán con el Defensor Público, el Notario Público y el Conservador de Bienes Raíces de ellas.

En ambos casos debe haber un Presidente de la Junta y un Secretario, si en la provincia hay una Corte de Apelaciones, el Presidente corresponde al Fiscal Judicial de esa corte, y si no hay Corte de Apelaciones, el cargo cae en el Defensor Público. El Secretario corresponde al Conservador de Bienes Raíces de la provincia.

3.2. Proceso de Selección

Por cada proceso electoral, de los cinco vocales totales se designan dos nuevos vocales para elecciones de diputados y senadores, y tres nuevos en elecciones municipales. Los vocales restantes se escogen entre los cinco vocales que ejercieron ese rol en las elecciones anteriores, para que apoyen a los nuevos vocales en el proceso. Si la mesa es nueva se eligen cinco nuevos vocales, es decir, no se mueven vocales desde otras mesas.

Para elegir a los nuevos vocales, cada miembro de la Junta Electoral debe elegir diez ciudadanos por mesa del padrón definitivo entregado por el Servicio Electoral, como potenciales candidatos para el cargo. Para elegirlos deben considerar a aquellos que consideran como los más aptos para desempeñar la labor de vocal [2]. El criterio de elección no es explicitado en el reglamento por lo que es frecuentemente subjetivo y discrecional dependiente de la junta electoral.

Posteriormente los tres miembros de la Junta deben juntar las nóminas correspondientes a la misma mesa y realizar un sorteo para elegir los cinco vocales para la mesa y los cinco reemplazantes en caso de excusas. Las listas, al juntarse, deben ordenarse por orden alfábetico según apellidos de los potenciales vocales. Dicho sorteo es público y algunas Juntas Electorales permiten la presencia de personas asociadas a partidos políticos para supervisar el proceso. Cabe destacar que no es un sorteo por mesa, sino que es un solo sorteo de índices, los cuales se aplican para todas las mesas.

Las nóminas creadas por los miembros de la Junta Electoral deben incluirse en un libro firmado por ellos que es de carácter público, resguardado por el Secretario de la Junta. Además estos nombres deben ser publicados en un periódico y las personas elegidas deben ser notificadas por correo.

Como apoyo a todo este proceso, el Servicio Electoral dispone de un software desarrollado internamente para las Juntas Electorales. No es obligación que este software sea usado por las juntas, pero la gran mayoría lo ha adoptado en su proceso de selección de vocales en los últimos años.

En dicho software está cargado el padrón electoral separado por mesa, y junto al nombre de las personas se muestra la dirección, edad y profesión en caso de estar en las bases de datos del Registro Civil; estos datos son usados por las Juntas para seleccionar a las personas *más aptas*, por ejemplo, evitar elegir a personas de la tercera edad.

Para esta tesis se tuvo la oportunidad de conversar con una junta electoral sobre qué tipo de personas son elegidas generalmente para desempeñar como vocales. Se nos indicó que las juntas intentan escoger a profesionales, principalmente abogados; y que personas como carabineros no son elegidos porque por ley no pueden ejercer como vocales de mesa. También se nos señaló que el software del SERVEL no posee toda la información que requieren para el sorteo, ya que gran parte de las profesiones no están informadas, y tampoco se muestra si la persona pertenece al registro nacional de discapacidad, ya que éstas tampoco deben ser consideradas para el sorteo.

Las Juntas Electorales deben realizar el sorteo de forma externa al software, el cuál sólo les permite ingresar los números resultantes del sorteo de vocales y suplentes. Para efectivamente sortear los números, las juntas suelen recurrir a tómbolas de números (ver Figura 3.1) para luego indicar en el software los números seleccionados.

Figura 3.1: Junta electoral durante proceso de elección de vocales con una tómbola [9].

Hablamos también con el equipo de Tecnologías de la Información del Servicio Electoral, en particular con desarrolladores del software mencionado. Se nos mencionó que el sorteo era posible de hacer dentro de la aplicación en el pasado, pero debido a distintos reclamos por parte de las Juntas Electorales que preferían hacerlo por separado, el botón para realizar el sorteo tuvo que eliminarse. Los reclamos decían relación con la pérdida de una prerrogativa existente de las juntas electorales sin un beneficio claro.

El software del SERVEL también permite generar las cartas de notificación de los vocales

elegidos, además de descargar las listas de los seleccionados.

El correcto funcionamiento de este proceso depende no sólo de que la información correcta sobre los votantes llegue a la junta electoral, sino también de que la junta realice correctamente su trabajo o de que público adicional se encuentre presente para supervisar el correcto funcionamiento del sorteo, y de que los vocales elegidos sean notificados correctamente de su labor.

3.3. Casos de Ataque a la Selección de Vocales

A fin de modelar potenciales ataques, a continuación se considerarán distintas situaciones en las cuales la integridad del sorteo de vocales de mesa pudiera verse comprometida, explicando cómo serán modelados para las secciones posteriores de análisis de ataques.

3.3.1. Toda la junta está comprometida

En este caso, los tres miembros de la junta electoral serían maliciosos y trabajarían en conjunto. Como tienen control total sobre la selección de vocales en cada mesa, pueden alterar el sorteo para que cada mesa tenga tantos vocales maliciosos como la junta electoral puede conseguir. Para poder elegir a estos vocales maliciosos, basta que en el momento de la creación de listas, pongan a todos los vocales maliciosos a lo largo de las mesas en las mismas posiciones de la lista de candidatos a vocales, y luego alteren el sorteo de números para que salgan elegidos los índices con los vocales maliciosos. Como las listas finales deben estar ordenadas alfabéticamente, la junta comprometida debe asegurarse de seleccionar también a ciertos potenciales candidatos no comprometidos, con apellidos que aseguren que los vocales maliciosos queden en las posiciones deseadas.

En caso de que se tengan que repetir candidatos de la elección anterior, como los puestos de la junta electoral son vitalicios mientras se mantengan en el cargo, basta que elijan a los vocales de mesa en un período cuando sean nuevos vocales, y luego los pueden mantener para la siguiente elección. Este supuesto se mantendrá para los casos posteriores.

3.3.2. Un solo miembro de la junta es malicioso

En esta sección consideraremos un caso más restringido, donde sólo un miembro en la junta electoral es malicioso, mientras que los dos miembros restantes se suponen honestos. Supondremos que el miembro malicioso cuenta como un conjunto de potenciales candidatos a vocales maliciosos, los cuales intentará asignar (de forma ilegítima) como vocales de mesa.

En el caso de que un miembro de la junta electoral quiera alterar el resultado del sorteo, como se sortean cinco números, supondremos que durante el sorteo de cada número hay un intento de alterar el número obtenido. Ejemplos de alteraciones serían, en el caso de una tómbola, sugerir a los otros miembros de la junta nombrar a una persona en particular por recomendación del miembro comprometido de la junta, reemplazar una bolita en un momento en que los otros miembros de la junta no estén mirando, o escribir otro valor al momento de anotar los números en documentos oficiales, entre otras opciones.

Debido a que el sorteo de los vocales de mesa es sólo uno para todas las mesas, en vez de uno para cada mesa, el miembro de la junta electoral comprometido debe tener esto en cuenta para lograr incluir la mayor cantidad de vocales comprometidos. La forma en que se modeló esto es la siguiente: una vez que se forma una lista completa de potenciales vocales para una mesa, el miembro malicioso de la junta electoral registra los números en que se encuentran sus vocales maliciosos dentro de la lista. Una vez termina la elección de los candidatos, puede enviar la información a un tercero que calcule cuáles son los números con más candidatos maliciosos, para así intentar alterar el sorteo para que esos números sean elegidos.

3.3.3. Dos miembros de la junta son maliciosos

Para este caso se trabaja bajo el supuesto de que ambos miembros maliciosos de la junta están trabajando en conjunto y tienen los mismos intereses políticos.

Este caso se modela de la misma forma que el caso de un miembro malicioso. La diferencia es que en el momento de decidir si el vocal a agregar estará comprometido por acción de la junta, cada miembro malicioso intenta alterar el resultado por separado, alterando el resultado si es que alguno de los dos es exitoso, o si ambos lo son.

3.3.4. Un tercero intenta alterar resultados al momento de realizar el sorteo

Algunas juntas electorales tienen público presente al momento del sorteo de vocales de mesa, por lo que es posible que un miembro del público intente alterar los resultados. Como probablemente exista algún tipo de barrera entre los miembros de la junta y el público, ya sea física o simplemente de distancia, este caso se considera similar al de un miembro de la junta malicioso, pero la probabilidad de éxito es mucho menor y, a la vez, la cantidad de potenciales vocales comprometidos es mucho menor, ya que es poco probable que uno de los candidatos a vocal sea elegido en la lista.

3.3.5. Un tercero hackea el sistema computacional usado

El sistema computacional usado guía a la junta durante todo el proceso, excepto por el sorteo, que debe realizarse de forma externa. Un tercero podría intervenir este sistema, modificando los candidatos seleccionados después de haberse realizado el sorteo.

Los resultados del sorteo deben publicarse en la oficina de uno de los miembros de la Junta Electoral, publicados en la prensa y cada vocal debe ser notificado por carta a su domicilio. El sistema computacional permite exportar la lista de seleccionados para comunicarlos a la prensa y a la vez permite generar automáticamente las cartas de notificación para los vocales, por lo tanto, si una persona interviene el sistema, tanto la prensa como las cartas tendrán información errónea y la lista correcta sólo será publicada físicamente en una oficina. Aunque la ley establece que el documento oficial que dice quién es vocal de mesa es la lista publicada en esa oficina, no hay forma de que alguien note el error en la selección si los verdaderos vocales no son notificados. Incluso si los vocales verdaderos fueran notificados, se generaría un gran problema de desinformación y desconfianza en el proceso de selección de vocales.

Como el sorteo es intervenido posteriormente y todos los vocales son reemplazados por vocales maliciosos, los resultados son equivalentes a los que se tienen cuando toda la junta electoral está comprometida.

Capítulo 4

Día de Votación

4.1. Personal Involucrado

Existen distintos roles dentro del personal del recinto de votación [2], entre ellos están:

- Vocales de Mesa: Descritos en el capítulo anterior, elegidos aleatoriamente para ayudar a los votantes a sufragar, llevar registro de ellos y contar los resultados.
- Delegado de la Junta Electoral: Elegido personalmente por la Junta Electoral, su labor incluye informar a los votantes sobre su mesa de votación, velar por la constitución de las mesas, entregar y recibir útiles electorales para las mesas, entre otras funciones.
- Personal de Enlace del Servicio Electoral (PESE): Generalmente es una persona por local de votación junto a dos asistentes, son contratados por el Servicio Electoral y deben preocuparse de que las mesas de votación sean establecidas correctamente, además de revisar que se llenen las distintas actas a lo largo del día.
- Digitador: Persona contratada por la empresa encargada del sistema de transmisión de datos, su deber es operar el sistema de transmisión de información, actualizando información sobre la constitución de mesas, escaneando las actas e ingresando los conteos parciales de los votos de cada mesa. Existe uno por recinto de votación.

4.1.1. Digitador

A diferencia de los otros cargos que se ven en el día de las votaciones, los digitadores son contratados directamente por la empresa que presta el servicio de conectividad para el envío de datos[1]. Esta empresa es contratada mediante licitación pública, usualmente con sólo un postulante por los altos requisitos que tiene (poder instalar un computador con acceso a internet en todos los locales de votación del país), aunque en los últimos años más empresas han intentado adjudicarse la licitación.

Para la selección de los digitadores no se tiene un concurso público ni una selección aleatoria. Más bien, la empresa escoge a quienes contratar desde una base de datos propia, los cuales son contactados y contratados directamente por ésta.

[1]En el momento de la escritura de este trabajo, esta empresa corresponde a Telefónica.

Como debe haber al menos un digitador por local de votación, Telefónica debe contratar a más de dos mil digitadores y además contar con, al menos, la misma cantidad de computadores especiales para la ocasión, junto a un escáner para poder enviar las actas al Servicio Electoral. Estos computadores deben conectarse a internet mediante una red exclusiva para éstos, la cual debe habilitarse en las semanas anteriores a la votación. Según nos fue relatado por funcionarios de un colegio usado como local de votación, está red sigue funcional incluso fuera de los periodos de elecciones.

Además de los digitadores también existen sus respectivos supervisores, que trabajan el día de la elección y realizan tareas como hacer las gestiones en caso de que uno de los computadores a usar por uno de los digitadores falla, para reemplazarlo a tiempo. También proveen soporte técnico en caso de haber problemas con el software de envío de información.

4.2. Desarrollo de la Votación

4.2.1. Constitución de mesas

El día anterior a las votaciones se debe llenar un formulario con datos básicos del personal del local de votación, como lo son el PESE, sus ayudantes, y el digitador. Este formulario se llena manualmente, se escanea y también se digita en el sistema online.

Luego, en el día de votación, se rellenan cuatro informes a distintas horas de la mañana indicando el estado de las mesas de votación: si las mesas están constituidas o no, a qué hora se constituyeron y el número de vocales por mesa. Si una mesa tiene más vocales del mínimo necesario (tres vocales) y otra mesa tiene menos del mínimo, se pueden mover vocales entre mesas, sin cambiar el lugar donde votan oficialmente los vocales trasladados. Esto muestra una resistencia a los fallos en caso de que partes del proceso (vocales de mesa) se ausenten.

Si la totalidad de las mesas se constituye antes de que se hagan todos los informes, no es necesario hacer los siguientes. Al final del proceso se rellena otro formulario resumen del proceso de constitución.

Algunas imágenes de las actas descritas en esta sección se muestran en el Anexo A.

4.2.2. Votación en las mesas

El votante se acerca a su mesa de votación asignada, donde es atendido por los vocales de mesa. Si hay más de un votante al mismo tiempo, éstos deben hacer fila en un lugar ligeramente apartado de la mesa, es decir, no deben estar cerca de ella.

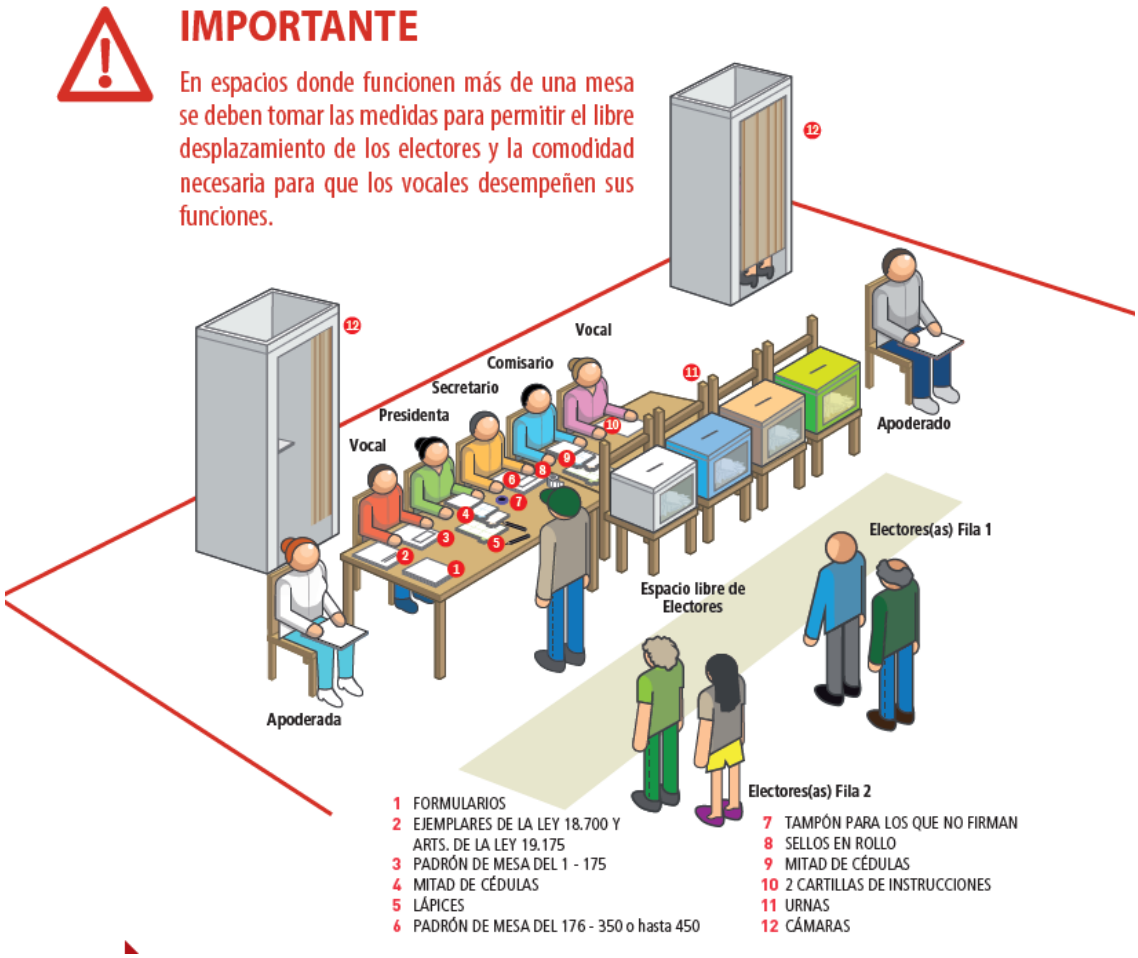


Figura 4.1: Imagen informativa del local de votación, entregada en cartilla informativa para vocales de mesa [11].

Los vocales solicitan un documento para verificar la identidad del votante, como la cédula de identidad o el pasaporte, y una vez que es comprobada, el votante debe firmar en el Padrón Electoral de la mesa para tener un registro de que asistió a votar.

Posteriormente, el presidente de la mesa toma una cédula de votación de cada tipo (Presidente, Senador, Diputado, etc.), y el secretario toma nota del número de serie de la cédula y lo anota en el padrón, entregándole el voto al votante sin remover el número de serie.

El votante se acerca a la cámara secreta, donde tiene un minuto para marcar su opción en secreto, luego de esto debe sellar el voto. Es ilegal que deje algún registro de cuál opción seleccionó, por ejemplo, es ilegal que le tome una foto al voto.

Luego se debe hacer entrega del voto al presidente de la mesa para que compruebe que el voto que selló es el mismo que se le fue entregado. Una vez comprobado se corta el número de serie del voto, desvinculando al votante de su voto, se guarda el número de serie y el votante deposita el voto en la urna.

El proceso de votación supone que los votantes llegarán y marcarán la opción que muestre

su preferencia, y de que su voto sea contabilizado más tarde.

4.2.3. Conteo de votos

Antes de realizar el conteo, el Secretario de la mesa debe escribir en el Padrón Electoral, uno por uno, la expresión "no votó" en los recuadros para las firmas de los votantes que no hayan votado [2].

Luego el Presidente cuenta el número de votantes que participó en la elección y el número de talones de números de serie, para anotarlas en el acta correspondiente.

Posteriormente se procede a abrir las urnas de votos, contando la cantidad de votos de cada categoría sin abrirlos. Si algún voto se depositó en la urna incorrecta, los vocales deben moverlos a la urna correspondiente, es decir, si se depositó un voto de senador en la urna de presidente, este voto debe ser depositado en la de senadores.

Luego se comienza a abrir los votos, tanto Secretario como Presidente firman el voto por el reverso antes de abrirlo, luego el Secretario abre el voto y el Presidente lee en voz alta la preferencia de éste.

Para realizar el conteo general, los vocales suelen contar anotando a la vista de todos los resultados parciales, como se ve en la Figura 4.2, o simplemente en una hoja de papel en la mesa de votación.

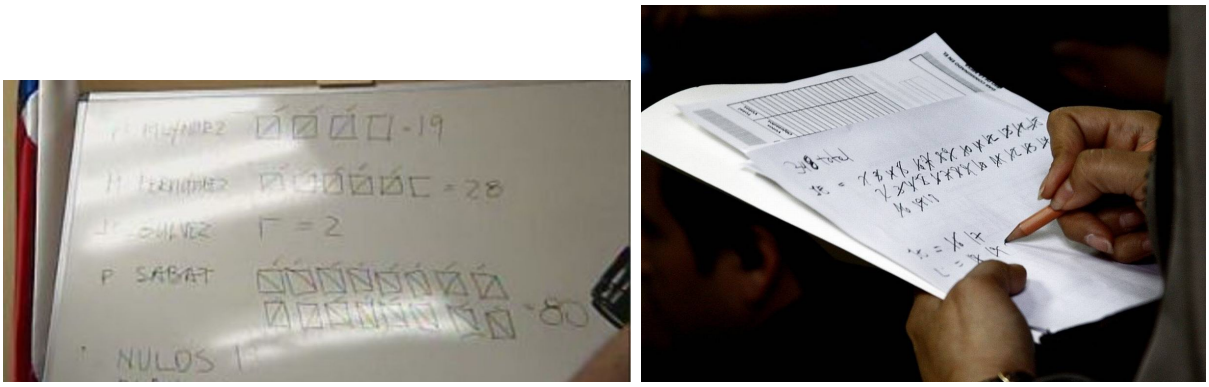


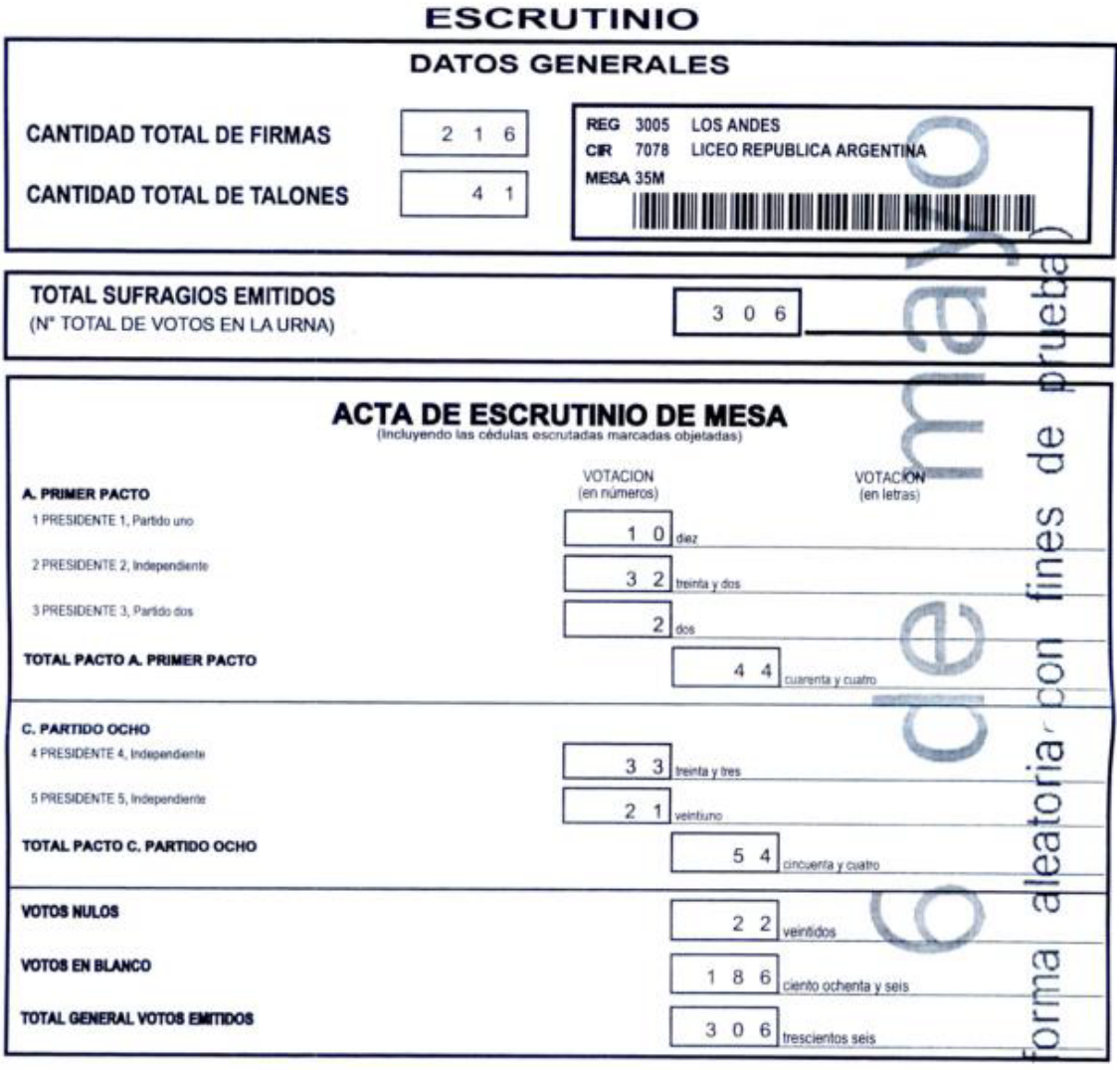
Figura 4.2: Conteo de votos en pizarra [3] y conteo de votos en papel [29].

Este conteo es completamente público, y es supervisado principalmente por los apoderados de mesa, que corresponden a personas enviadas por los partidos políticos para supervisar el correcto funcionamiento de las mesas, y reclamar la validez de los votos que no cumplen con todas las condiciones de un voto válido, según su conveniencia. El número de apoderados en cada elección ha bajado considerablemente en años recientes, llegando a valores cercanos al 5 % del total de las mesas, número que no es suficiente para supervisar todas las mesas o locales del país.

Los votos contados son agrupados por categorías de autoridades elegidas y son guardados en sobres facilitados por el Servel, los que son enviados de vuelta al Servicio Electoral para su almacenamiento. Éstos son almacenados durante aproximadamente un mes en bodegas administradas por el Servel, en caso de que el TRICEL los requiera más adelante.

Para concluir su labor, los vocales deben completar el acta de escrutinio (Figura 4.3), documento oficial con los resultados de la mesa. Se deben hacer tres ejemplares que son enviados a distintas entidades, y deben contar con los siguientes datos, entre otros:

- Hora de inicio y cierre de la votación.
- Hora de inicio y término del escrutinio.
- Identificadores de la mesa como número, local de votación y Circunscripción Electoral.
- Cantidad de firmas en el padrón.
- Cantidad de talones con número de serie de los votos.
- Total de sufragios en la mesa.
- Indicación si cuadran los votos contados con las firmas y los talones.
- Cantidad de votos por candidato, votos nulos y en blanco, en letras y números, indicando los votos marcados y/o objetados.


ESCRUTINIO

DATOS GENERALES

CANTIDAD TOTAL DE FIRMAS 216

CANTIDAD TOTAL DE TALONES 41

REG 3005 LOS ANDES
CIR 7078 LICEO REPUBLICA ARGENTINA
MESA 35M

TOTAL SUFRAGIOS EMITIDOS
(N° TOTAL DE VOTOS EN LA URNA) 306

ACTA DE ESCRUTINIO DE MESA
(Incluyendo las cédulas escrutadas marcadas objetadas)

	VOTACION (en números)	VOTACION (en letras)
A. PRIMER PACTO		
1 PRESIDENTE 1, Partido uno	10	diez
2 PRESIDENTE 2, Independiente	32	treinta y dos
3 PRESIDENTE 3, Partido dos	2	dos
TOTAL PACTO A. PRIMER PACTO	44	cuarenta y cuatro
C. PARTIDO OCHO		
4 PRESIDENTE 4, Independiente	33	treinta y tres
5 PRESIDENTE 5, Independiente	21	veintiuno
TOTAL PACTO C. PARTIDO OCHO	54	cincuenta y cuatro
VOTOS NULOS	22	veintidos
VOTOS EN BLANCO	186	ciento ochenta y seis
TOTAL GENERAL VOTOS EMITIDOS	306	trescientos seis

Figura 4.3: Ejemplo de acta con los votos de una mesa de votación.

Los tres ejemplares del acta de escrutinio deben entregarse a:

- El Secretario de la mesa, que hace entrega del acta al funcionario delegado por Correos de Chile, para que envíe el acta al Tribunal Calificador de Elecciones.
- El Presidente de la mesa, que le entrega el acta al Delegado de la Junta Electoral, para que ésta sea usada por el Colegio Escrutador el día siguiente para el escrutinio posterior.
- El Comisario de la mesa, que hace entrega del acta al PESE para que el digitador la escanee y escriba la información al sistema de envío de información.

Además, los apoderados de mesa también pueden solicitar copias de las actas si así lo desean.

El proceso de conteo y creación de actas funciona correctamente siempre y cuando todos los votos sean contados de acuerdo a la preferencia que marcó el votante y los vocales de mesa escriban correctamente las actas luego del conteo. También requiere que las actas no sean extraviadas.

4.2.4. Envío de información

Una vez completadas las actas, ellas se entregan al PESE, quien se las entrega al digitador del recinto de votación. El digitador ingresa al sistema computacional de envío de información con su propio nombre de usuario y contraseña, donde ve una lista de todas las mesas que debe ingresar al sistema, como se ve en la Figura 4.4. Durante una visita a un ensayo del procedimiento del día de las elecciones, se vio que la contraseña asignada al digitador venía impresa en una hoja con instrucciones, pero se desconoce si ésta es la misma que es usada fuera de los ensayos.

Figura 4.4: Imagen del sistema computacional con la lista de mesas a ingresar por el digitador. [10]

Para comenzar el proceso de ingreso de información, primero debe seleccionar una mesa y escanear el acta de votación que va a ingresar. Luego debe ingresar los votos que recibió cada candidato, junto con el total de votos que contaron los vocales de mesa y el total de talones de las cédulas. Si la información es inconsistente, se ingresa de todas formas al sistema para que el Colegio Escrutador la revise posteriormente; si el digitador comete un error, el PESE debe autorizar el cambio de la información mediante la digitación de una clave que sólo él tiene.

Este proceso debe hacerse en orden de resultados de Presidente, Senadores y Diputados, y cada uno tiene su propia sección en el sistema.

4.2.5. Resultados de la elección

Una vez se tienen todos los votos del país, se procede a calcular los totales para evaluar quienes resultan elegidos a los cargos. Para esto se utiliza la mayoría simple en el caso de que sea sólo un cargo a elegir, es decir, se elige al candidato con la mayoría de votos; para los otro cargos se utiliza el sistema D'Hondt [2].

El sistema D'Hondt funciona de la siguiente forma, cuando se eligen n candidatos:

- Cada candidato, además de pertenecer a un partido político, pertenece a un pacto, generalmente conformado por más de un partido político.
- Una vez que se tienen los votos de cada candidato, se suman los votos que tiene cada pacto.
- Luego los votos del pacto se dividen por los números naturales desde el 2 hasta la cantidad de cargos a elegir en la zona.
- Se ordenan todos estos números (en total correspondería a la cantidad de pactos multiplicada por los cargos a elegir) de mayor a menor, y se elige un representante de cada pacto por cada vez que el pacto aparezca en los primeros n lugares de la lista.

El proceso no termina aquí, ya que cada pacto puede estar formado por más de un partido político. Si es de un sólo partido, entonces se eligen los candidatos con más votos del partido, de acuerdo a la cantidad de cargos que hayan obtenido en el proceso anterior.

Si hay más de un partido político (y más de un candidato elegido en el pacto) se vuelve a usar el sistema D'Hondt, pero esta vez en vez de elegir entre los distintos pactos y la cantidad de cargos a elegir totales por la división electoral, se realiza enter los partidos políticos del pacto y la cantidad de cargos para los que fueron seleccionados en el proceso D'Hondt realizado anteriormente.

Finalmente el SERVEL recibe los resultados de las elecciones de todo el país y publica los resultados preliminares en su sitio web. Estos resultados no son oficiales, siendo oficiales sólo los validados por el TRICEL, explicados en el capítulo 7.

Ejemplo

Para una más fácil comprensión del sistema D'Hondt, se propone el siguiente ejemplo. Consideremos el siguiente conteo final de votos para un caso ficticio, donde se eligen 4 cargos:

Pacto	**Partido Político**	**Candidato**	**Votos**
α	A	1	8000
		2	3000
	B	3	10000
β	C	4	25000
		5	3500
	D	6	13500
		7	500
γ	E	8	31000
		9	9500

Tabla 4.1: Resultados para ejemplo de elección.

Si la elección fuera por mayoría simple, se elegirían a los candidatos 8, 4, 6 y 3.

Para el sistema D'Hondt, primero se deben sumar los totales de cada pacto, dividirlos por los números del 1 al 4 (cuatro candidatos a elegir), y ordenar estos resultados de mayor a menor para determinar los candidatos que deben ser elegidos. Para este caso obtenemos los siguientes resultados, en donde las celdas más oscuras muestran a los pactos con candidatos elegidos:

Pacto	**División**	**Votos**
β	1	42500
γ	1	40500
β	2	21250
α	1	21000
γ	2	20250
β	3	14166.66
γ	3	13500
β	4	10625
α	2	10500
γ	4	10125
α	3	7000
α	4	5250

Tabla 4.2: Resultados por pacto en sistema D'Hondt.

Es decir, el pacto α recibe un cupo, β dos, y γ uno.

Ahora hay que hacer el mismo proceso para los tres pactos.

- En el pacto α, el partido A tiene 11000 votos y el B 10000, por lo tanto el partido A es el que tiene a su candidato con la mayoría de votos elegido, es decir, el candidato 1.
- En el pacto β se eligen dos candidatos, por lo tanto se realiza el proceso de dividir por 1 y 2, para ordenar de mayor a menor. Se obtiene la siguiente tabla:

Partido	**División**	**Votos**
C	1	28500
C	2	14250
D	1	14000
D	2	7000

Tabla 4.3: Resultados para partido β en sistema D'Hondt.

  De lo que se obtiene que el partido C tiene a dos candidatos elegidos. Como tiene sólo a dos, se eligen a los candidatos 4 y 5.
- Finalmente el partido γ tiene a un candidato elegido, y como sólo está conformado por un partido político, su candidato elegido es el con más votos, el candidato 8.

En resumen, con sistema D'Hondt se eligen a los candidatos 1, 4, 5 y 8; mientras que con mayoría simple se elegirían a 3, 4, 6 y 8.

4.2.6. Flujo de información

Como resumen, se muestra un diagrama del flujo de información durante el día de votación.

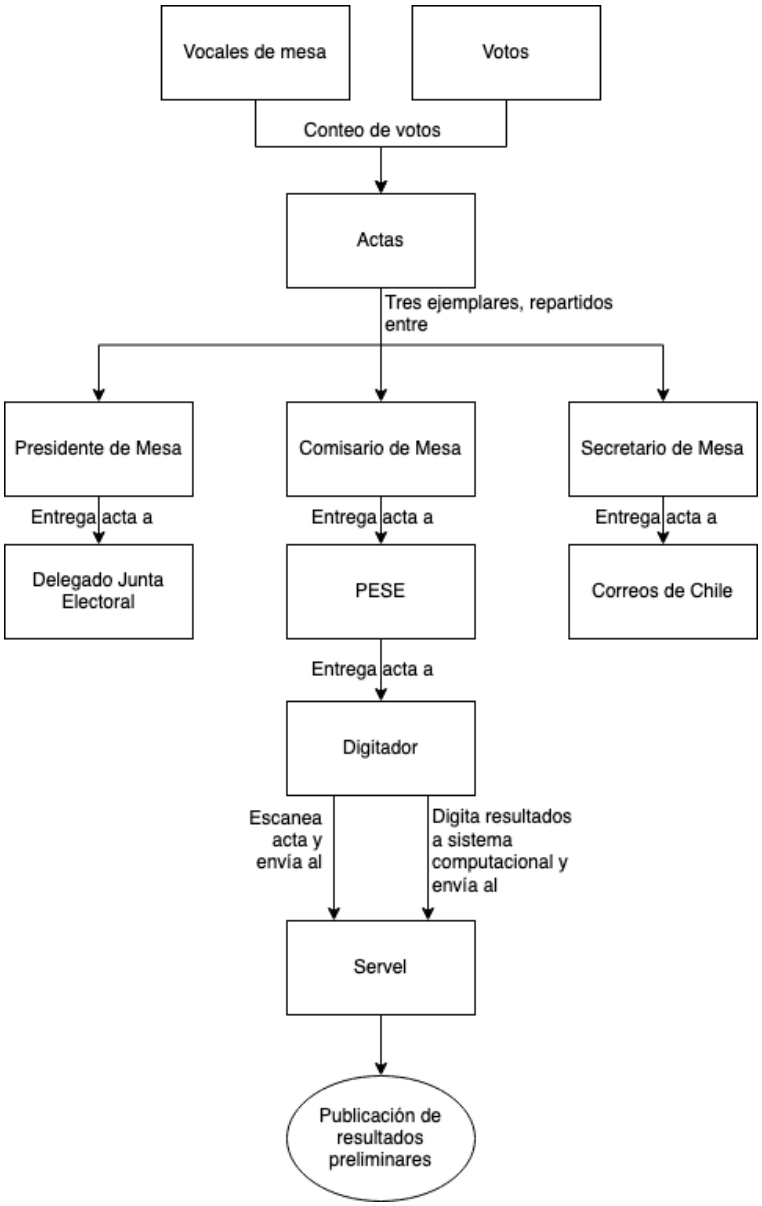


Figura 4.5: Flujo de información en el día de votación.

4.3. Posibles Casos de Ataque

4.3.1. Vocales de mesa modifican resultados

Este caso corresponde a cuando los vocales de mesa, una vez realizado el conteo de los votos, en vez de escribir los resultados correctos en las actas para el envío de información,

escriben resultados alterados, internamente consistentes. Es decir, mantiene el total de votos originalmente reportados y la suma del total de votos de la alteración es la misma que el total de votos original.

Los vocales pueden crear actas erróneas debido a que:

- los procesos de conteo y creación de actas suelen realizarse hasta tarde en la noche, por lo tanto el público general probablemente no esté presente hasta el final.
- aunque el conteo se haga correctamente, las actas no están disponibles para que el público las vea, por lo tanto se puede realizar un conteo correcto pero el acta puede decir algo distinto.
- la presencia de apoderados de partidos políticos ha disminuido considerablemente en cada proceso en años recientes, llegando a sólo un 5 %, por lo tanto es poco probable que la persona externa autorizada a supervisar el proceso desde cerca esté durante la creación de actas.
- Es posible que sólo sea necesario escribir un acta errónea, ya que la ley permite escribir sólo una y luego fotocopiarla, siempre y cuando las fotocopias sean firmadas por los vocales de mesa.
- Los vocales de mesa, en días anteriores a la elección, deben reunirse para capacitaciones y para la constitución de mesas del día anterior. En estos procesos, otras actas son llenadas, por lo tanto información como las firmas de los vocales de mesa quedan a la vista de un vocal malicioso, el cual puede practicar estas firmas y crear nuevas actas alteradas, con la firma falsificada del resto de los vocales de la mesa.

4.3.2. Digitador modifica resultados

En este caso, el digitador logra cambiar los datos ingresados al sistema computacional. El proceso de envío de información lo realiza el digitador solo, sin necesidad de supervisión. Aunque los instructivos dicen que el digitador debe ser constantemente supervisado por el PESE, una entrevista reveló que muchas veces los digitadores hacen su trabajo solos porque el PESE tiene otras labores al mismo tiempo, o simplemente porque el mismo digitador pide trabajar de manera individual.

Como el sistema sólo revisa si los resultados de la mesa cuadran en las sumas, de acuerdo al total de votos y firmas, cualquier alteración hecha por el digitador no será encontrada inmediatamente.

4.3.3. Sistema computacional es hackeado el día de las elecciones

El sistema computacional utilizado posee las funciones de enviar los estados de constitución de las mesas, los resultados ingresados por los digitadores y también el escaneo de las actas de votación.

El caso principal de hackeo que se estudia es que, de alguna forma, los resultados enviados por el digitador no correspondan a los que éste escribió, sino que a los que un tercero logró enviar. Aunque no fue posible tener acceso completo a este sistema computacional para este trabajo, se logró examinar lo suficiente el proceso para notar lo siguiente:

- Los computadores usados por los digitadores son antiguos y no tienen las últimas versiones del sistema operativo Windows, por lo que es probable que tampoco tengan todas las actualizaciones de seguridad requeridas, haciendo posible que sean intervenidos mediante vulnerabilidades del sistema operativo no disponibles en versiones más nuevas.
- La línea de cable de internet para el envío de datos permanecería disponible a lo largo de todo el año y permite la conexión con cualquier computador, por lo tanto es posible que un tercero interfiera con la conexión física y modifique la información a medida que es enviada. Este ataque sólo funcionaría cuando la comunicación no está encriptada, por lo tanto se considera un caso poco probable, ya que los protocolos SSL/TLS [22] hoy son comunes. Por la contingencia nacional al momento del desarrollo de este trabajo y la disponibilidad por parte del Servel, no fue posible comprobar con la institución si efectivamente usan estos protocolos.
- Según lo observado en un ensayo de envío de información, las claves de acceso para los digitadores eran generadas por la empresa encargada del sistema y tenían como formato el primer nombre del digitador y luego algunos dígitos de su RUT. Como cada digitador sólo tiene acceso a las mesas asociadas a él, es posible que esta información esté asociada a la cuenta del digitador, por lo tanto, un hacker con acceso a un computador y a la lista de digitadores, podría tener acceso a modificar todas las mesas de votación. Al igual que en el punto anterior, por la contingencia nacional y disponibilidad del Servel, no se pudo comprobar si este mecanismo de entrega de contraseñas se mantiene en el día de las elecciones, por lo que se decidió no explorar el alcance de esta posible vulnerabilidad con más detalle, aunque sí se explora más adelante el efecto que ésta puede tener.

Además de lo anterior, un tercero podría optar por simplemente hacer que el sistema de envío de datos falle. Si opta por alterar físicamente la conexión por cable ethernet, los computadores cuentan con una tarjeta de red propia con la que pueden enviar información siempre y cuando las comunicaciones celulares y de datos estén disponibles. Se supondrá que estas redes no se verán afectadas el días de las votaciones, por lo tanto este tipo de ataque se descartó.

Por otro lado, otro ataque posible es que los computadores fallen en el envío de datos. En estos casos, los digitadores pueden contactar a sus jefes para obtener computadores de reemplazo, y pueden proceder con el envío normal de datos.

Capítulo 5

Simulación de una Elección

Para estudiar el efecto que pueden causar los distintos tipos de ataque estudiados en este trabajo, se programó una simulación de elecciones. En ella las distintas entidades que participan en una elección fueron creadas, simulando los procesos descritos anteriormente y variando distintos parámetros asociados a distintos casos más optimistas o pesimistas. Por cada conjunto de parámetros se evaluó el efecto en la cantidad de resultados de las elecciones (candidatos elegidos) que logran ser alterados, comparados con una elección sin ataques.

5.1. Datos

5.1.1. Resultados de elecciones

Para realizar los experimentos, se usaron datos disponibles públicamente sobre los resultados de las elecciones, descargados desde el sitio web del Servicio Electoral [23]. Estos tienen información de elecciones de Presidente, Senadores y Diputados, pero las simulaciones sólo se hicieron con los datos de Diputados.

En estos datos se detallan los votos obtenidos por cada candidato en cada mesa de votación del país, junto con información adicional sobre la división geográfica y política de la mesa. Un detalle de las columnas está en la Tabla 5.1.

Columna	**Explicación**	**Ejemplo**
Región	Número de la región de la mesa de votación	2
Provincia	Provincia de la mesa de votación	ANTOFAGASTA
Circunscripción Senatorial	Marca la división para la elección de senadores	3a Circunscripción
Distrito	Marca la división para la elección de diputados	3
Comuna	Comuna de la mesa de votación	ANTOFAGASTA
Circunscripción Electoral	Unidad básica de división electoral	ANTOFAGASTA NORTE
Local	Recinto donde se encuentra la mesa de votación	ESCUELA ARTURO PRAT
Número Mesa	Número asignado a la mesa	69
Tipo Mesa	Varones, mujeres o mixta	V
Mesas Fusionadas	Indica si la mesa se juntó con otra mesa	69V
Electores	Número de electores en la mesa de votación	345
Número en Voto	Número del candidato en la cédula de votación	50
Lista	Lista (letra) a la que pertenece el candidato	B
Pacto	Pacto político al que pertenece el candidato	POR TODO CHILE
Partido	Partido político al que pertenece el candidato	INDEPENDIENTE PROGRESISTA
Candidato	Nombre del candidato	JANETT SHIRLEY GUERRA ABURTO
Votos TRICEL	Votos que obtuvo el candidato en la mesa	0

Tabla 5.1: Atributos de los datos usados.

5.2. Simulación

La simulación fue implementada a través de un programa hecho en el lenguaje de programación Scala [19], por su capacidad de trabajar con grandes cantidades de datos de forma eficiente. Además se decidió hacer una simulación escrita desde cero y sin usar software adicional, ya que la descripción de los procesos de la elección es la componente principal de ésta. Por ello las partes como el manejo de probabilidades, donde otro software podría ayudar, se encuentran en medio de los procesos. Si bien se podría haber utilizado,software adicional, se estimó que ello haría más compleja la ejecución y comprensión del código.

A continuación se explicarán sus principales componentes y cómo funciona.

5.2.1. Clases principales

Candidato

Una instancia por candidato, posee el nombre de éste y además del pacto político y partido político que posee.

Junta

Se crea una instancia por cada junta electoral en el país. Sus atributos incluyen el nombre, el distrito al que pertenecen, los números de vocales de mesa que fueron sorteados y la cantidad de miembros de la junta comprometidos.

Entre sus funciones está el sortear la cantidad de miembros comprometidos de ésta, y la función para realizar el sorteo de los vocales.

Mesa

Una instancia por mesa de votación en el país. Posee dentro de sus atributos la junta a la que está asociada, su comuna, local y número para identificación, el número de votantes, su distrito y su circunscipción senatorial.

Además posee la cantidad de vocales comprometidos en la mesa, y los resultados de la elección.

Sus funciones incluyen la generación del acta de votos, proceso que incluye el cambio de votos si es que hay vocales de mesa comprometidos, y el sorteo de los números de potenciales vocales comprometidos para el sorteo de vocales.

5.2.2. Parámetros globales

Dentro del código, existe una variedad de parámetros globales que se fueron variando en los experimentos para obtener los distintos resultados, con el objetivo de capturar las distintas formas en que el resultado de la votación pudiera ser alterado. Éstos son:

- PORCENTAJE_EDICION: Porcentaje de votos adicionales que recibe un candidato cuando alguien en su mesa logra modificar los votos a su favor. Este parámetro modela

los distintos escenarios de daño que un vocal malicioso puede causar cuando logra alterar resultados.

- PROB_VOCAL_MESA: Probabilidad de que un vocal (trabajando solo) falle en cambiar los resultados de una mesa. Esto modela el grado de seguridad que hay al momento de crear actas, ya sea personas externas supervisando o los mismos vocales de mesa revisando que todo funcione correctamente. Se consideró la misma probabilidad para todas las mesas de votación, pensado en este valor como el promedio general de la probabilidad descrita.
- THRESHOLD_VOCALES: Mínimo de vocales comprometidos necesarios para considerar que una mesa tendrá sus resultados alterados con una probabilidad de 100 %.
- PROBABILIDAD_COMPUESTA: Considera la posibilidad de que, al momento de que uno o más miembros de la junta electoral intenten alterar el sorteo de vocales de mesa, este trabajo sea más difícil (y por lo tanto, la probabilidad de alteración más baja) si ya se logró alterar el sorteo con anterioridad. Corresponde a un valor binario, en donde o se tiene esta disminución de probabilidad de alteración, o no se tiene.
- CANDIDATOS_MIEMBRO: Cantidad máxima de potenciales vocales maliciosos que puede tener un miembro de la junta electoral comprometido en una mesa.
- PROB_FALLA: Probabilidad de que un miembro comprometido de una junta electoral falle en alterar un número del sorteo de vocales de mesa. Este parámetro modela la seguridad del sorteo y su correcta realización.
- PROB_JUNT_COMP: Probabilidad de que un miembro de una junta electoral esté comprometido. Modela el alcance que pueden tener unos pocos miembros comprometidos en una junta electoral.
- PROB_ENCONTRAR_VOCAL: Para que un miembro comprometido de una junta electoral pueda agregar candidatos maliciosos a la lista de los sorteos, primero debe contar con gente dispuesta a realizar este trabajo. Este parámetro modela la probabilidad de que un miembro comprometido de una junta electoral logre encontrar a una persona para agregar a la lista. Modela qué tan probable es que se encuentren personas dispuestas a alterar una elección en una mesa. Como ejemplo, si esta probabilidad es de un 50 % y se intentan buscar cinco potenciales miembros de la lista de vocales, se realizan cinco cálculos con un 50 % de probabilidad de que cada sorteo sea exitoso.

Más adelante en las tablas de resultados, algunas de estas variables fueron graficadas como su probabilidad opuesta para una más fácil comprensión.

5.2.3. Proceso

A continuación se explicará el proceso realizado para las simulaciones de elecciones.

Preprocesamiento

Como se puede ver en la explicación de los datos usados para la simulación, la junta electoral a la que pertenece cada circunscripción electoral no está especificada directamente en los datos (Tabla 5.1). Esta información estaba disponible en la página web del Servicio Electoral [24], así que se creó un diccionario para asociar las circunscripciones a las junta.

De la misma forma, la cantidad de diputados y senadores que se eligen en cada distrito y circunscripción senatorial varía dependiendo de cada una, por lo que también se crea un diccionario para el número de parlamentarios elegidos por división.

Carga de datos

Para esta etapa, primero se cargan los datos asociados a cada región del país. Para ello, se crean todos los candidatos de la región, los cuales tienen un partido asociado, este último codificado por un número único por partido.

Luego se crean las juntas electorales, asociando las circunscripciones electorales a su junta respectiva, y finalmente se crean las mesas, con información como el número de votantes y el local y número para identificación. Después de crear los objetos de las clases mencionadas, se agrega a cada mesa el total de votos obtenidos por cada candidato en ésta, información incluida en los datos con los que se trabaja.

Asignación de miembros comprometidos

Primero, la simulación debe designar cuáles de los miembros de las juntas electorales tomarán el rol de maliciosos que intentarán alterar el sorteo. Esto se realiza de forma aleatoria, sorteando en cada junta si cada uno de sus integrantes será maliciosa o no. Este sorteo se realiza por cada miembro de junta electoral del país, considerándolo comprometido con la probabilidad asociada a PROB_JUNT_COMP.

Luego, para modelar el efecto de un miembro malicioso de la junta electoral en la selección de vocales, se deben sortear cuántos potenciales vocales de mesa logra obtener cada miembro comprometido de cada junta para incluir en la lista del sorteo. Cada miembro comprometido de la junta electoral podrá tener una cantidad máxima de potenciales vocales comprometidos en la lista, valor asociado a CANDIDATOS_MIEMBRO. Para obtener la cantidad específica con la que se trabaja, se calcula con probabilidad PROB_ENCONTRAR_VOCAL si logra encontrar a una persona para incluir en la lista, y este cálculo se repite CANDIDATOS_MIEMBRO veces.

A cada potencial vocal de mesa se le asigna un número del 1 al 30 en la lista. Como las tres listas de candidatos a vocales escogidas por cada miembro son mezcladas al ser ordenadas alfabéticamente, se considera que no es posible para un miembro de la junta electoral el poder influenciar el número al que están asignados sus vocales maliciosos.

Selección de vocales de mesa

Una vez en el sorteo, dado que los índices escogidos al azar por la junta definen los vocales seleccionados en todas las listas de potenciales candidatos a vocales, la simulación calcula los índices que maximizan el número de vocales corruptos elegidos. Luego de esto se realiza el sorteo de cada número para los vocales de mesa.

Si toda la junta electoral llegase a estar comprometida, entonces ellos eligen los cinco números con más vocales de mesa comprometidos.

De lo contario, por cada uno de los cinco números sorteados se determina con cierta

probabilidad si los miembros comprometidos de la junta electoral logran alterar el sorteo, y si fallan o no hay miembros comprometidos, se realiza el sorteo normal de ese número de forma aleatoria. La probabilidad mencionada corresponde al complemento de la probililidad de que fallen, la cual es calculada como una probabilidad base si es un miembro comprometido, y esta probabilidad base al cuadrado si son dos. La probabilidad base es PROB_FAILURE si PROBABILIDAD_COMPUESTA es $false$, y si es $true$ entonces por cada alteración exitosa se promedia PROB_FAILURE con 1.

Para finalizar el sorteo anterior, se registran cuántos vocales maliciosos se obtuvieron en cada mesa de votación.

Conteo de votos

Como los datos vienen separados por mesa y candidato, no se tienen inmediatamente los resultados de quién salió elegido en cada cargo. Es por esto que se debe hacer un proceso de conteo de votos por cada división electoral, encontrando el total de votos de cada candidato, y usando la información de cuántos parlamentarios se eligen por zona, se encuentra la lista de los ganadores.

Luego de contar los votos de cada candidato, se ve quién salió elegido mediante el sistema de D'Hondt descrito en el capítulo 4.2.5.

Como resultado adicional de este conteo, también se encuentra al candidato por cada división electoral a favorecer en la edición de votos. Para esto se ve cuál pacto es el que requiere menos votos adicionales para obtener otro candidato elegido, y se le agregan los votos al candidato con más votos de ese pacto que no fue electo. Esta elección de candidato encuentra al candidato para el cual es más fácil alterar el resultado de la elección.

Alteración de votos

La función de alteración de resultados tiene dos maneras de funcionar

- Si se le da como parámetro a un candidato, la alteración favorecerá a ese candidato si es que está presente en la lista de candidatos del distrito o circunscripción senatorial.
- Si no se le da ningún candidato, la junta electoral maliciosa simulada posee un parámetro indicando a qué pacto apoyaría, y se favorecerá el candidato con la mayor cantidad de votos de ese partido. Las simulaciones finales no usaron esta opción.

Como en la sección anterior se obtuvo el candidato que no fue elegido con la mayor cantidad de votos en cada división electoral, se optó por favorecer a éste.

En la simulación, lo primero que se revisa es si la cantidad de vocales comprometidos en la mesa a alterar alcanza la cantidad THRESHOLD_VOCALES. Si no la alcanza se considera que con probabilidad

$$\rho = 1 - p^n$$

se altera el resultado, el valor de p corresponde a PROB_VOCAL_MESA, y n corresponde al número de vocales de mesa comprometidos en ésta. Si los dos chequeos anteriores fallan, entonces los resultados de la mesa no se alteran.

Cuando los chequeos son exitosos, se encuentra el candidato que recibirá más votos, como se explicó anteriormente. Si no hay ningún candidato del partido al que favorece una junta, tampoco se altera el resultado.

Luego se encuentra la cantidad de votos a agregar al candidato, usando el parámetro PORCENTAJE_EDICION, y se procede a agregar estos votos. Como una medida para evitar que la alteración sea descubierta mediante comparación con otros documentos oficiales como el libro de firmas de votantes, se busca mantener la cantidad de votos totales de la mesa.

Para mantener la cantidad de votos, se quitan votos de manera equitativa a los demás candidatos de la mesa. Por ejemplo si se quieren agregar 100 votos a un candidato, y hay 11 candidatos en la mesa, se le quitan 10 votos a los otros 10 candidatos, manteniendo el total. En caso de que un candidato tenga menos votos que la cantidad que se le debe quitar, no se le quitan, ya que es más probable que se encuentre una alteración si un candidado, sabiendo que tenía votos en una mesa, ve que al final no tiene ninguno. Los votos que no se le quitan al candidato de pocos votos se le quitan al resto.

Una forma de lograr que las alteraciones logren hacer que el candidato favorecido sea elegido puede ser quitar más votos al candidato elegido con la menor cantidad de votos, pero esto tiene dos problemas:

- Es más probable que la diferencia de votos sea descubierta.
- Los vocales de mesa no tienen forma de saber quién será el candidato que saldrá último de los elegidos, sólo pueden saber los resultados de su propia mesa.

por lo tanto no se consideró esta forma de alteración de resultados.

Finalmente se cuenta el resultado de la elección con las alteraciones y se comparan.

5.3. Resultados y Análisis

Para los experimentos se corrió la simulación a lo largo de todo el país, obteniendo los resultados originales y alterados de cada distrito electoral para diputados como se describió anteriormente.

De los experimentos realizados mediante la variación de los parámetros con los valores descritos en la sección anterior, se obtuvo de cada uno tres resultados:

- Miembros de juntas electorales comprometidos
- Vocales de mesa comprometidos
- Candidatos cambiados

A continuación se muestran los resultados generales de la simulación.

Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
69.7	9143.2	1.03

Tabla 5.2: Resultados generales de la elección.

Por la gran cantidad de datos obtenidos, se mostrarán los promedios de los tres valores descritos anteriormente, agrupando los resultados por valores específicos de parámetros y obteniendo el promedio de los experimentos que usaron ese valor en todas las combinaciones evaluadas. Estos resultados son usados principalmente para comparar el efecto que tiene la variación de un parámetro, y no para ver el número particular del promedio, que es afectado por valores extremos como los obtenidos con grandes porcentajes de juntas comprometidas o edición de votos.

Para evaluar más en detalle ciertos parámetros estudiados, también realizamos experimentos en que se dejaron fijos todos los parámetros excepto uno, variando este en pequeños incrementos y ejecutando experimentos cada vez. Como los experimentos dependen de probabilidades y pueden variar cada vez, se ejecutó cada conjunto de parámetros 10 veces y se trabajó con el promedio obtenido.

Además, por la gran cantidad de parámetros estudiados, se presentan los resultados e inmediatamente su análisis, para una lectura más fácil del trabajo.

5.3.1. Probabilidad compuesta

Resultados

Prob. Compuesta	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
No	70.0	9210.9	1.01
Sí	69.3	9075.6	1.05

Tabla 5.3: Resultados agrupados por inclusión de probabilidad compuesta (PROBABILIDAD_COMPUESTA).

Análisis

Como las probabilidades de alterar sorteos usadas en las simulaciones ya son bajas, reducirlas aún más mediante la probabilidad compuesta estudiada tuvo un efecto muy reducido en la cantidad de candidatos efectivamente cambiados.

5.3.2. Límite de vocales

Resultados

Límite Vocales	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
3	69.5	9117.1	1.13
5	69.9	9169.4	0.92

Tabla 5.4: Resultados agrupados por valores de límite de vocales (asociado a parámetro TRESHOLD_VOCALES).

Análisis

Se ve que aumentar el requerimiento para poder alterar con 100 % de probabilidad los resultados de una mesa de 3 a 5 vocales, disminuye la cantidad de candidatos cambiados en un 18 %. El motivo para considerar sólo tres vocales para el 100 % en la simulación fue porque tres de los vocales tienen cargos importantes que manipulan actas de votación. Para mejorar la seguridad se podría distribuir la responsabilidad de los vocales, para que cada vocal sea igualmente importante en los procesos que se realizan en una mesa y en el contacto con las actas de votación, haciendo imposible que sólo 3 vocales deban ponerse de acuerdo para alterar resultados.

5.3.3. Porcentaje de edición

Resultados

Porcentaje Edición	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
50 %	69.6	9163.3	0.57
70 %	69.7	9101.5	1.03
90 %	69.7	9164.9	1.48

Tabla 5.5: Resultados agrupados por valores de porcentaje de edición de votos por los vocales de mesa (asociado a parámetro PORCENTAJE_EDICION).

Análisis

Respecto al porcentaje de edición de votos por parte de las mesas que logran cambiar resultados, vemos que frente a aumentos de 20 % en la cantidad de votos para el candidato favorecido, se aumenta en cantidades cercanas a 0.4 candidatos. Esto corresponde a un aumento de más del 80 % en la cantidad de candidatos cambiados. Para detectar este tipo

de ataques, se propone una auditoría estadística que será descrita en una sección posterior, la cual tiene una mayor probabilidad de encontrar este tipo de alteraciones entre más votos sean cambiados por los vocales de mesa.

5.3.4. Probabilidad de éxito de vocal de mesa

En esta sección revisamos el efecto (expresado en número de candidatos electos cambiados) al variar la probabilidad de que un vocal de mesa malicioso realice un ataque exitoso.

Resultados

Prob. Vocal Mesa	**Miembros de juntas comprometidos**	**Vocales comprometidos**	**Candidatos electos cambiados**
20 %	69.5	9116.0	2.16
10 %	69.9	9179.0	0.75
5 %	69.7	9134.7	0.18

Tabla 5.6: Resultados agrupados por valores de probabilidad de éxito de un vocal en la edición de votos (relacionado a parámetro PROB_VOCAL_MESA).

Por la gran variación en la cantidad de candidatos cambiados, se estudió este parámetro con más detalle, llegando a los siguientes resultados.

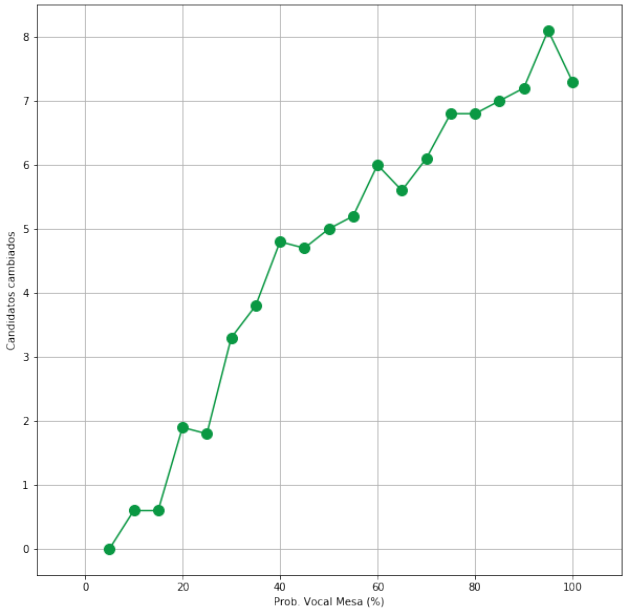


Figura 5.1: Candidatos cambiados en función de la probabilidad de éxito de un vocal al intervenir actas.

Análisis

Frente a una disminución en la probabilidad de éxito por parte de los vocales de mesa comprometidos al intentar alterar votos, se ve que la cantidad de candidatos cambiados varía en un gran porcentaje. Al disminuir el éxito de 20 % a 10 %, los candidatos cambiados disminuyeron a menos de un tercio, y lo mismo ocurre cuando baja la probabilidad de éxito de 10 % a 5 %. La Figura 5.1 refuerza estos resultados, mostrando un crecimiento relativamente lineal a medida que la probabilidad de éxito aumenta. Esto muestra que hacer más difícil el trabajo de alterar actas tiene un efecto significativo al momento de querer aumentar la seguridad de las elecciones. Para hacer las alteraciones más difíciles de realizar, se pueden realizar capacitaciones para vocales de mesa, donde se enseñe a reportar a las autoridades cualquier comportamiento extraño que se vea por parte de otros vocales de mesa; y también haciendo que los procesos más públicos y concurridos, ya sea por parte del público general (por ejemplo fomentando la difusión de las partes públicas de las actas por redes sociales o vía crowdsourcing), o fomentando la presencia de apoderados de mesa de los partidos políticos.

5.3.5. Probabilidad de éxito de miembro de la junta

Resultados

Prob. Éxito Miembro Junta	**Miembros de juntas comprometidos**	**Vocales comprometidos**	**Candidatos electos cambiados**
30 %	70.0	9363.4	1.14
20 %	69.3	9126.1	1.02
10 %	69.7	8940.2	0.92

Tabla 5.7: Resultados agrupados por valores de probabilidad de éxito por parte de un miembro de la junta electoral para alterar el sorteo (asociado a parámetro PROB_FALLA).

Análisis

Cuando se disminuye la probabilidad de éxito de alteración del sorteo de vocales de mesa, se ve que hay una tendencia a la disminución en la cantidad de vocales de mesa cambiados. Con el objetivo de llevar esta probabilidad a 0 %, se propone el uso de aleatoriedad verificable para el sorteo, la que será descrita en un capítulo posterior.

5.3.6. Probabilidad de junta comprometida

Resultados

Prob. Junt. Comp.	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
10 %	35.0	4565.7	0.34
20 %	69.6	9137.3	0.94
30 %	104.4	13 726.7	1.81

Tabla 5.8: Resultados agrupados por valores de probabilidad de que un miembro de una junta electoral sea corrupto (asociado a parámetro PROB_JUNT_COMP).

Análisis

Respecto a la probabilidad de que los miembros de la junta estén comprometidos, la cantidad de miembros de juntas comprometidos y vocales de mesa comprometidos son directamente proporcionales a este cambio. Un aumento de 10 % a 20 % casi triplica los candidatos cambiados, mientras que el aumento de 20 % a 30 % los duplica. Esto muestra que las elecciones son sensibles a que estos altos cargos se vean afectados. Actualmente ya es una buena idea el tener como miembros de las juntas electorales a personas con cargos importantes como lo son notarios o los fiscales, pero también sería interesante considerar que las personas a cargo vayan rotando, para así no mantener posibles miembros comprometidos por más de un período de elección.

5.3.7. Probabilidad de encontrar vocales y cantidad de vocales

Resultados

Prob. Encontrar Vocal	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
40 %	69.8	7398.9	0.70
60 %	69.5	10 887.6	1.36

Tabla 5.9: Resultados agrupados por valores de probabilidad de que un miembro comprometido de una junta encuentre un vocal comprometido para el sorteo (asociado a PROB_ENCONTRAR_VOCAL).

También se estudió este parámetro con más detalle, llegando a los siguientes resultados.

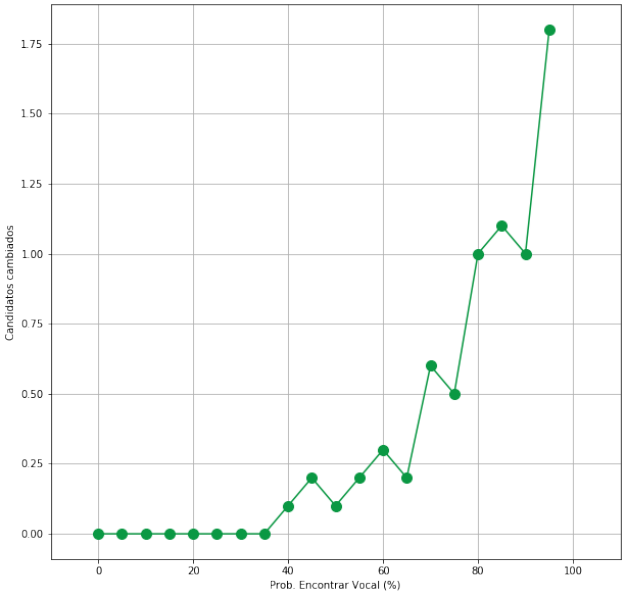


Figura 5.2: Candidatos cambiados en función de la probabilidad de encontrar vocales corruptos.

Candidatos Máximos por Miembro	**Miembros de juntas comprometidos**	**Vocales comprometidos**	**Candidatos electos cambiados**
3	69.4	6929.9	0.57
5	69.9	11 356.6	1.48

Tabla 5.10: Resultados agrupados por cantidad máxima de vocales de mesa comprometidos que puede tener un miembro de junta comprometido (asociado a parámetro CANDIDATOS_MIEMBRO).

Análisis

La probabilidad de encontrar posibles vocales de mesa comprometidos por parte de las juntas, en ambos casos, muestra que al aumentar de un 40 % a 60 %, es decir, un aumento de un 50 %, también sube la cantidad de vocales comprometidos en casi 50 %, y cambia los resultados cambiados a casi el doble. El mismo efecto se observa cuando se aumenta la cantidad de vocales comprometidos que se intenta agregar a la lista, donde un aumento de un 66 % casi triplica los candidatos cambiados. La Figura 5.2 también muestra este comportamiento, mostrando un crecimiento acelerado en la cantidad de candidatos cambiados a medida que se aumenta la probabilidad de encontrar vocales de mesa. Esto muestra que reducir tanto la probabilidad como el número de potenciales vocales es una forma efectiva de disminuir el riesgo de una elección comprometida. Para esto se debe aumentar la fiscalización y educar a la población de la importancia de las tareas de los vocales de mesa para la democracia, y también informar de las penas asociadas a los vocales de mesa que alteran las votaciones.

5.3.8. Probabilidad de junta comprometida y de encontrar vocal

Se estudió la variación en el caso de que se agrupara por estos dos parámetros al mismo tiempo.

Resultados

Prob. Junt. Comp	Prob. Encontrar Vocal	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
10 %	40 %	35.2	3657.8	0.21
10 %	60 %	34.9	5473.6	0.46
20 %	40 %	69.5	7354.3	0.63
20 %	60 %	69.8	10 920.2	1.24
30 %	40 %	104.9	11 184.4	1.25
30 %	60 %	103.9	16 268.9	2.38

Tabla 5.11: Resultados agrupados por valores de probabilidad de miembros de junta comprometida y probabilidad de encontrar vocales comprometidos para el sorteo (parámetros PROB_JUNT_COMP y PROB_ENCONTRAR_VOCAL).

Análisis

Al agrupar las dos probabilidades anteriores, vemos que en promedio la cantidad de candidatos cambiados para los valores más bajos es mínima, llegando a sólo 0.2 cambiados en promedio. En consecuencia, si se aplican medidas para disminuir los valores de estos parámetros, se pueden evitar la mayoría de las alteraciones a las votaciones.

5.3.9. Sorteo individual por mesa

Como una forma de evaluar si lo que se realiza actualmente es la mejor opción en términos de seguridad, también analizamos una variante donde el sorteo de los vocales de mesa se realiza de manera individual para cada mesa, es decir, si hay un conjunto de cinco números para cada mesa. Si bien esta variante no es parte de los procesos de selección válidos realizados por las juntas electorales, decidimos analizarlos por ser una variante práctica a considerar.

En estos casos un miembro comprometido de la junta electoral puede intentar alterar el sorteo en cada instancia, beneficiando a sus candidatos en cada momento, en vez de elegir los números que en promedio le dan más candidatos comprometidos a lo largo de todas las mesas. En este caso también se considera que si toda la junta es maliciosa, se eligen todos los vocales maliciosos que se puedan, en todas las mesas por separado. De lo contrario se realiza el mismo proceso descrito anteriormente para la probabilidad de alterar el sorteo, y en caso de ser exitoso se agrega un vocal comprometido para esa mesa en particular, de lo contrario

se elige un al azar. Este proceso de sorteo y posibles alteraciones se hace en cada mesa de votación asociada a la junta.

Resultados

Los valores generales obtenidos en el caso de realizar un sorteo por mesa, son los siguientes:

Tipo Sorteo	**Miembros de juntas comprometidos**	**Vocales comprometidos**	**Candidatos electos cambiados**
Por mesa	69.5	24 290.2	3.76
Por junta	69.7	9143.2	1.03

Tabla 5.12: Resultados en caso de sorteo de mesa, comparado con el sorteo por junta.

El resto de los resultados de este caso de simulación se encuentran en el Anexo B.

Para visualizar mejor el efecto de cambiar el tipo de sorteo, se decidió graficar los vocales corruptos de una elección en función de la probabilidad de éxito de la alteración del sorteo de vocales, mostrando el caso de sorteo general por Junta, y el sorteo por mesa. Los resultados son los siguientes:

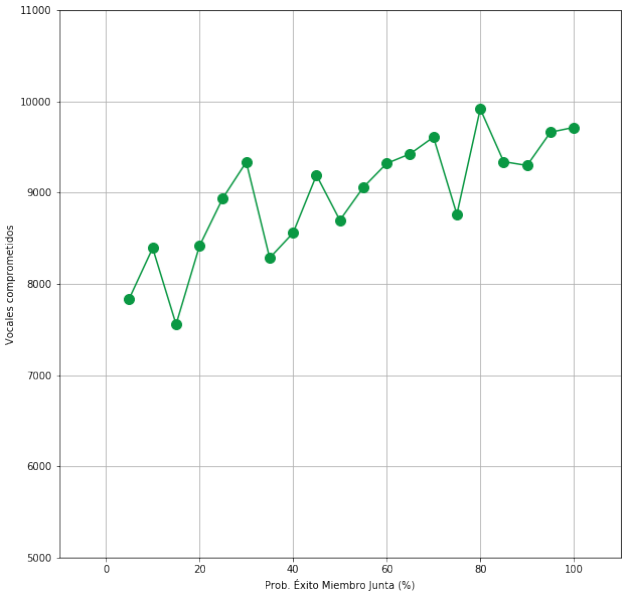


Figura 5.3: Vocales corruptos en función de la probabilidad de éxito de alteración de sorteo por Junta Electoral.

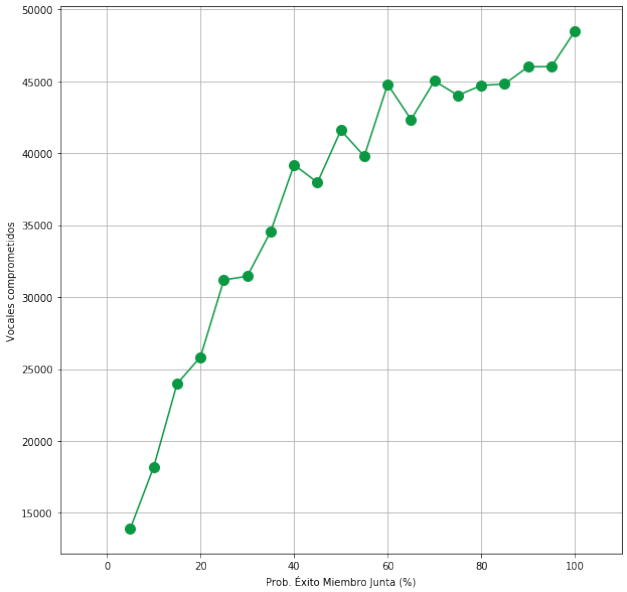


Figura 5.4: Vocales corruptos en función de la probabilidad de éxito de alteración de sorteo por mesa.

Análisis

El resultado más relevante es que, a lo largo de todas las tablas de resultados, se ve que el sorteo por mesa tiene muchos más vocales corruptos y candidatos cambiados que el sorteo por junta, llegando a tener casi tres veces la cantidad de vocales corruptos y cuatro veces la cantidad de candidatos cambiados en promedio. Con esto se ve que hoy en día es una buena idea tener el sorteo único por junta, ya que minimiza el posible actuar malicioso por parte de miembros de juntas electorales.

Por último, otro resultado relevante de estos experimentos es la probabilidad de fallo de las juntas comprometidas para alterar sorteos. Cuando se realiza el sorteo por mesa hay un cambio mucho más pronunciado en la cantidad de candidatos cambiados comparado con el sorteo por junta. Esto se ve más claramente en las Figuras 5.3 y 5.4, donde se ve que al disminuir la probabilidad en el sorteo por mesa causa un decrecimiento en la cantidad de vocales de mesa comprometidos en cada intervalo, mientras que el sorteo por junta tiene resultados distintos, donde se ve una oscilación en los resultados, pero frente a probabilidades más bajas vemos una tendencia a tener menos vocales comprometidos. La poca diferencia se debe a que los miembros de la junta deben encontrar los números con la mayor cantidad de vocales comprometidos en el sorteo, pero cuando los eligen también se ven obligados a elegir vocales no comprometidos en una gran parte de las mesas, restricción a la que no están sujetos cuando el sorteo se realiza por mesa.

5.3.10. Elección distinta de candidato para modificación de votos

Para las simulaciones anteriores, se consideró que los vocales maliciosos editan las actas agregándole votos al candidato que quieren beneficiar, aumentando en un porcentaje la cantidad de votos del candidato, proporcional a los votos que ya obtuvo. El sistema de D'Hondt permite una segunda forma de beneficiar a un candidato (o a una lista): realizar el mismo

proceso de adición de votos proporcionales a los ya obtenidos, pero agregándole más al candidato que ya tiene más votos, agregando más votos al pacto, que finalmente beneficiarán a los candidatos que no serían elegidos normalmente.

Resultados

Los resultados generales simulados de este tipo de ataque son los siguientes:

Tipo Asignación	**Miembros de juntas comprometidos**	**Vocales comprometidos**	**Candidatos electos cambiados**
Mayor del pacto	69.5	9128.7	1.37
Mayor no electo	69.7	9143.2	1.03

Tabla 5.13: Resultados en caso de asignación al mayor del pacto, comparado con caso de asignación a candidato a elegir.

El resto de los resultados de este caso de simulación se encuentran en el Anexo B.

El análisis de esta simulación se presenta en conjunto con el análisis de la siguiente variación a la simulación.

5.3.11. Elección por mayoría simple

A fin de evaluar una nueva variación para la simulación, se consideró el caso en que la elección de diputados se haga por mayoría simple una vez contados los votos, en vez de considerar el sistema D'Hondt. En este caso los vocales intentan favorecer al candidato con la mayor cantidad de votos que no fue elegido.

Resultados

Los resultados son los siguientes:

Tipo Elección	**Miembros de juntas comprometidos**	**Vocales comprometidos**	**Candidatos electos cambiados**
Mayoría simple	69.4	9013.6	1.07
D'Hondt	69.7	9143.2	1.03

Tabla 5.14: Resultados en caso de mayoría simple, comparado con sistema D'Hondt.

El resto de los resultados de este caso de simulación se encuentran en el Anexo B.

Análisis

Cuando se considera darle votos al candidato con más votos de un pacto, se ve que hay un aumento cercano al 40 % en candidatos cambiados al comparar con el caso original simulado. Esto muestra que el sistema D'Hondt permite ataques más efectivos al momento de alterar las elecciones, ya que al comparar con el caso de mayoría simple, se observa que los resultados son muchos más cercanos a la primera simulación, aunque ligeramente peores. A pesar de los peores resultados, el sistema D'Hondt tiene otros beneficios para la elección de candidatos (mejor representatividad de la población), por lo que, en nuestra opinión, no se justifica un cambio. Esta decisión también es respaldada por la simulación con elección por mayoría simple, donde vemos que al comparar el caso original de sistema D'Hondt y la elección por mayoría simple, el sistema D'Hondt logra menos candidatos cambiados a lo largo del país, con la mayoría simple obteniendo un 3 % más de candidatos cambiados.

5.3.12. Datos generales

Para el escenario estudiado con el modelo actual de sorteos, de los 1296 casos, 556 resultaron con algún resultado cambiado. De estos, 222 corresponden a un diputado cambiado, 139 a dos diputados, y el resto varía entre 3 y 11, disminuyendo la frecuencia a medida que el número aumenta. Esto es interesante ya que aunque el promedio general obtenido es cercano a uno, los peores casos muestran una mayor cantidad de distritos en donde los resultados pueden alterarse.

Revisando un caso en particular, con los siguientes valores para los parámetros:

- Porcentaje Edición: 50 %
- Prob. Vocal Mesa: 20 %
- Límite Vocales: 5
- Probabilidad Compuesta: Sí
- Candidatos Miembro: 3
- Prob. Éxito Miembro Junta: 20 %
- Prob. Junt. Comp.: 20 %
- Prob. Encontrar Vocal: 60 %

En dicho caso, se logró alterar el resultado de un distrito, logrando cambiar el resultado de una diputada. En particular se cambia a Joanna Pérez Olea, del pacto Convergencia Democrática, por María Ríos Aycaguer, del pacto Chile Vamos, en el distrito 21.

En el Distrito 21, hay 11 juntas electorales, es decir 33 miembros totales en la región. Al fijar la probabilidad de tener un miembro comprometido en 20 % se tiene un valor esperado de 6.6 miembros maliciosos, siendo 6 el valor real de miembros de juntas comprometidos obtenidos en la simulación. Estos 6 miembros de junta electoral consiguieron un total de 637 vocales de mesa, pero sólo 20 % de éstos fueron exitosos en su tarea, por lo que efectivamente sólo se necesitaron 127 vocales para alterar el resultado.

El cambio de resultado en este distrito se debe al sistema D'Hondt, en donde la candidata que ganó en la elección pasada tenía cerca de 12000 votos, y la que la reemplazó en la

simulación sólo cerca de 9600, pero al agregarle cerca de 700 votos, la gran cantidad de votos de los otros miembros del pacto (33000 y 22000) lograron que esta candidata con menos votos saliera elegida. Como en este caso vemos que al tener 637 vocales de mesa alterando una diferencia de 700 votos se logra cambiar un resultado, podemos ver que en promedio cada vocal de mesa que logra cambiar resultados agregó un poco más de un voto a la candidata que se favoreció. Este bajo número promedio abre la posibilidad para que otras formas de alteración de resultados sean posibles, como lo es el *ballot stuffing*, mencionado en la sección de trabajo futuro al final de este trabajo.

Capítulo 6

Escrutinio Posterior

6.1. Descripción del Proceso

6.1.1. Antes del escrutinio

Con el propósito de comprobar los resultados obtenidos en el día de la elección, se convoca un grupo de personas denominado el Colegio Escrutador [2]. Cada Junta Electoral escoge al menos uno de estos colegios, en un proceso de selección similar al de vocales de mesa. Esto es:

- Cada miembro de la junta electoral crea una nómina de 20 personas como potenciales miembros del Colegio Escrutador. El criterio especificado para nominar a estas personas es indicar una lista de quienes los miembros de la Junta Electoral consideren más aptos para el cargo.
- Se realiza un sorteo público para elegir los candidatos, eligiendo cinco personas de esta lista de forma aleatoria, y se repiten cinco miembros del Colegio Escrutador de la elección anterior. Si es un Colegio Escrutador nuevo, se sortean los diez miembros.

Los elegidos son notificados por carta a su domicilio, y el Secretario de la Junta Electoral publica la lista de miembros, de acuerdo a la ley 18.700.

Además de los 10 miembros aleatorios, el Consejo del Servicio Electoral nombra a un Secretario del Colegio Escrutador, encargado de presidir el proceso de escrutinio. La labor cae preferentemente en "notarios, secretarios de juzgados de letras y en auxiliares de la administración de justicia u otros ministros de fe", aunque teóricamente cualquiera podría ser seleccionado en este rol si el Servicio Electoral quisiera.

6.1.2. Escrutinio

Se realiza el día siguiente al día de elecciones. Asisten a éste el Secretario del Colegio Escrutador y los miembros del Colegio, los cuáles deben sortear entre ellos un presidente que lidere al equipo.

Una vez constituido el Colegio con los miembros necesarios, se llena un acta dejando constancia de los miembros.

Para el escrutinio, el Colegio Escrutador revisa el acta de votos que se creó en cada mesa y que fue entregada al Delegado de la Junta Electoral (que no es la misma acta usada para subir la información publicada el día de las elecciones). Con esta acta, se cuentan los votos de cada candidato en cada mesa, para sumarlos e ingresar los datos a un sistema computacional, que también muestra los datos ingresados el día anterior para poder realizar comparaciones [2]. Este proceso también puede ser observado por apoderados de partidos políticos.

Si se encontrasen errores en el ingreso de los datos en el sistema del día anterior o en el correcto llenado del acta, se ingresarán los datos al sistema de todas formas, dejando constancia en éste de los errores encontrados.

Luego de esto se generan copias de todos los datos ingresados, para que cada miembro del Colegio Escrutador y apoderados presentes revisen la información y encuentren posibles errores en lo que ellos ingresaron, no en la información del día anterior. Si todos están de acuerdo en corregir un error entonces se modifica la información.

Finalmente, se generan tres actas: una queda en el Libro de Actas, otra es entregada al presidente del Tribunal Calificador de Elecciones y la última es recibida por el Director del Servicio Electoral.

Un supuesto importante para el correcto funcionamiento del proceso de escrutinio posterior es que la comparación de actas se haga de la forma descrita por la ley, es decir, todo el Colegio Escrutador revise al mismo tiempo una mesa, y no se dividan en grupos para hacer el trabajo más rápido. Si no es así, los ataques descritos en la sección siguiente se podrían realizar más fácilmente.

6.1.3. Flujo de información

A continuación se muestra una versión resumida del flujo de información del proceso de escrutinio posterior.

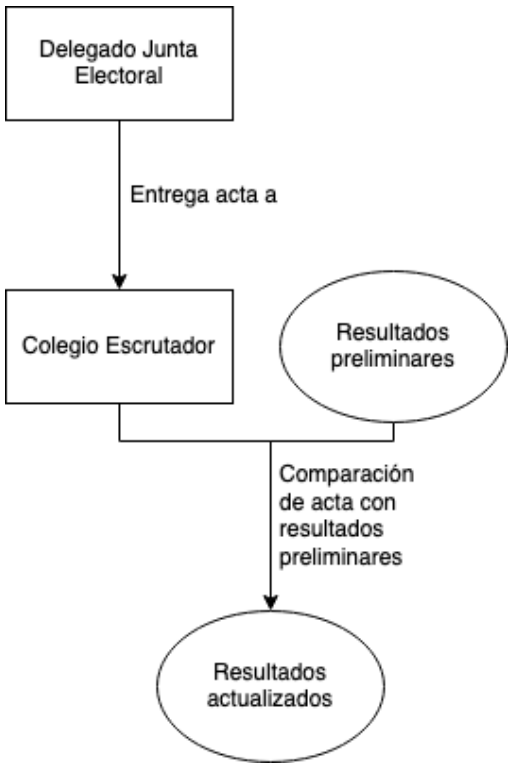


Figura 6.1: Flujo de información del escrutinio posterior.

6.2. Casos de Ataque al Escrutinio

A continuación se analizarán casos de potenciales ataques al proceso de Escrutinio descrito en la sección anterior.

6.2.1. Miembros del Colegio intentan cambiar resultados en el escrutinio

Al igual que en las secciones anteriores de este trabajo, es posible hacer una simulación de los cambios que puede generar un Colegio malicioso. Éstos involucran reportar un resultado distinto al original por medio del software de reporte de datos, o incluso modificar el acta de resultados que reciben del día de la votación. No realizamos una simulación para dichos casos puesto que estos ataques son detectables, como veremos en el capítulo de análisis.

6.2.2. Miembros del Colegio coludido con vocales de mesa corruptos

En este escenario, si los vocales de mesa ya fueran corruptos, éstos ya podrían haber modificado los resultados y esto se vería reflejado en las actas. El Colegio podría actuar normalmente y aceptar los resultados cambiados, o trabajar de forma similar al caso anterior, modificando aún más los resultados de la votación.

6.2.3. Colusión con digitador

En este tipo de ataque, consideramos el caso donde el digitador modifica los resultados que debía ingresar al sistema informático el día de la elección, y el Colegio Escrutador está al tanto de aquello, dejando pasar estos cambios y declarando que la mesa que fue alterada no tiene conflictos.

Capítulo 7

Tribunal Calificador de Elecciones

Durante el desarrollo de esta tesis, nos enteramos de la existencia del Tribunal Calificador de Elecciones. Aunque originalmente no estaba contemplado incluir esta parte del proceso de elecciones dentro de nuestra investigación, el TRICEL posee una labor fundamental en el desarrollo de las elecciones y la publicación de resultados. Su rol no puede quedarse fuera de esta investigación sobre las elecciones chilenas, por lo que en esta sección analizaremos los procesos que lo involucran.

7.1. Descripción

El Tribunal Calificador de Elecciones (TRICEL) es un organismo compuesto por cinco miembros, cuya labor es actuar de jurado frente a la correcta realización de las elecciones de Presidente, Diputados y Senadores, resolviendo reclamos a las elecciones y proclamando a los candidatos elegidos [1].

Los cargos dentro del Tribunal duran cuatro años y los cinco cupos son sorteados de la siguiente forma:

- Uno entre quienes hayan desempeñado los cargos de Presidentes o Vicepresidentes de la Cámara de Diputados por más de un año.
- Uno entre quienes hayan desempeñado los cargos de Presidentes o de Vicepresidentes del Senado por más de un año.
- Dos entre quienes desempeñen los cargos de Ministros de la Corte Suprema.
- Uno entre quienes desempeñen los cargos de Ministros de la Corte de Apelaciones de la ciudad donde celebre sus sesiones el Congreso.

7.2. Proceso de Escrutinio General

El TRICEL se reúne después de que el Colegio Escrutador realiza su trabajo, y mediante la ayuda de sistemas computacionales y actas, revisa los resultados todas las mesas de votación del país de norte a sur. Esto se realiza en las sesiones diarias que sean necesarias para revisar

las mesas de todo el país, las cuales son públicas, y los candidatos pueden asistir hasta con dos apoderados.

Si una mesa no tiene reclamos por parte de candidatos ni de los colegios escrutadores, el TRICEL simplemente revisa que su ejemplar del acta del día de votación coincida con lo que muestre el sistema computacional, y si todo está correcto pasa a la siguiente mesa.

Si se encuentra algún problema, ya sea uno reportado por el Colegio Escrutador o por reclamo de un candidato, el TRICEL usa los ejemplares de las actas que tiene, tanto de la elección como del Colegio, para determinar cuál es el resultado correcto. En última instancia puede solicitar los votos de la mesa y recontarlos.

Frente a un error en el conteo original, y si el error puede significar un cambio en el resultado de la elección, el TRICEL puede llamar a hacer nuevamente la votación en las mesas afectadas.

Luego de hacer todos los procesos anteriores, se procede a proclamar a los candidatos que fueron elegidos, dando origen a los resultados oficiales de las elecciones.

Este proceso depende de la correcta revisión de las actas de las mesas, incluso en casos en que no hay reclamos, para evitar un ataque como uno de los escritos en la siguiente sección.

7.2.1. Flujo de información

A continuación se muestra un resumen del flujo de información del proceso de calificación de elecciones por el TRICEL.

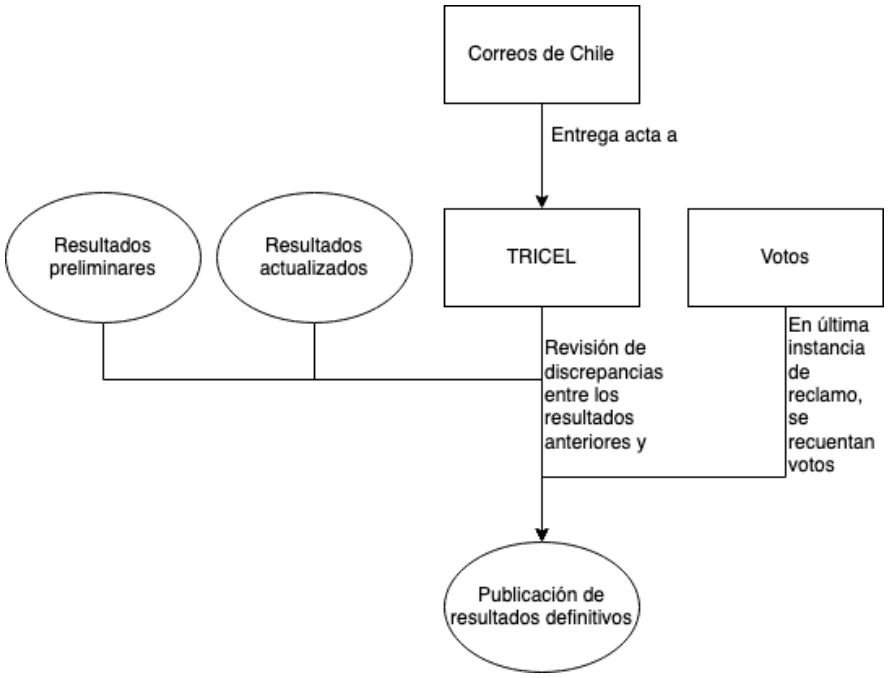


Figura 7.1: Flujo de información del TRICEL.

7.3. Casos de Ataque al Escrutinio General

7.3.1. TRICEL intenta alterar resultados

Si bien es en principio posible que el TRICEL intentase alterar los resultados (los resultados reportados por esta entidad no pueden ser objetados), el proceso de escrutinio general es realizado con candidatos presentes, principalmente los que realizaron reclamos al proceso de conteo de votos, por lo tanto éstos prestarán atención al escrutinio, significativamente facilitando la detección de posibles alteraciones.

7.3.2. Hackeo general a sistemas computacionales

En este caso extremo, todos los sistemas computacionales que el Servicio Electoral utiliza en el proceso electoral pudiesen ser controlados por un agente malicioso.

Por ejemplo, el sistema computacional de envío de datos el día de la elección podría enviar resultados alterados cuando el digitador reporta los resultados correctos. Además, en el día del escrutinio posterior, el Colegio Escrutador vea en el sistema computacional los resultados correctos, a pesar de que los resultados publicados sean los alterados. Esto se debe a que el caso en que los Colegios Escrutadores vean los resultados alterados en el sistema es equivalente al caso en que el sistema computacional sea hackeado el día de las elecciones, descrito en la sección 4.3.3.

Capítulo 8

Análisis Global

A continuación analizamos los distintos ataques mencionados en este trabajo, proponiendo y evaluando mitigaciones. Al final de este capítulo se muestra una tabla resumen con los ataques y las medidas propuestas.

8.1. Antes de las Elecciones

8.1.1. Miembros de la junta comprometidos

Estos casos fueron estudiados y analizados en el Capítulo 5. El efecto neto reportado fue que es posible que unos pocos miembros comprometidos de algunas Juntas Electorales logren incluir vocales de mesa corruptos en el proceso.

Para mitigar este tipo de ataque se propuso el uso del Faro de Aleatoriedad para la realización de sorteos, descrito en el capítulo siguiente, y la rotación de miembros de Juntas Electorales.

8.1.2. Intento de alterar resultados al momento de realizar el sorteo por parte de un tercero

El agente externo pudiera intentar alterar los resultados de dos formas: cambiando el vocal seleccionado o cambiando el número de sorteo seleccionado.

El primer caso no se considera viable, puesto que el vocal que se debe seleccionar es el asociado a un número específico de una lista de 30 personas ordenadas alfabéticamente, por lo tanto para lograr cambiar un resultado correctamente debería sustituirse por alguien que ocuparía el mismo lugar en la lista, lo que tiene una baja probabilidad de cumplirse.

El segundo caso tampoco se considera viable, porque para este tipo de ataque se consideró que la probabilidad de alterar el sorteo es menor a la que tienen los miembros de la junta electoral, y revisando los resultados de los experimentos, cerca de la mitad de los experimentos resultaron con ningún resultado final alterado. Incluso más no tuvieron candidatos cambiados

en los casos de alta probabilidad de fallo de alteración del sorteo y baja probabilidad de juntas comprometidas, por lo que, en este caso, se tendría una tasa muy baja de éxito.

8.1.3. Un tercero hackea el sistema computacional usado

En esta sección, analizaremos el caso que todos los vocales terminan siendo escogidos en forma maliciosa (son corruptos) por un ataque al sistema computacional.

Se realizaron experimentos con el mismo sistema explicado en el Capítulo 5, y para realizar una comparación equivalente se consideró que todas las juntas estaban comprometidas, por lo tanto todos los vocales también son maliciosos. Esta manera de simularlo es justificada por el hecho de que alguien con acceso a modificar la lista de vocales puede agregar todos los vocales maliciosos que quiera. Junto a esto se consideró un porcentaje edición de 70 % adicional para el candidato a favorecer en cada mesa, y como resultado se obtuvo que en 24 de los 28 distritos del país se logró cambiar el resultado de la elección. Este resultado es casi imposible en la realidad ya que la cantidad de vocales de mesa comprometidos que se requieren son más de 200.000, pero el resultado detrás de esto es que frente a un hackeo del sistema computacional, la mayoría de los distritos del país son vulnerables a una alteración de resultados si se presenta este tipo de hackeo.

Para evitar este tipo de ataques, además de tener sistemas computacionales robustos, se propone el uso de la aleatoriedad verificable anteriormente descrita, verificando que la lista que se publicó con anterioridad al sorteo sea la misma que maneja la junta electoral, y así dejando en evidencia si hay una discordancia entre los resultados esperados y los reales. El publicar la lista de potenciales vocales con anterioridad también permite que un hackeo del sistema computacional se haga evidente más tempranamente, ya que una discordancia entre lo publicado y los vocales elegidos en el sorteo quedaría expuesta al momento del sorteo y no al momento de la publicación de la lista oficial de vocales de mesa.

Para poder tener los sistemas computacionales robustos mencionados en el párrafo anterior, se sugiere tener computadores sin virus y con sistemas operativos actualizados, uso de certificados para la autenticación de usuarios, cifrado de punto a punto para las comunicaciones, autenticación de múltiples factores con dispositivos móviles o mediante indicadores biométricos, servidores con interacciones en internet protegidas, servidores replicados y bases de datos redundantes. En la actualidad no sabemos qué medidas de las mencionadas ya se encuentran implementadas en los sistemas utilizados del SERVEL.

8.2. Día de las Elecciones

8.2.1. Modificación de resultados por vocales de mesa

Este es el principal caso estudiado en este trabajo, con sus efectos vistos en el capítulo 5. Viendo el flujo de información que ocurre al momento de una elección, reflejado en la Figura 8.1 (el cual resume los tres flujos mostrados en capítulos anteriores), se puede ver que el proceso depende de que la información sea traspasada correctamente en el momento en que la información fluye desde los votos contados a las actas, ya que los votos nunca más son revisados, excepto cuando en última instancia el TRICEL pudiera contar nuevamente los

votos, por ejemplo en caso de que se encuentren irregularidades entre las actas.

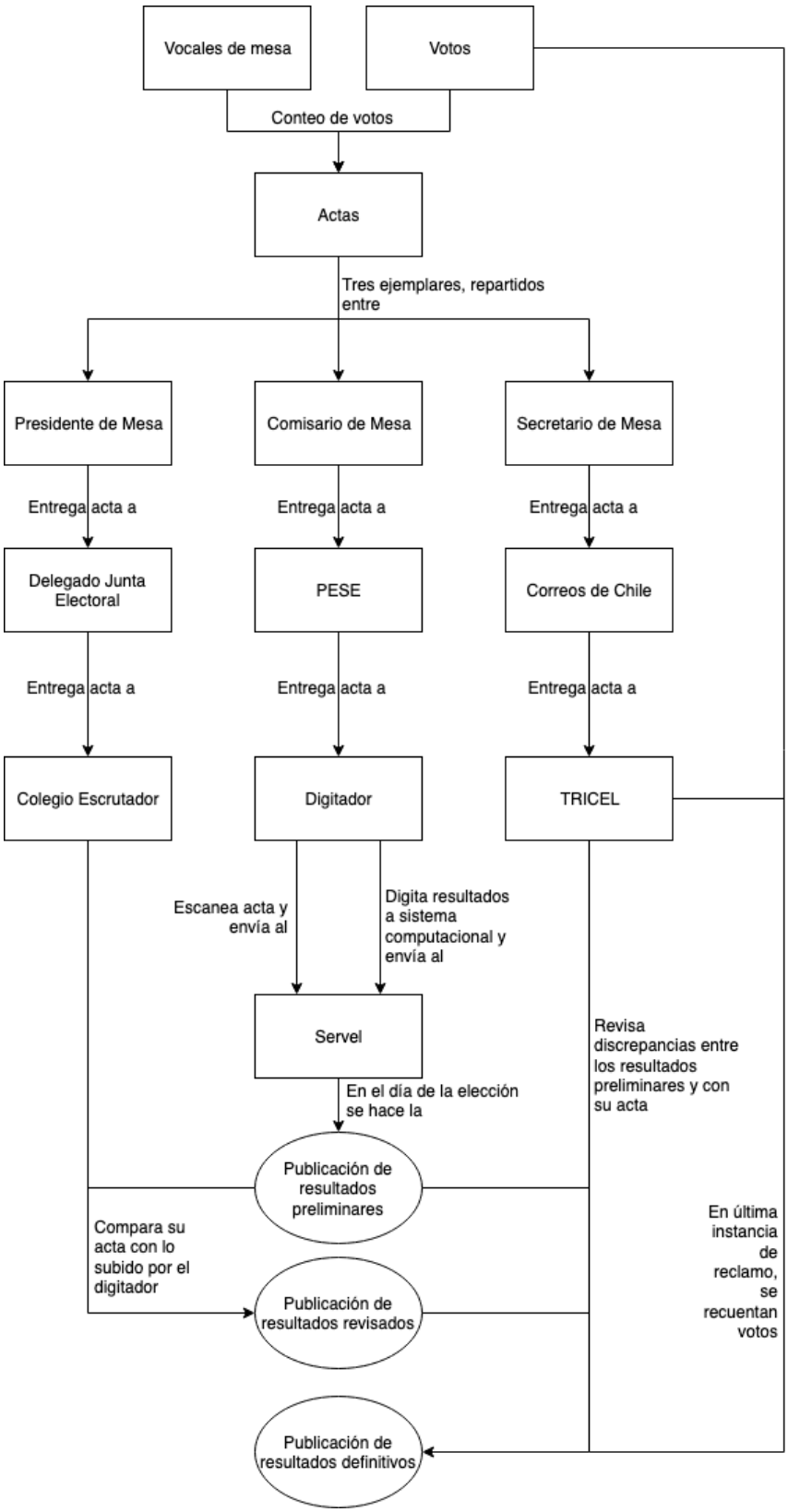


Figura 8.1: Flujo de información para los resultados de las elecciones en Chile.

Debido a que el Colegio Escrutador sólo revisa las actas, y estamos en el caso en que los vocales las modifican todas al momento de escribirlas, no es posible que este tipo de ataque sea detectado por medio del proceso de escrutinio posterior a la elección.

Para poder detectar este tipo de ataques, se propone un proceso de auditoría estadística de votos, que se describirá más adelante. Además se proponen más capacitaciones a vocales de mesa, para que reporten comportamientos sospechosos que vean en el día de la elección. Por último se debe fomentar más la participación del público general en el proceso de conteo, y de los apoderados de los partidos políticos.

8.2.2. Modificación de resultados por parte del digitador

Como se vio en el proceso de escrutinio posterior, el acta revisada es distinta a la que tiene el digitador, y por lo tanto, los valores que aparecen en el sistema en línea (publicados en tiempo real el día anterior al escrutinio) y los que ve el Colegio Escrutador son distintos, encontrándose el ataque sin problemas para su corrección.

Este tipo de alteración no afecta la elección de candidatos correctos, pero sí puede llevar a efectos secundarios como la baja en el nivel de confianza en los organismos del Estado.

Aunque el ataque no está al nivel de una alteración de resultados indetectable, también se debiera querer evitar estos ataques. Una forma es la creación de un reporte impreso por parte del sistema computacional, que se genere una vez que todas las mesas asignadas al digitador estén en el sistema, y que sea revisado y firmado por el PESE y/o el Delegado de la Junta Electoral.

8.2.3. Sistema computacional es hackeado el día de las elecciones

En este caso se supone que el sistema usado fue alterado y que se envían resultados incorrectos para ser publicados. Este caso es equivalente al anterior para efecto del Colegio Escrutador, el cual debería ver las diferencias entre lo subido y lo que dicen las actas, y así corregir los resultados.

Una diferencia en este tipo de ataque es que el digitador tiene buenas intenciones, pero no tiene forma de probar que la información que ingresó y la información que se envió es la misma.

Para esta vulnerabilidad se propone, al igual que en la anterior, la creación de una traza en papel de la información ingresada por el digitador. Ésta debe indicar los valores ingresados por el digitador, para que tanto éste como personal en el local de votación, ya sea PESE y/o el Delegado del SERVEL, comprueben el correcto ingreso de los datos. Esta traza debe ser guardada junto con una de las actas.

Así, en caso de que el digitador modifique la información ingresada, será detectado por la gente que comprueba los datos el día de la votación, y si un tercero altera los datos en un momento posterior, se sabrá que esto no es culpa del digitador, ya que tiene la evidencia respaldada por el resto del personal para defenderse.

También se propone el uso de mejores medidas de seguridad computacional, con computadores con sistemas operativos actualizados que sólo puedan conectarse a servicios del SERVEL para evitar ataques externos, mayores restricciones para la red de internet de los locales de votación y generación aleatoria de contraseñas, además de las medidas mencionadas en la sección 8.1.3.

8.3. Escrutinio Posterior

8.3.1. Colegio Escrutador cambia resultados en el escrutinio

Cualquier cambio realizado por el Colegio no es de carácter permanente, sino que debe ser aprobado en última instancia por el Tribunal Calificador de Elecciones (TRICEL).

Es el TRICEL el que, frente a discrepancias entre los resultados reportados en el día de la elección y por el escrutinio posterior, debe usar toda la información disponible, en particular las actas creadas o incluso los votos, para decidir cuál es el resultado correcto.

En el caso en que se reporte algo distinto por el sistema computacional, las actas seguirán diciendo el resultado correcto y por lo tanto el TRICEL debería reportar finalmente los resultados originales. Si el acta también es alterada, entonces el TRICEL debería ver la discrepancia entre su ejemplar del acta y el del Colegio Escrutador, y en este caso puede solicitar un reconteo de la mesa, encontrando el resultado original en última instancia.

8.3.2. Colegio coludido con vocales de mesa corruptos

En el caso en que tanto vocales de mesa como Colegio Escrutador sean corruptos, si el Colegio intenta modificar aún más los resultados, esto tiene un efecto negativo para los vocales y miembros del Colegio corruptos, ya que frente a la discrepancia de resultados que habrá entre los dos organismos, el TRICEL deberá revisar las actas y es posible que incluso encuentre necesario recontar los votos. En este caso el resultado final, en vez de ser alterado aún más, será el resultado correcto que indican los votos y no los notificados en las actas.

Por otra parte, si los vocales ya modificaron el valor en las actas, también está el caso en que el Colegio Escrutador opte por no hacer trabajo adicional en cambiar resultados, ya que éstos ya fueron modificados. Este caso es equivalente al mencionado anteriormente en que sólo se tienen vocales de mesa corruptos.

8.3.3. Colusión de Colegio Escrutador con digitador

Debido a que el proceso que siguen los colegios escrutadores para revisar los resultados dice que todos los miembros deben revisar en conjunto cada mesa, para que un cambio hecho por un digitador no sea reportado, todos los miembros del Colegio Escrutador deben estar de acuerdo en que no hay problemas. Esto requiere que los diez miembros de éste y el Delegado de la Junta Electoral estén comprometidos, lo que es lo suficientemente improbable como para no considerarlo en los casos de estudios, ya que la elección de éstos también es aleatoria. Por lo tanto, este tipo de ataque se considera infactible.

8.4. Escrutinio General

8.4.1. Hackeo general a sistemas computacionales

Como los colegios escrutadores no proclaman ganadores, sino que sólo revisan mesas para ver que cuadren, la discrepancia entre lo que le muestre el sistema computacional (resultados reales de la votación) y lo que el público sabe (resultados alterados) no se notará, por lo tanto el TRICEL es la última instancia donde este hackeo puede ser detectado.

Frente a una mesa que no presente problemas según el Colegio Escrutador, el TRICEL debe de todas formas comprobar la concordancia entre la cuadratura del Colegio (visualizada en el sistema computacional) y el acta que obtuvo del día de las elecciones. Por esto, si el sistema intervenido muestra los resultados alterados, el hackeo sería evidente, por lo que en última instancia el TRICEL lo detectaría.

Por otra parte, si el sistema muestra los resultados correctos, el TRICEL no encontraría problemas entre los resultados, procediendo a la proclamación oficial de candidatos ganadores, la cual no se hace de manera automática por el sistema computacional. En esta proclamación se notarían las discrepancias entre los resultados anteriores y los nuevos, por lo tanto también se detectaría el hackeo.

Ambos casos descritos generarían una gran controversia y harían mucho menos confiable el sistema de elecciones. Además de mejorar la seguridad de los sistemas computacionales que en este caso ficticio fueron intervenidos, otra forma de detectar este tipo de ataque masivo antes de que el TRICEL lo note es hacer que el Colegio Escrutador, además de comprobar que el sistema computacional y su ejemplar de acta coincidan, que comprueben que éstos coincidan con lo que está publicado en la página del Servicio Electoral para el público general.

Ataque	**Medida**
Miembros de Juntas Electorales intentan alterar sorteo	• Aleatoriedad Verificable • Rotación de miembros de Junta Electoral
Tercero intenta alterar sorteo de vocales	• Efecto mínimo, no requiere medidas
Hackeo al sistema de selección de vocales	• Aleatoriedad verificable y revisión de publicación correcta de listas • Sistemas computacionales robustos
Vocales de mesa modifican resultados	• Auditoría estadística • Capacitación de vocales para reportar conductas sospechosas • Presencia de público general y apoderados de mesa en conteo
Digitador modifica resultados	• Detectable a través del trabajo del Colegio Escrutador • Generación de reporte impreso verificado por personal del local de votación
Sistema computacional es hackeado el día de las elecciones	• Detectable a través del trabajo del Colegio Escrutador • Generación de reporte impreso verificado por personal del local de votación • Computadores actualizados, red restringida y generación aleatoria de contraseñas
Colegio Escrutador cambia resultados	• Detectado por TRICEL
Colusión de Colegio Escrutador con digitador	• Poco probable ya que requiere la colusión del 100 % del Colegio Escrutador
Colusión de Colegio Escrutador con vocales de mesa	• Detectado por TRICEL • Auditoría Estadística
TRICEL intenta alterar resultados	• Poco probable debido a que el proceso realizado es concurrido por candidatos
Hackeo general al sistema computacional	• Detectado por TRICEL • Hacer que el Colegio Escrutador revise los resultados publicados • Sistemas computacionales robustos

Tabla 8.1: Cuadro resumen de los distintos ataques analizados y las respectivas medidas de mitigación.

Capítulo 9

Mitigaciones a Ataques

A continuación se profundizan algunas de las medidas propuestas para disminuir el efecto de los ataques al proceso de elecciones chileno.

9.1. Aleatoriedad Verificable

Una de las tecnologías mencionadas para mejorar el proceso de elecciones, en particular para mejorar la seguridad y transparencia de varios procesos durante la votación, corresponde a la aleatoriedad verificable. En particular nos referimos al Faro de Aleatoriedad de Random UChile [31].

9.1.1. Acerca del Faro

La función del Faro es entregar pulsos de bits aleatorios de manera periódica (en particular, cada minuto), generados mediante varias fuentes de aleatoriedad, y que son conservados a lo largo del tiempo, de manera que si un proceso público requiere aleatoriedad dentro de éste, una persona externa puede comprobar que la parte aleatoria no fue alterada.

Estos pulsos de bits aleatorios pueden ser usados directamente para procesos aleatorios, o pueden ser usados como semilla para un generador de números pseudo-aleatorios.

Un generador de números pseudo-aleatorio [13] es un algoritmo que toma como entrada un valor aleatorio (al azar o uniforme), llamado semilla, y produce una secuencia de números indistinguible a una secuencia de números aleatorios, pero el resultado no es realmente aleatorio ya que depende completamente de la semilla utilizada (resultado determinista). Existen varios de estos algoritmos (basados en herramientas criptográficas) considerados seguros, esto es, que producen una distribución indistinguible de una aleatoria.

Generación del pulso

Los pasos que sigue el Faro en cada minuto son los siguientes:

- Primero se obtienen valores de distintas fuentes que contienen un carácter aleatorio y

que cumplen ciertas condiciones [33]. Las fuentes que actualmente se usan en el Faro son el Centro Sismológico Nacional [8], la Radio de la Universidad de Chile [30], Tweets y la Blockchain de Ethereum [36].

- Paralelamente, se obtiene un valor aleatorio de manera interna usando un *TRNG (True Random Number Generator)*, hardware que genera bits aleatorios usando procesos cuánticos.
- Finalmente se juntan los valores de aleatoriedad externos e internos y se concatenan con la firma de Random UChile (obtenida mediante un algoritmo de firma digital). Esta concatenación se pasa por una función de $hash$[1] lento [16] antes de ser publicada, para asegurar que el valor final tome una cierta cantidad de tiempo en ser obtenido.

Los valores aleatorios generados por el Faro son firmados digitalmente y almacenados en forma permanente, estando disponibles públicamente para verificación.

Usos del Faro

Distintos organismos públicos en Chile tienen aleatoriedad en sus procesos, principalmente para la selección de personas. Sin embargo, a los organismos les es difícil demostrar que la selección realizada fue realmente aleatoria, propiciando con ello acusaciones de que ciertas personas fueron beneficiadas o perjudicadas en el proceso. Esto ha llevado a casos como selecciones hechas con tómbolas en sesiones abiertas al público.

El Faro de Aleatoriedad es ideal para estos procesos, ya que la responsabilidad de la correcta realización del sorteo pasa a manos de Random UChile. Más aún, el diseño matemático del Faro permite argumentar que gracias a los algoritmos utilizados para la generación de valores aleatorios, nadie puede haberlos influenciado, ni siquiera los mismos participantes de Random UChile.

Actualmente organizaciones ya han trabajado con Random UChile para incorporar aleatoriedad verificable en sus procesos, como lo son la Contraloría General de la República [7, 32], que usa el Faro para la selección verificable de funcionarios públicos para auditorías; y La Liga de la Entropía [6], colaboración de distintos servicios de aleatoriedad pública para crear un Faro de Aleatoriedad distribuido.

Además de lo descrito anteriormente, la aleatoriedad verificable puede usarse en procesos comunes, como reordenar una lista, elegir números para la lotería, etc.

9.1.2. Uso de Faro para Selección de Vocales

La elección de vocales de mesa se realiza de manera local por cada junta electoral, y su correcto funcionamiento depende de las personas involucradas en el proceso. El proceso sólo puede ser auditado (examinado) por terceros que asisten presencialmente el día del sorteo, siendo ellos los únicos agentes que posiblemente puedan encontrar posibles irregularidades. Es por esto que proponemos el uso del Faro de Aleatoriedad de Random UChile para selección de los vocales de mesa, para poder tener una mayor seguridad de que la selección de vocales

[1]Función que transforma una cadena de largo variable en un elemento de un conjunto de tamaño finito, generalmente entre 0 y 2^N, con N algún número natural.

no puede ser intervenida por agentes maliciosos, al facilitar a la población un mecanismo para comprobar que el proceso fue realizado correctamente.

El proceso sería el siguiente:

- Al igual que como se realiza actualmente, los miembros de la junta electoral seleccionan sus candidatos para vocales de mesa.
- Las listas creadas por cada miembro de la junta electoral se juntan y son subidas al sistema computacional que controla el Servel.
- En vez de realizar el sorteo presencialmente mediante una tómbola, el sistema usa el pulso generado por el Faro en una hora predeterminada, y éste es usado como semilla para un algoritmo de aleatoriedad para sortear los cinco números de vocales de mesa y los cinco de suplentes. La posibilidad de realizar el sorteo de esta forma sólo aparecerá disponible para las juntas electorales que aprobaron su uso con anterioridad.
- Los resultados de los números sorteados son publicados en la página del Servicio Electoral donde se informa quiénes son vocales de mesa, junto con la hora del pulso usada para que cualquier persona pueda comprobar la correcta realización del sorteo. Las personas que fueron parte de la lista de vocales de mesa también serán notificados del número que ocuparon en la lista.

Es importante notar que al permitir que las juntas electorales sigan eligiendo los candidatos, no se disminuye la participación de esta entidad dentro del proceso de selección, puesto que su criterio es importante para elegir a los más aptos para el cargo de vocal de mesa.

Para que este proceso no sea alterable por parte de un miembro de junta maliciosa, el sorteo no se puede rehacer indiscriminadamente, de lo contrario se podrían sortear números hasta que salgan los deseados. Por lo anterior, se impone una restricción de intentos para poder rehacer un sorteo.

De la misma forma, las listas de potenciales vocales de mesa debiesen ser publicadas con cierta anterioridad, de lo contrario no se podría probar que los candidatos asignados a los números del sorteo son los mismos que fueron publicados.

Además de potencialmente disminuir la probabilidad de alteraciones a los sorteos, la inclusión de aleatoriedad verificable y la publicación de listas permite que la población, que actualmente en su mayoría no tiene conocimiento del proceso de selección de vocales de mesa, esté más presente deurante los procesos electorales, aumentando la transparencia del proceso.

Un prototipo de este sistema de elección de vocales de mesa fue diseñado por Franco Pino [21] como trabajo de memoria asociado a este proyecto. Una junta electoral manifestó su interés por el sistema, por lo que pudiera ser implementado en una elección en el futuro.

9.1.3. Ataques al Faro de Aleatoriedad

Si bien el uso del Faro de Aleatoriedad potencialmente otorga soluciones a los problemas mencionados, también es posible que éste se vea afectado por distintos ataques. Los dos ataques principales que se pueden considerar son los siguientes:

- Un agente malicioso intenta afectar el resultado: Es posible que un atacante (ya sea interno o externo) intente alterar el resultado del valor de aleatoriedad generado por el Faro. Esto podría realizarse modificando los valores de las fuentes de aleatoriedad, pero muchas de éstas son externas y no dependen de los dueños del Faro, y basta que sólo una de las fuentes sea aleatoria para que el resultado sea aleatorio. La otra forma de modificar el valor sería modificando directamente el valor final. Afortunadamente, el valor final puede ser comprobado con los valores individuales de aleatoriedad, y no puede ser modificado más adelante debido a que los valores futuros almacenan un *hash* para evitar modificaciones a los valores anteriores.
- Ataques de denegación de servicio (DDoS): Es posible que un atacante intente utilizar toda la capacidad del Faro mediante un ataque de denegación de servicio, pero las funcionalidades del Faro no son únicas del Faro de la Universidad de Chile, sino que existen diversos Faros en el mundo con funcionalidades similares. Por lo tanto, en caso de que un atacante incluso lograse que el Faro de la Universidad de Chile esté no disponible al momento de realizar el sorteo, el sistema propuesto puede detectar esto y usar uno de los otros Faros existentes.

9.1.4. Efecto del Faro en ataques a selección de vocales

Con un sistema aleatorio verificable, aunque es posible que los miembros de una junta electoral seleccionen candidatos a vocales de mesa maliciosos, no es posible que éstos sean elegidos manualmente por la junta mediante alteraciones al sorteo, debido a que el resultado del sorteo no depende de la junta, sino que de lo que seleccione el sorteo del Faro en ese momento. Para que esto funcione correctamente, las listas de potenciales vocales deben ser publicadas antes del sorteo, de lo contrario se podría editar la lista de candidatos con posterioridad a la selección, para dejar a los candidatos maliciosos en las posiciones elegidas. Cabe destacar que la publicación de listas sin aleatoriedad verificable no es suficiente para evitar ataques, debido a que el sorteo de los números podría verse afectado de todas formas.

9.1.5. Simulación usando Faro de Aleatoriedad

Se incorporó el uso del Faro de Aleatoriedad para la selección de vocales de mesa, y considerando lo explicado en secciones anteriores, se consideró este sorteo como uno en el que no es posible para los miembros de las juntas electorales alteren el sorteo, por lo tanto este es siempre aleatorio. Esto se codificó en la variable TIPO_SORTEO, que especifica si es un sorteo por tómbola, o usando el Faro.

Se realizaron los experimentos con los mismos valores de los parámetros de los experimentos anteriores, para poder comparar los resultados del sorteo con y sin uso del Faro de aleatoriedad.

A continuación se presentan los resultados relevantes, junto con sus análisis. Resultados de simulaciones no relevantes para el análisis se encuentran en el Anexo B.

Resultados generales

Tipo Sorteo	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	69.8	8612.2	0.90
Tómbola	69.7	9143.2	1.03

Tabla 9.1: Resultados para los distintos tipos de sorteo simulados.

Análisis

Se puede ver que en promedio, el uso del Faro disminuye la cantidad total de vocales de mesa comprometidos que pueden llevar a alterar resultados. En particular logró disminuir el total de vocales comprometidos en un poco más de un 9 %, disminuyendo así el total de candidatos cambiados en casi un 14 %. Esto muestra que el Faro es efectivo en disminuir el riesgo al momento de elegir vocales de mesa.

Probabilidad de éxito de miembro de la junta

Resultados

Tipo Sorteo	Prob. Éxito Miembro Junta	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	30 %	69.4	8597.3	0.93
Faro	20 %	70.1	8647.3	0.86
Faro	10 %	69.8	8591.9	0.90
Tómbola	30 %	70.0	9363.4	1.14
Tómbola	20 %	69.3	9126.1	1.02
Tómbola	10 %	69.7	8940.2	0.92

Tabla 9.2: Resultados para los distintos tipos de sorteo simulados, agrupados por valores de probabilidad de éxito por parte de un miembro de la junta electoral para alterar el sorteo (asociado a parámetro PROB_FALLA).

Análisis

Se ve que el uso del Faro efectivamente disminuye la cantidad de vocales comprometidos y candidatos cambiados, manteniendo el número relativamente constante a medida que se varía el parámetro estudiadio. Esto último ocurre ya que la verificabilidad de los procesos realizados a través del Faro de Aleatoriedad permite que una alteración de resultados no

sea posible de las maneras estudiadas en este trabajo. Esto muestra que el uso del Faro de Aleatoriedad efectivamente reduce el riesgo de que una elección sea intervenida.

Sorteo individual por mesa

Con el objetivo de estudiar si era posible disminuir aún más la cantidad de candidatos cambiados en el caso de usar el Faro, se estudió su efecto en conjunto con el sorteo individual por mesa, ya que se tendría una distribución más uniforme en los números sorteados por cada mesa.

Resultados

Tipo Sorteo	**Miembros de juntas comprometidos**	**Vocales comprometidos**	**Candidatos electos cambiados**
Por mesa	69.1	8510.1	0.93
Por junta	69.8	8612.2	0.90

Tabla 9.3: Resultados en caso de sorteo de mesa y por junta, cuando se usa el Faro de aleatoriedad.

Análisis

Comparando ambos tipos de sorteo, vemos que hay una pequeña diferencia en la cantidad de candidatos cambiados, siendo 0.93 en promedio para el sorteo por mesa, y 0.90 para el sorteo general, mostrando que mantener el sorteo por junta electoral es una mejor opción que un sorteo por mesa de votación, especialmente considerando que el sorteo por mesa tuvo una mayor cantidad de candidatos cambiados, incluso con menos miembros de junta comprometidos y vocales comprometidos.

9.2. Auditoría Estadística

Podemos ver que gran parte de los ataques se basan en el hecho de que una vez que se cuentan los votos, los sistemas de corroboración de datos usados se basan casi exclusivamente en las actas del día de votación, siendo el reconteo de votos una medida usada sólo en última instancia.

Como resultado de esto, y tomando el análisis anterior como punto de partida, un ataque que modifica las actas de manera consistente permanecerá sin detectarse. Claramente una forma de poder evitar eso sería recontar todos los votos después de las elecciones, pero esto sería altamente costoso debido a la cantidad de recursos humanos y temporales requeridos para hacer este conteo, ya que esta labor quedaría en manos de los Colegios Escrutadores, los cuales abarcan mucho más de una mesa, o de un nuevo organismo encargado de hacer el conteo, requiriendo aún más personal en el proceso.

Una forma más eficiente de comprobar que un conteo ha sido correcto consiste en utilizar una auditoría estadística [17], que corresponde a un proceso mediante el cual se revisan ciertos votos elegidos aleatoriamente entre distintas mesas de votación, y con este pequeño porcentaje de votos recontados, se obtiene con una alta certeza que un conteo se realizó correctamente.

Dos tipos importantes de auditorías estadísticas son:

- Conteo a nivel de voto: corresponde a recontar una cantidad reducida de votos elegidos aleatoriamente para evaluar la representatividad de éstos. Se elige un margen de error, y se recuentan votos hasta que se llega a un resultado que asegure que el conteo general se hizo correctamente (dentro del margen de error elegido). Si el resultado está incorrecto, entonces, con una probabilidad de 100 % menos el margen de error, se seguirán contando votos hasta contarlos todos, llegando al resultado correcto.
- Conteo de comparación: Evalúa los resultados arrojados por sistemas automáticos, como lo son las máquinas de votación electrónica y sistemas ópticos [14]. Para esto se revisa que los subtotales contados por las máquinas correspondan a los reales, proceso realizado mediante sumas manuales, y luego se comparan votos aleatorios de la máquina y revisando su interpretación. Si la interpretación de la máquina es distinta a la interpretación de la persona que audita, este resultado se guarda y contribuye a considerar el conteo original como no válido.

El conteo a nivel de votos es el mejor para las votaciones de Chile, ya que puede realizarse sin necesidad de la existencia de un sistema de voto electrónico. Además, este proceso calza perfectamente con lo que necesitamos, un proceso que permita comprobar que los resultados sean correctos sin tener que recontar todos los votos.

Una consideración a realizar es que el sistema de elección de candidatos en el país, para el caso de diputados y senadores, es el sistema D'Hondt descrito anteriormente, se requiere de un tipo de conteo estadístico diseñado para este método. Para esto, se propone utilizar el sistema descrito por Stark et al. [27], que describe en detalle cómo realizar auditorías estadísticas para elecciones con este sistema en particular.

También se propone que para el proceso de elección aleatoria de votos a recontar, se use el Faro de Aleatoriedad descrito anteriormente, para asegurar la transparencia del proceso, e incluso se podría publicar la descripción completa del proceso en línea, de forma que cualquier persona pueda recrear el reconteo en su casa usando los valores de aleatoriedad publicados en la página del Faro y las horas a las que se realizó la extracción de los pulsos.

Actualmente existe un prototipo en desarrollo por parte de Diego Vargas que implementa las sugerencias aquí descritas, entre otros mecanismos de auditoría estadística [35].

Conclusión

En este trabajo logramos modelar cada parte del proceso de votación en Chile, para así realizar un análisis detallado de la seguridad de las partes que lo componen.

En particular logramos identificar los distintos actores en el proceso de selección de vocales de mesa, dividiéndolo en la fase de creación de listas y la de sorteo, mostrando el importante rol que tienen las Juntas Electorales, y las distintas formas en que unos pocos miembros corruptos de éstas pueden generar un efecto en cadena, alterando el resultado de una elección, mediante la incorporación de más agentes corruptos al modelo creado.

Además, mostramos el flujo de la información durante el día de la votación, a través de las distintas etapas de constitución de mesas, desarrollo de votación, conteo y envío de información, en donde la información de los votos es traspasada a las actas de votación y enviada a distintas otras entidades, las cuales se encargan de publicar la información y corroborar su correctitud. También se identificaron actores no tan conocidos como lo son los digitadores y la empresa responsable de éstos.

Mediante un proceso de simulación de ataques al sistema de elecciones, se logró cuantificar el riesgo asociado a cada una de las etapas del proceso de votación descritas anteriormente, encontrando resultados como la sensibilidad que tienen los resultados respecto a la edición de votos por parte de los vocales, a la probabilidad de éxito de los vocales para alterar actas, y a los miembros de juntas electorales corruptas; además de proponer distintas soluciones para contrarrestar estos problemas, como lo son el fomentar que los procesos sean más públicos y la rotación de los cargos de las juntas electorales.

También se comprobó la utilidad de la incorporación de aleatoriedad verificable en la elección de vocales de mesa, reduciendo el riesgo de alteraciones a los resultados de elecciones, mejorando la transparencia de los procesos electorales al hacerlos más accesibles para la población.

Finalmente se propuso la implementación de auditorías estadísticas para las votaciones, procesos principalmente usados para votación electrónica, para así lograr encontrar posibles ataques que el proceso actual no logra detectar, debido a que el flujo de información depende ampliamente del supuesto de que las actas del día de votación fueron llenadas correctamente.

Conclusión sobre las elecciones

El análisis anteriormente señalado nos permite concluir que el proceso de elecciones en Chile es resiliente, significativamente resistente a una amplia variedad de ataques, aunque susceptible a otros, pero en general, seguro. Esto es una interesante consecuencia para un sistema que funciona principalmente por medio de papel.

El sistema es vulnerable a un ataque donde un digitador modifica los resultados, sin embargo, tal ataque es detectable con las medidas actuales, pero igual podría generar problemas de desconfianza en las instituciones públicas. Es por esto que, aunque en la actualidad se tengan medidas para evitar que estos ataques prosperen, de todas maneras existen mejoras para evitar el éxito de éstos en una etapa más temprana, como por ejemplo, una fase de comparación de resultados de acta con resultados enviados por parte de personal del local de votación.

El riesgo que conllevan algunos de los ataques se puede disminuir mediante la incorporación de medidas propuestas en los capítulos anteriores, siendo las principales la auditoría estadística (ara encontrar errores en el conteo con una alta probabilidad) y el sorteo aleatorio verificable (para hacer el proceso más transparente y también evitar alteraciones a la selección de vocales y miembros del Colegio Escrutador).

Como conclusión se sugiere que, antes de empezar una transición a un sistema de votación electrónica para las elecciones nacionales en Chile, se implementen las medidas propuestas, particularmente, la auditoría estadística. Nuestro trabajo demuestra que ellas no sólo robustecen el sistema actual sino que, pueden seguir usándose aun en caso de una eventual migración a un sistema de votación electrónica presencial en el país.

Trabajo futuro

Ataques al padrón electoral

Existen ataques que involucran la alteración de parte del padrón electoral, es decir, de la lista los votantes habilitados con sus respectivos locales de votación, mesa de votación, y otra información relevante como domicilio y profesión. Sin embargo, ellos no fueron incluidos en este trabajo debido a que requería una mayor investigación acerca de los procesos asociados con otra entidad, como lo es el Registro Civil.

Por ejemplo, cuando los miembros de la junta electoral deben elegir sus candidatos a vocales, deben hacerlo de forma que escojan a los que consideren más aptos para el cargo. Conversando con una junta electoral, nos enteramos que una de las únicas formas que tienen de determinar esto es mediante la edad y la profesión. La profesión está en su mayoría sin documentar en el padrón, ya que no es requerida por el Registro Civil al momento de obtener una cédula de identidad, por lo tanto un tercero podría modificar el padrón para informar profesiones erróneas de sus potenciales vocales comprometidos mediante un hackeo a los sistemas del Registro Civil, de forma que estas personas sean fácilmente elegidas por los miembros de la junta, por ejemplo, señalando que son abogados o contadores.

Otro posible caso de ataque sería alterar el padrón del Registro Civil de forma de mover

ciertos porcentajes de los votantes de sus locales de votación originales a otros nuevos, y esperar que no revisen su información en línea para enterarse del cambio, efectivamente quitándoles su oportunidad para (y derecho a) votar.

Estos ataques requieren saber cuál es el proceso para informar profesiones o tener conocimiento acerca de los sistemas computacionales usados por el Registro Civil. Por ello, se propone como trabajo futuro investigar sobre estos procesos para realizar un análisis del efecto que podrían tener estos ataques.

Efectos de la compra de votos

Este trabajo analizó como actores maliciosos dentro del proceso de la elección podían alterar los resultados, pero también es posible hacer un análisis de ataques que afecten directamente a la entrada del sistema: los votantes y sus votos.

Es posible que mediante distintos métodos, ya sean sobornos o amenazas, un tercero logre hacer que el votante marque una preferencia que no refleje sus verdaderas intenciones, es decir, que un mensaje se envíe desde un principio con el contenido equivocado.

Como los votos no están asociados a los votantes y no es posible saber oficialmente qué marcó el votante en la cédula, el actor externo debe asegurarse de que el votante marcó la preferencia indicada. Hoy en día esto podría ser posible gracias a las cámaras de los celulares.

Entonces, como trabajo futuro se propone ver la factibilidad de este tipo de ataques, analizando si las medidas actuales pueden prevenirlos y proponiendo mejoras para los casos en que el sistema actual no detecta los ataques.

Ballot stuffing

Un caso no analizado por este trabajo es la posibilidad de que los vocales de mesa realicen *ballot stuffing*, es decir, agreguen votos adicionales a las urnas con su preferencia. Como además éstos tienen acceso a los libros de firmas, pueden firmar por las personas que aún no han votado.

Para evitar la posibilidad de que una persona llegue a votar y encuentre que su voto ya está marcado, el proceso de *ballot stuffing* se puede llevar a cabo cuando quede poco tiempo para cerrar las mesas. Además, como los vocales tienen acceso a la lista de gente que aún no vota, pueden elegir rellenar con los datos de personas que sea poco probable de que lleguen a votar, por ejemplo, si gente de la tercera edad tiende a ir a votar en la mañana, es menos riesgoso rellenar con votos de tercera edad en la tarde ya que probablemente esta gente ya no vaya al local de votación.

Se propone entonces estudiar más a fondo si estos ataques son viables para alterar los resultados de las elecciones.

Modelo formal de las elecciones

Para demostrar formalmente las propiedades de las elecciones en Chile mostradas en este trabajo, se propone como trabajo futuro modelar todo el proceso con un lenguaje de demostración de teoremas como Coq[2], para enunciar los supuestos en los que se basan las elecciones, y llegar a las propiedades esperadas mediante razonamiento matemático.

Otros tipos de ataques

Ciertos tipos de ataques en el día de votación no fueron capturados por las simulaciones realizadas. Entre ellos, el ataque donde un vocal de mesa intente anular un voto válido, agregándole una marca adicional por otro candidato, o que intente marcar un voto blanco con alguna preferencia. Una posible continuación a este trabajo sería incorporar este tipo de ataques a la simulación y evaluar sus efectos en los resultados.

Votación electrónica en Chile

Es posible que al incluir ciertas formas de votación electrónica (particularmente las de tipo presencial) se pueda disminuir el riesgo durante el día de votaciones, ya sea disminuyendo los momentos donde pueda existir error humano o generando una replicación de la información que sea verificada más adelante. Por lo tanto como trabajo futuro se propone evaluar el reemplazo de la votación en Chile por un sistema con componente electrónica y discutir sus efectos.

[2]https://coq.inria.fr/

Bibliografía

[1] *Ley 18.460, Ley Orgánica Constitucional del Tribunal Calificador de Elecciones*. Diario Oficial de la República de Chile, 1985.

[2] *Ley 18.700, Ley Orgánica Constitucional Sobre Votaciones Populares y Escrutinios*. Diario Oficial de la República de Chile, 1988.

[3] Tele 13, Nov 2012. URL: `https://static.t13.cl/images/sizes/1090x613/mgr_630_foto_pizarra_voto.jpg`.

[4] Edward G Amoroso. *Fundamentals of computer security technology*. PTR Prentice Hall New Jersy, 1994.

[5] Tomer Ashur, Orr Dunkelman, and Nimrod Talmon. Breaching the Privacy of Israel's Paper Ballot Voting System. In *International Joint Conference on Electronic Voting*, pages 108–124. Springer, 2016.

[6] Cloudflare. Distributed Randomness Beacon. URL: `https://www.cloudflare.com/leagueofentropy/`.

[7] Constanza Andrea Csori Pinto. Achieving transparency in public decision making processes via verifiable randomness. 2019.

[8] Universidad de Chile. Centro Sismológico Nacional. URL: `http://www.sismologia.cl/`.

[9] Conservadores Digitales. Juntas electorales: Sorteo de vocales de mesa, Jun 2017. URL: `http://fojas.conservadores.cl/noticias/juntas-electorales-sorteo-vocales-mesa`.

[10] Servicio Electoral. Video tutorial PESE, Oct 2013. URL: `https://www.youtube.com/watch?v=oFVnalmI6DM`.

[11] Servicio Electoral. Cartilla de Instrucciones para Mesa Receptora de Sufragios, 2017.

[12] Ariel J Feldman, J Alex Halderman, and Edward W Felten. Security analysis of the Diebold AccuVote-TS voting machine. 2006.

[13] F. James. A review of pseudorandom number generators. *Computer Physics Commu-*

nications, 60(3):329–344, 1990.

[14] Douglas W. Jones. On optical mark-sense scanning, Jan 1970. URL: https://link.springer.com/chapter/10.1007/978-3-642-12980-3_10.

[15] Tadayoshi Kohno, Adam Stubblefield, Aviel D Rubin, and Dan S Wallach. Analysis of an electronic voting system. In *Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on*, pages 27–40. IEEE, 2004.

[16] Arjen K. Lenstra and Benjamin Wesolowski. A random zoo: sloth, unicorn, and trx. Cryptology ePrint Archive, Report 2015/366, 2015. https://eprint.iacr.org/2015/366.

[17] Mark Lindeman and Philip B. Stark. A Gentle Introduction to Risk-Limiting Audits. *IEEE Security & Privacy*, 10(5):42–49, 2012. doi:10.1109/msp.2012.56.

[18] Stephan Neumann, Jurlind Budurushi, and Melanie Volkamer. Analysis of Security and Cryptographic Approaches to Provide Secret and Verifiable Electronic Voting. *Design, Development, and Use of Secure Electronic Voting Systems. Ed. by Dimitrios Zissis and Dimitrios Lekkas. IGI Global*, page 27, 2014.

[19] Martin Odersky, Philippe Altherr, Vincent Cremet, Burak Emir, Sebastian Maneth, Stéphane Micheloud, Nikolay Mihaylov, Michel Schinz, Erik Stenman, and Matthias Zenger. An overview of the Scala programming language. Technical report, 2004.

[20] Harold Pardue, Jeffrey Landry, and Alec Yasinsac. A risk assessment model for voting systems using threat trees and Monte Carlo simulation. In *Requirements Engineering for e-Voting Systems (RE-VOTE), 2009 First International Workshop on*, pages 55–60. IEEE, 2010.

[21] Franco Aníbal Pino Córdova. Elección de vocales de mesa con aleatoriedad verificable. 2019.

[22] Eric Rescorla. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, August 2018. URL: https://rfc-editor.org/rfc/rfc8446.txt, doi:10.17487/RFC8446.

[23] SERVEL. Resultados en Excel por Mesa (a partir del año 2012). URL: https://www.servel.cl/resultados-en-excel-por-mesa-a-partir-del-ano-2012/.

[24] SERVEL. Juntas Electorales. URL: https://www.servel.cl/juntas-electorales/.

[25] SERVEL. Servicio Electoral. URL: https://www.servel.cl/servicio-electoral-de-chile/.

[26] Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J Alex Halderman. Security analysis of the Estonian internet voting system. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 703–715. ACM, 2014.

[27] Philip B Stark, Vanessa Teague, and Aleksander Essex. Verifiable european elections: Risk-limiting audits for D'Hondt and its relatives. {*USENIX*} *Journal of Election Technology and Systems ({JETS})*, 1:18–39, 2014.

[28] Andrew S Tanenbaum and Maarten Van Steen. *Distributed systems: principles and paradigms*. Prentice-Hall, 2007.

[29] TVN, Oct 2012. URL: `https://www.24horas.cl/incoming/article368630.ece/ALTERNATES/w620h450/Recuento%20de%20votos%20Colegio%20Lastarria18.jpg`.

[30] Radio UChile. Diario y Radio U Chile. URL: `https://radio.uchile.cl/`.

[31] Random UChile. Acerca de. URL: `https://random.uchile.cl/about/`.

[32] Random UChile. Contraloría General de la República. URL: `https://random.uchile.cl/projects/contraloria/`.

[33] Random UChile. ¿Cómo Funciona? URL: `https://random.uchile.cl/randomness-beacon/`.

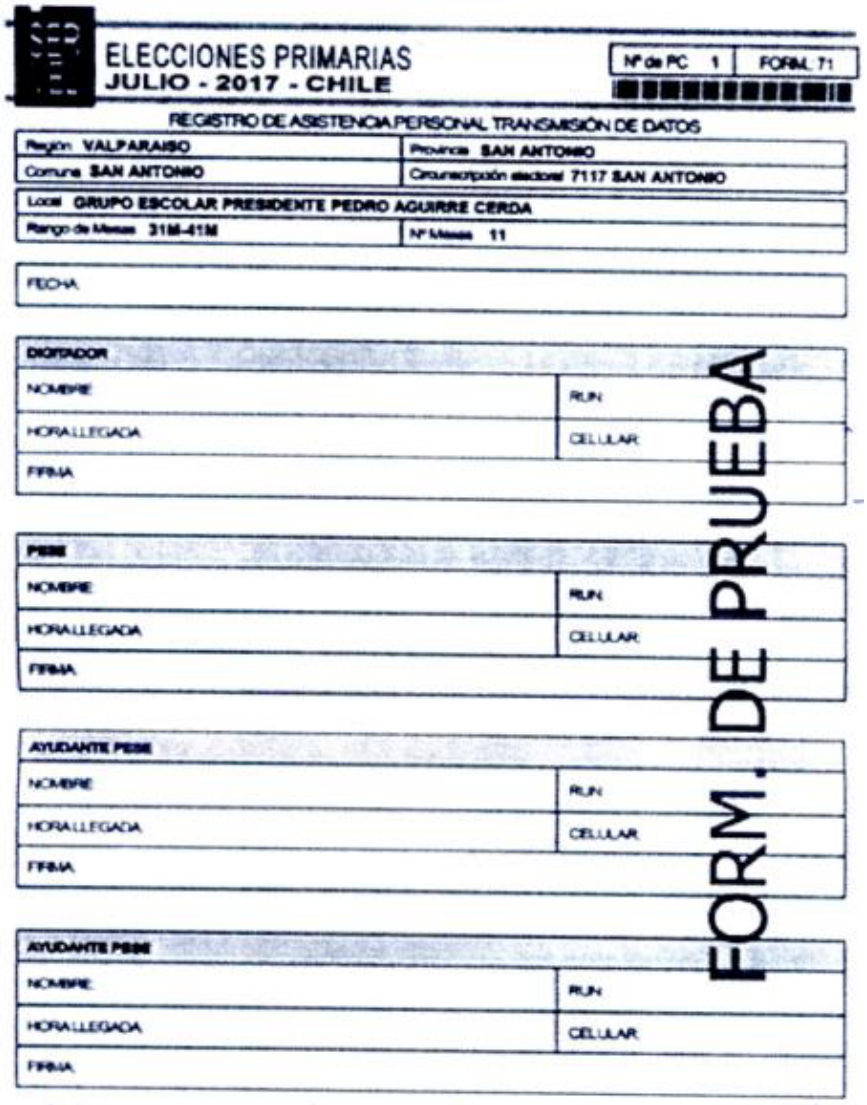
[34] André van Cleeff, Trajce Dimkov, Wolter Pieters, and Roel Wieringa. Realizing security requirements with physical properties: A case study on paper voting. In *Proceedings of the International Conference on IT Convergence and Security 2011*, pages 51–67. Springer, 2012.

[35] Diego Vargas. Confirmación de resultados para elecciones chilenas usando aleatoriedad verificable. Memoria en preparación, Universidad de Chile, 2020.

[36] Gavin Wood et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–32, 2014.

Anexo A

Actas del Día de Votación



ELECCIONES PRIMARIAS
JULIO - 2017 - CHILE

Nº de PC 1 | FORM. 71

REGISTRO DE ASISTENCIA PERSONAL TRANSMISIÓN DE DATOS

Región: VALPARAISO	Provincia: SAN ANTONIO
Comuna: SAN ANTONIO	Circunscripción electoral: 7117 SAN ANTONIO
Local: GRUPO ESCOLAR PRESIDENTE PEDRO AGUIRRE CERDA	
Rango de Mesas: 31M-41M	Nº Mesas: 11

FECHA:

DIGITADOR	
NOMBRE:	RUN:
HORA LLEGADA:	CELULAR:
FIRMA:	

PEBE	
NOMBRE:	RUN:
HORA LLEGADA:	CELULAR:
FIRMA:	

AYUDANTE PEBE	
NOMBRE:	RUN:
HORA LLEGADA:	CELULAR:
FIRMA:	

AYUDANTE PEBE	
NOMBRE:	RUN:
HORA LLEGADA:	CELULAR:
FIRMA:	

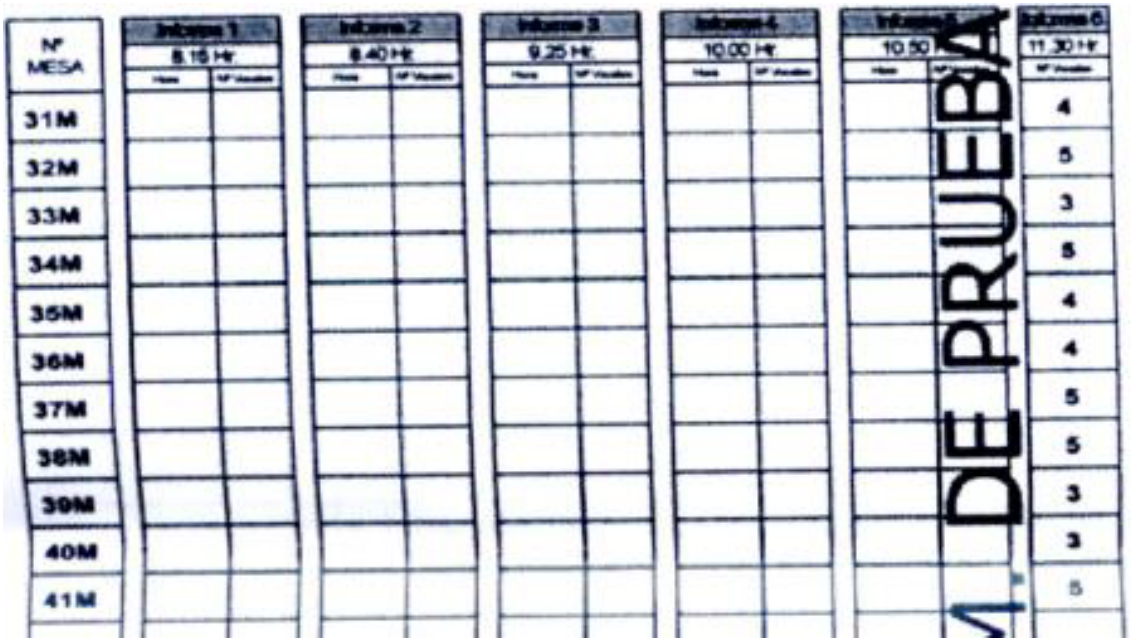
FORM. DE PRUEBA

Acta con datos del personal del local de votación.

- Anotar e ingresar sólo Mesas constituidas.
- Cotejar las Mesas constituidas que se ingresen en esta planilla con los resultados que obtenga el Delegado de la Junta Elector antes de su transmisión.

MESA	CONSTITUIDA (S/N)	HORA	Nº VOCALES
43V			4
44V			4
45V			5
46V			3
47V			3
48V			5
49V			4
50V			3
51V			5
52V			4
53V			3
54V			5
55V			3
56V			3
57V			4
58V			3
59V			3
60V			3
61V			3
62V			3

Acta de estado de las mesas de votación.



Acta con resumen de la constitución de mesas.

Anexo B

Resultados Adicionales de Simulaciones

Las tablas siguientes corresponden a los resultados completos de las simulaciones descritas a lo largo de este trabajo, cuyos valores no fueron tan relevantes para el análisis realizado como las discutidas en la parte central de este trabajo. Se incluye también el resultado de la simulación en caso de que se haya usado el Faro de Aleatoriedad en vez de el sorteo tradicional por tómbola incluso en casos especiales como el sorteo por mesa o por mayoría simple.

Tipo Sorteo	**Prob. Compuesta**	**Miembros de juntas comprometidos**	**Vocales comprometidos**	**Candidatos electos cambiados**
Faro	No	70.0	8652.1	0.87
Faro	Sí	69.5	8572.2	0.93
Tómbola	No	70.0	9210.9	1.01
Tómbola	Sí	69.3	9075.6	1.05

Resultados para los distintos tipos de sorteo simulados, agrupados por inclusión de probabilidad compuesta (PROBABILIDAD_COMPUESTA).

Tipo Sorteo	**Límite Vocales**	**Miembros de juntas comprometidos**	**Vocales comprometidos**	**Candidatos electos cambiados**
Faro	3	69.5	8572.0	1.01
Faro	5	70.0	8652.3	0.78
Tómbola	3	69.5	9117.1	1.13
Tómbola	5	69.9	9169.4	0.92

Resultados para los distintos tipos de sorteo simulados, agrupados por valores de límite de vocales (asociado a parámetro TRESHOLD_VOCALES).

Tipo Sorteo	**Porcentaje Edición**	**Miembros de juntas comprometidos**	**Vocales comprometidos**	**Candidatos electos cambiados**
Faro	50 %	69.7	8573.5	0.42
Faro	70 %	69.9	8641.4	0.97
Faro	90 %	69.6	8621.6	1.31
Tómbola	50 %	69.6	9163.3	0.57
Tómbola	70 %	69.7	9101.5	1.03
Tómbola	90 %	69.7	9164.9	1.48

Resultados para los distintos tipos de sorteo simulados, agrupados por valores de porcentaje de edición de votos por los vocales de mesa (asociado a parámetro PORCENTAJE_EDICION).

Tipo Sorteo	Prob. Vocal Mesa	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	20 %	69.6	8594.6	2.00
Faro	10 %	69.9	8615.0	0.56
Faro	5 %	69.8	8626.9	0.13
Tómbola	20 %	69.5	9116.0	2.16
Tómbola	10 %	69.9	9179.0	0.75
Tómbola	5 %	69.7	9134.7	0.18

Resultados para los distintos tipos de sorteo simulados, agrupados por valores de probabilidad de éxito de un vocal en la edición de votos (asociado a parámetro PROB_VOCAL_MESA).

Tipo Sorteo	Prob. Junt. Comp.	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	10 %	35.0	4271.8	0.29
Faro	20 %	69.6	8651.8	0.83
Faro	30 %	104.7	12 912.9	1.57
Tómbola	10 %	35.0	4565.7	0.34
Tómbola	20 %	69.6	9137.3	0.94
Tómbola	30 %	104.4	13 726.7	1.81

Resultados para los distintos tipos de sorteo simulados, agrupados por valores de probabilidad de que un miembro de una junta electoral sea corrupto (asociado a parámetro PROB_JUNT_COMP).

Tipo Sorteo	**Prob. Encontrar Vocal**	**Miembros de juntas comprometidos**	**Vocales comprometidos**	**Candidatos electos cambiados**
Faro	40 %	69.6	6865.8	0.56
Faro	60 %	69.9	10 358.5	1.23
Tómbola	40 %	69.8	7398.9	0.70
Tómbola	60 %	69.5	10 887.6	1.36

Resultados para los distintos tipos de sorteo simulados, agrupados por valores de probabilidad de que un miembro comprometido de una junta encuentre un vocal comprometido para el sorteo (PROB_ENCONTRAR_VOCAL).

Tipo Sorteo	**Candidatos Miembro**	**Miembros de juntas comprometidos**	**Vocales comprometidos**	**Candidatos electos cambiados**
Faro	3	69.5	6443.1	0.46
Faro	5	70.0	10 781.2	1.33
Tómbola	3	69.4	6929.9	0.57
Tómbola	5	69.9	11 356.6	1.48

Resultados para los distintos tipos de sorteo simulados, agrupados por cantidad máxima de vocales de mesa comprometidos que puede tener un miembro de junta comprometido (asociado a parámetro CANDIDATOS_MIEMBRO).

Tipo Sorteo	Prob. Junt. Comp	Prob. Encontrar Vocal	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	10 %	40 %	35.1	3398.5	0.13
Faro	10 %	60 %	34.9	5145.1	0.45
Faro	20 %	40 %	69.3	6918.9	0.49
Faro	20 %	60 %	69.8	10 384.7	1.17
Faro	30 %	40 %	104.2	10 280.1	1.06
Faro	30 %	60 %	105.1	15 545.7	2.07
Tómbola	10 %	40 %	35.2	3657.8	0.21
Tómbola	10 %	60 %	34.9	5473.6	0.46
Tómbola	20 %	40 %	69.5	7354.3	0.63
Tómbola	20 %	60 %	69.8	10 920.2	1.24
Tómbola	30 %	40 %	104.9	11 184.4	1.25
Tómbola	30 %	60 %	103.9	16 268.9	2.38

Resultados para los distintos tipos de sorteo simulados, agrupados por valores de probabilidad de miembros de junta comprometida y probabilidad de encontrar vocales comprometidos para el sorteo (parámetros PROB_JUNT_COMP y PROB_ENCONTRAR_VOCAL).

Tipo Sorteo	Prob. Compuesta	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	No	69.3	8492.2	0.88
Faro	Sí	68.8	8528.0	0.98
Tómbola	No	69.6	25 975.9	4.13
Tómbola	Sí	69.4	22 604.6	3.40

Resultados en caso de sorteo de mesa, agrupados por inclusión de probabilidad compuesta.

Tipo Sorteo	Límite Vocales	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	3	68.7	8475.3	1.01
Faro	5	69.4	8544.9	0.84
Tómbola	3	69.6	24 291.2	4.16
Tómbola	5	69.4	24 289.3	3.37

Resultados en caso de sorteo de mesa, agrupados por valores de límite de vocales.

Tipo Sorteo	Porcentaje Edición	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	50 %	69.5	8598.0	0.50
Faro	70 %	68.6	8441.3	0.97
Faro	90 %	69.1	8491.1	1.31
Tómbola	50 %	69.2	24 042.5	2.81
Tómbola	70 %	69.7	24 387.7	3.94
Tómbola	90 %	69.6	24 440.6	4.53

Resultados en caso de sorteo de mesa, agrupados por valores de porcentaje de edición de votos por los vocales de mesa.

Tipo Sorteo	Prob. Vocal Mesa	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	20 %	69.0	8479.2	2.03
Faro	10 %	69.6	8624.0	0.62
Faro	5 %	68.5	8427.2	0.14
Tómbola	20 %	69.9	24 501.0	5.70
Tómbola	10 %	69.7	24 336.9	3.59
Tómbola	5 %	68.8	24 032.8	2.00

Resultados en caso de sorteo de mesa, agrupados por valores de probabilidad de éxito de un vocal en la edición de votos.

Tipo Sorteo	Prob. Éxito Miembro Junta	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	30 %	69.2	8536.9	0.93
Faro	20 %	69.1	8480.0	0.92
Faro	10 %	68.8	8513.5	0.94
Tómbola	30 %	69.0	29 559.1	4.60
Tómbola	20 %	69.7	24 939.2	3.92
Tómbola	10 %	69.7	18 372.5	2.76

Resultados en caso de sorteo de mesa, agrupados por valores de probabilidad de éxito por parte de un miembro de la junta electoral para alterar el sorteo.

Tipo Sorteo	Candidatos Miembro	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	3	68.8	6369.3	0.48
Faro	5	69.3	10 651.0	1.38
Tómbola	3	69.4	21 069.5	3.24
Tómbola	5	69.5	27 511.0	4.28

Resultados en caso de sorteo de mesa, agrupados por cantidad máxima de vocales de mesa comprometidos que puede tener un miembro de junta comprometido.

Tipo Sorteo	Prob. Junt. Comp.	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	10 %	34.3	4219.7	0.28
Faro	20 %	69.3	8531.3	0.84
Faro	30 %	103.6	12 779.4	1.66
Tómbola	10 %	34.3	11 674.4	1.70
Tómbola	20 %	69.8	24 186.4	3.83
Tómbola	30 %	104.4	37 009.9	5.76

Resultados en caso de sorteo de mesa, agrupados por valores de probabilidad de que un miembro de una junta electoral sea corrupto.

Tipo Sorteo	Prob. Encontrar Vocal	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	40 %	68.8	6786.6	0.56
Faro	60 %	69.3	10 233.6	1.30
Tómbola	40 %	69.7	21 768.4	3.39
Tómbola	60 %	69.2	26 812.1	4.14

Resultados en caso de sorteo de mesa, agrupados por valores de probabilidad de que un miembro comprometido de una junta encuentre un vocal comprometido para el sorteo.

Tipo Sorteo	**Prob. Junt. Comp**	**Prob. Encontrar Vocal**	**Miembros de juntas comprometidos**	**Vocales comprometidos**	**Candidatos electos cambiados**
Faro	10 %	40 %	34.2	3394.8	0.14
Faro	10 %	60 %	34.3	5044.6	0.42
Faro	20 %	40 %	69.1	6761.6	0.50
Faro	20 %	60 %	69.4	10 300.9	1.19
Faro	30 %	40 %	103.0	10 203.5	1.02
Faro	30 %	60 %	104.2	15 355.4	2.30
Tómbola	10 %	40 %	34.7	10 437.0	1.49
Tómbola	10 %	60 %	33.9	12 911.8	1.91
Tómbola	20 %	40 %	69.8	21 762.8	3.43
Tómbola	20 %	60 %	69.7	26 610.0	4.22
Tómbola	30 %	40 %	104.7	33 105.4	5.25
Tómbola	30 %	60 %	104.1	40 914.4	6.28

Resultados en caso de sorteo de mesa, agrupados por valores de probabilidad de miembros de junta comprometida y probabilidad de encontrar vocales comprometidos para el sorteo.

Tipo Sorteo	Prob. Compuesta	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	No	69.7	8621.7	1.24
Faro	Sí	69.6	8605.9	1.25
Tómbola	No	69.4	9233.3	1.43
Tómbola	Sí	69.5	9024.0	1.30

Resultados en caso de asignación al mayor del pacto, agrupados por inclusión de probabilidad compuesta.

Tipo Sorteo	Límite Vocales	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	3	69.6	8586.4	1.33
Faro	5	69.7	8641.1	1.16
Tómbola	3	69.4	9129.1	1.52
Tómbola	5	69.5	9128.2	1.22

Resultados en caso de asignación al mayor del pacto, agrupados por valores de límite de vocales.

Tipo Sorteo	**Porcentaje Edición**	**Miembros de juntas comprometidos**	**Vocales comprometidos**	**Candidatos electos cambiados**
Faro	50 %	70.0	8639.6	0.89
Faro	70 %	69.6	8649.5	1.31
Faro	90 %	69.2	8552.3	1.52
Tómbola	50 %	69.1	9090.2	0.94
Tómbola	70 %	69.5	9119.0	1.40
Tómbola	90 %	69.8	9176.8	1.76

Resultados en caso de asignación al mayor del pacto, agrupados por valores de porcentaje de edición de votos por los vocales de mesa.

Tipo Sorteo	**Prob. Vocal Mesa**	**Miembros de juntas comprometidos**	**Vocales comprometidos**	**Candidatos electos cambiados**
Faro	20 %	70.3	8751.1	2.44
Faro	10 %	69.0	8521.7	0.99
Faro	5 %	69.6	8568.5	0.30
Tómbola	20 %	69.8	9261.9	2.64
Tómbola	10 %	69.8	9057.6	1.10
Tómbola	5 %	69.5	9066.5	0.37

Resultados en caso de asignación al mayor del pacto, agrupados por valores de probabilidad de éxito de un vocal en la edición de votos.

Tipo Sorteo	Prob. Éxito Miembro Junta	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	30 %	69.5	8582.6	1.24
Faro	20 %	69.3	8615.5	1.23
Faro	10 %	70.1	8643.2	1.26
Tómbola	30 %	69.1	9302.4	1.47
Tómbola	20 %	69.5	9135.6	1.37
Tómbola	10 %	69.7	8948.0	1.28

Resultados en caso de asignación al mayor del pacto, agrupados por valores de probabilidad de éxito por parte de un miembro de la junta electoral para alterar el sorteo.

Tipo Sorteo	Candidatos Miembro	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	3	69.7	6468.6	0.77
Faro	5	69.6	10 759.0	1.72
Tómbola	3	69.5	6940.1	0.91
Tómbola	5	69.4	11 317.2	1.82

Resultados en caso de asignación al mayor del pacto, agrupados por cantidad máxima de vocales de mesa comprometidos que puede tener un miembro de junta comprometido.

Tipo Sorteo	**Prob. Junt. Comp.**	**Miembros de juntas comprometidos**	**Vocales comprometidos**	**Candidatos electos cambiados**
Faro	10 %	35.0	4370.4	0.50
Faro	20 %	69.9	8664.7	1.20
Faro	30 %	104.0	12 806.2	2.03
Tómbola	10 %	34.5	4512.7	0.56
Tómbola	20 %	69.7	9183.3	1.38
Tómbola	30 %	104.2	13 690.0	2.17

Resultados en caso de asignación al mayor del pacto, agrupados por valores de probabilidad de que un miembro de una junta electoral sea corrupto.

Tipo Sorteo	**Prob. Encontrar Vocal**	**Miembros de juntas comprometidos**	**Vocales comprometidos**	**Candidatos electos cambiados**
Faro	40 %	69.9	6901.6	0.86
Faro	60 %	69.4	10 325.9	1.63
Tómbola	40 %	69.3	7366.5	0.99
Tómbola	60 %	69.6	10 890.8	1.75

Resultados en caso de asignación al mayor del pacto, agrupados por valores de probabilidad de que un miembro comprometido de una junta encuentre un vocal comprometido para el sorteo.

Tipo Sorteo	**Prob. Junt. Comp**	**Prob. Encontrar Vocal**	**Miembros de juntas comprometidos**	**Vocales comprometidos**	**Candidatos electos cambiados**
Faro	10 %	40 %	35.5	3529.9	0.33
Faro	10 %	60 %	34.6	5211.0	0.68
Faro	20 %	40 %	70.2	6907.1	0.89
Faro	20 %	60 %	69.5	10 422.3	1.51
Faro	30 %	40 %	104.0	10 267.9	1.36
Faro	30 %	60 %	104.0	15 344.6	2.69
Tómbola	10 %	40 %	34.3	3631.5	0.34
Tómbola	10 %	60 %	34.7	5393.9	0.79
Tómbola	20 %	40 %	70.0	7394.6	1.01
Tómbola	20 %	60 %	69.5	10 971.9	1.74
Tómbola	30 %	40 %	103.7	11 073.4	1.60
Tómbola	30 %	60 %	104.7	16 306.7	2.73

Resultados en caso de asignación al mayor del pacto, agrupados por valores de probabilidad de miembros de junta comprometida y probabilidad de encontrar vocales comprometidos para el sorteo.

Tipo Sorteo	Prob. Compuesta	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	No	69.4	8448.0	0.94
Faro	Sí	69.6	8434.6	0.91
Tómbola	No	69.4	9066.3	1.08
Tómbola	Sí	69.4	8960.9	1.07

Resultados en caso de mayoría simple,, agrupados por inclusión de probabilidad compuesta.

Tipo Sorteo	Límite Vocales	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	3	69.6	8450.5	1.02
Faro	5	69.5	8432.0	0.82
Tómbola	3	69.1	8947.2	1.16
Tómbola	5	69.8	9080.1	0.99

Resultados en caso de mayoría simple, agrupados por valores de límite de vocales.

Tipo Sorteo	Porcentaje Edición	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	50 %	69.8	8438.0	0.45
Faro	70 %	69.5	8500.8	0.96
Faro	90 %	69.3	8385.0	1.36
Tómbola	50 %	69.3	9012.8	0.61
Tómbola	70 %	69.8	9039.7	1.07
Tómbola	90 %	69.2	8988.4	1.54

Resultados en caso de mayoría simple, agrupados por valores de edición de votos por los vocales de mesa.

Tipo Sorteo	Prob. Vocal Mesa	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	20 %	69.3	8427.7	2.05
Faro	10 %	69.6	8449.7	0.59
Faro	5 %	69.7	8446.4	0.14
Tómbola	20 %	69.5	9065.1	2.33
Tómbola	10 %	69.6	9009.9	0.73
Tómbola	5 %	69.2	8965.8	0.16

Resultados en caso de mayoría simple, agrupados por valores de probabilidad de éxito de un vocal en la edición de votos.

Tipo Sorteo	Prob. Éxito Miembro Junta	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	30 %	69.2	8407.6	0.96
Faro	20 %	69.5	8468.6	0.96
Faro	10 %	69.8	8447.6	0.85
Tómbola	30 %	69.3	9201.2	1.09
Tómbola	20 %	69.5	9072.1	1.07
Tómbola	10 %	69.5	8767.6	1.06

Resultados en caso de mayoría simple, agrupados por valores de probabilidad de éxito por parte de un miembro de la junta electoral para alterar el sorteo.

Tipo Sorteo	Candidatos Miembro	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	3	69.9	6372.6	0.46
Faro	5	69.1	10 509.9	1.39
Tómbola	3	69.5	6845.7	0.56
Tómbola	5	69.6	11 181.5	1.58

Resultados en caso de mayoría simple agrupados por cantidad máxima de vocales de mesa comprometidos que puede tener un miembro de junta comprometido.

Tipo Sorteo	Prob. Junt. Comp.	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	10 %	35.0	4224.5	0.27
Faro	20 %	69.2	8355.2	0.80
Faro	30 %	104.3	12 744.0	1.70
Tómbola	10 %	34.7	4483.3	0.33
Tómbola	20 %	69.0	8906.4	0.94
Tómbola	30 %	104.6	13 651.3	1.95

Resultados en caso de mayoría simple, agrupados por valores de probabilidad de que un miembro de una junta electoral sea corrupto.

Tipo Sorteo	Prob. Encontrar Vocal	Miembros de juntas comprometidos	Vocales comprometidos	Candidatos electos cambiados
Faro	40 %	69.5	6761.0	0.56
Faro	60 %	69.6	10 121.5	1.29
Tómbola	40 %	69.7	7320.4	0.67
Tómbola	60 %	69.2	10 706.8	1.47

Resultados en caso de mayoría simple, agrupados por valores de probabilidad de que un miembro comprometido de una junta encuentre un vocal comprometido para el sorteo.

Tipo Sorteo	**Prob. Junt. Comp**	**Prob. Encontrar Vocal**	**Miembros de juntas comprometidos**	**Vocales comprometidos**	**Candidatos electos cambiados**
Faro	10 %	40 %	35.5	3435.2	0.17
Faro	10 %	60 %	34.4	5013.9	0.37
Faro	20 %	40 %	69.0	6671.6	0.50
Faro	20 %	60 %	69.5	10 038.9	1.11
Faro	30 %	40 %	104.0	10 176.3	1.01
Faro	30 %	60 %	104.7	15 311.7	2.38
Tómbola	10 %	40 %	34.7	3654.8	0.20
Tómbola	10 %	60 %	34.8	5311.7	0.45
Tómbola	20 %	40 %	69.3	7223.9	0.54
Tómbola	20 %	60 %	68.7	10 588.8	1.35
Tómbola	30 %	40 %	105.0	11 082.5	1.28
Tómbola	30 %	60 %	104.1	16 220.0	2.61

Resultados en caso de mayoría simple, agrupados por valores de probabilidad de miembros de junta comprometida y probabilidad de encontrar vocales comprometidos para el sorteo.