

Tabla de Contenido

1. Introducción	1
1.1. Contexto	1
1.2. Problema a Resolver	2
1.3. Hipótesis	3
1.4. Objetivos	3
1.5. Metodología	3
1.6. Resultados Esperados	3
1.7. Estructura de la Tesis	4
1.8. Contribuciones de este Trabajo	4
2. Marco Teórico	6
2.1. Estado del Arte	6
2.1.1. Análisis al sistema de Israel	6
2.1.2. Análisis de propiedades físicas de seguridad	7
2.1.3. Modelación de riesgo para votaciones	7
2.2. Elecciones en Chile	7
2.2.1. División Electoral de Chile	8
2.3. Sistemas Distribuidos	8
2.3.1. Relevancia para este trabajo	9
3. Elección de Vocales de Mesa	10
3.1. Personal Involucrado	10
3.1.1. Vocales de Mesa	10
3.1.2. Junta Electoral	10
3.2. Proceso de Selección	11
3.3. Casos de Ataque a la Selección de Vocales	13
3.3.1. Toda la junta está comprometida	13
3.3.2. Un solo miembro de la junta es malicioso	13
3.3.3. Dos miembros de la junta son maliciosos	14
3.3.4. Un tercero intenta alterar resultados al momento de realizar el sorteo	14
3.3.5. Un tercero hackea el sistema computacional usado	14
4. Día de Votación	16
4.1. Personal Involucrado	16
4.1.1. Digitador	16
4.2. Desarrollo de la Votación	17

4.2.1.	Constitución de mesas	17
4.2.2.	Votación en las mesas	17
4.2.3.	Conteo de votos	19
4.2.4.	Envío de información	21
4.2.5.	Resultados de la elección	22
4.2.6.	Flujo de información	25
4.3.	Posibles Casos de Ataque	25
4.3.1.	Vocales de mesa modifican resultados	25
4.3.2.	Digitador modifica resultados	26
4.3.3.	Sistema computacional es hackeado el día de las elecciones	26
5.	Simulación de una Elección	28
5.1.	Datos	28
5.1.1.	Resultados de elecciones	28
5.2.	Simulación	30
5.2.1.	Clases principales	30
5.2.2.	Parámetros globales	30
5.2.3.	Proceso	31
5.3.	Resultados y Análisis	34
5.3.1.	Probabilidad compuesta	35
5.3.2.	Límite de vocales	36
5.3.3.	Porcentaje de edición	36
5.3.4.	Probabilidad de éxito de vocal de mesa	37
5.3.5.	Probabilidad de éxito de miembro de la junta	38
5.3.6.	Probabilidad de junta comprometida	39
5.3.7.	Probabilidad de encontrar vocales y cantidad de vocales	39
5.3.8.	Probabilidad de junta comprometida y de encontrar vocal	41
5.3.9.	Sorteo individual por mesa	41
5.3.10.	Elección distinta de candidato para modificación de votos	43
5.3.11.	Elección por mayoría simple	44
5.3.12.	Datos generales	45
6.	Escrutinio Posterior	47
6.1.	Descripción del Proceso	47
6.1.1.	Antes del escrutinio	47
6.1.2.	Escrutinio	47
6.1.3.	Flujo de información	48
6.2.	Casos de Ataque al Escrutinio	49
6.2.1.	Miembros del Colegio intentan cambiar resultados en el escrutinio	49
6.2.2.	Miembros del Colegio coludido con vocales de mesa corruptos	49
6.2.3.	Colusión con digitador	50
7.	Tribunal Calificador de Elecciones	51
7.1.	Descripción	51
7.2.	Proceso de Escrutinio General	51
7.2.1.	Flujo de información	52
7.3.	Casos de Ataque al Escrutinio General	53

7.3.1.	TRICEL intenta alterar resultados	53
7.3.2.	Hackeo general a sistemas computacionales	53
8.	Análisis Global	54
8.1.	Antes de las Elecciones	54
8.1.1.	Miembros de la junta comprometidos	54
8.1.2.	Intento de alterar resultados al momento de realizar el sorteo por parte de un tercero	54
8.1.3.	Un tercero hackea el sistema computacional usado	55
8.2.	Día de las Elecciones	55
8.2.1.	Modificación de resultados por vocales de mesa	55
8.2.2.	Modificación de resultados por parte del digitador	57
8.2.3.	Sistema computacional es hackeado el día de las elecciones	57
8.3.	Escrutinio Posterior	58
8.3.1.	Colegio Escrutador cambia resultados en el escrutinio	58
8.3.2.	Colegio coludido con vocales de mesa corruptos	58
8.3.3.	Colusión de Colegio Escrutador con digitador	58
8.4.	Escrutinio General	59
8.4.1.	Hackeo general a sistemas computacionales	59
9.	Mitigaciones a Ataques	61
9.1.	Aleatoriedad Verificable	61
9.1.1.	Acerca del Faro	61
9.1.2.	Uso de Faro para Selección de Vocales	62
9.1.3.	Ataques al Faro de Aleatoriedad	63
9.1.4.	Efecto del Faro en ataques a selección de vocales	64
9.1.5.	Simulación usando Faro de Aleatoriedad	64
9.2.	Auditoría Estadística	66
	Conclusión	68
	Bibliografía	72
A.	Actas del Día de Votación	75
B.	Resultados Adicionales de Simulaciones	78