

Tabla de Contenido

| | |
|---|-----------|
| 1. Introducción | 1 |
| 1.1. Contexto | 1 |
| 1.2. Objetivos | 2 |
| 1.2.1. Objetivo General | 2 |
| 1.2.2. Objetivos Específicos | 3 |
| 1.3. Descripción General de la Solución | 3 |
| 2. Marco Teórico | 6 |
| 2.1. Votaciones Chilenas | 6 |
| 2.2. Votación Electrónica | 7 |
| 2.3. Auditorías de Confirmación | 7 |
| 2.3.1. Características Generales | 7 |
| 2.3.2. Ballot-Polling Audits | 8 |
| 2.3.3. Comparison Audits | 8 |
| 2.3.4. Métricas de Certeza | 9 |
| 2.3.5. Variaciones Algorítmicas | 9 |
| 2.3.6. Aplicaciones | 10 |
| 2.4. Aleatoriedad Verificable | 11 |
| 2.4.1. Fuente de Aleatoriedad Verificable | 11 |
| 2.4.2. Selección de Muestras Aleatorias | 11 |
| 3. Problema | 12 |
| 3.1. Descripción del Problema | 12 |
| 3.2. Relevancia | 12 |
| 3.3. Requisitos de la Solución | 13 |
| 3.3.1. Características Generales | 13 |
| 3.3.2. Aleatoriedad | 14 |
| 3.3.3. Validación de Elecciones | 14 |
| 3.3.4. Transparencia | 15 |
| 4. Solución | 16 |
| 4.1. Selección de Variantes Algorítmicas | 16 |
| 4.2. Diseño de Algoritmos | 17 |
| 4.2.1. Suposiciones | 17 |
| 4.2.2. Definiciones | 18 |
| 4.2.3. Tamaño de las Muestras | 19 |
| 4.2.4. Selección de Muestras | 20 |

| | | |
|-----------|--|-----------|
| 4.2.5. | Confirmación de Resultados | 21 |
| 4.3. | Adaptación al Caso Chileno | 24 |
| 4.3.1. | ¿Por Qué Auditar? | 24 |
| 4.3.2. | Selección del Tipo de Auditoría | 25 |
| 4.3.3. | Selección de Parámetros | 25 |
| 4.3.4. | Condiciones para Auditar Votos | 26 |
| 4.3.5. | ¿Quién Puede Auditar? | 26 |
| 4.4. | Prototipo | 27 |
| 4.4.1. | Descripción General | 27 |
| 4.4.2. | Arquitectura General | 27 |
| 4.4.2.1. | Dependencias | 27 |
| 4.4.2.2. | Componentes | 28 |
| 4.4.2.3. | Django | 29 |
| 4.4.3. | Diseño de Base de Datos | 29 |
| 4.4.3.1. | Relaciones | 29 |
| 4.4.3.2. | Audit | 29 |
| 4.4.3.3. | RecountRegistry | 31 |
| 4.4.3.4. | SubAudit | 31 |
| 4.4.4. | Servicio Web | 32 |
| 4.4.4.1. | Vistas | 32 |
| 4.4.4.2. | Ejemplo de Uso | 32 |
| 4.4.5. | Limitaciones | 36 |
| 4.4.6. | Extensibilidad a un Producto Terminado | 37 |
| 4.5. | Aplicabilidad a Votación Electrónica | 37 |
| 5. | Validación | 39 |
| 5.1. | Resolución del Problema | 39 |
| 5.2. | Simulación de Casos | 40 |
| 5.2.1. | Configuración General | 40 |
| 5.2.2. | Mayoría Simple | 41 |
| 5.2.3. | Pluralidad | 42 |
| 5.2.4. | Mayoría Absoluta | 43 |
| 5.2.5. | D'Hondt | 44 |
| 5.3. | Optimización para Batch-Level Comparison | 45 |
| 6. | Conclusiones | 49 |
| 6.1. | Resumen | 49 |
| 6.2. | Revisión de Objetivos | 49 |
| 6.3. | Análisis de Resultados | 50 |
| 6.3.1. | Votos Auditados | 50 |
| 6.3.2. | Confirmaciones | 51 |
| 6.4. | Trabajo Futuro | 51 |
| | Bibliografía | 53 |