Universidad de Oviedo
Universidá d'Uviéu
University of Oviedo

Sistema de encuestas y votación telemática

TRABAJO FIN DE GRADO

GRADO EN INGENIERÍA INFORMÁTICA DEL SOFTWARE

AUTOR

Alejo Brandy García-Rovés

TUTOR

Benjamín López Pérez

Julio 2022

Resumen

Las votaciones son uno de los actos más importantes en el que las personas pueden tomar decisiones colectivas.

Durante los últimos años han aparecido distintos sistemas de voto electrónico, pero no todos han conseguido tener buena usabilidad, garantizar la confidencialidad de los votantes, además de la integridad y autenticidad de los votos.

Este trabajo describe una aplicación de escritorio para la realización de procesos electorales que cumplen con todos los objetivos citados anteriormente.

Se trata de una aplicación desarrollada por la Universidad de Palermo, que se ha implantado, estudiado, internacionalizado, adaptado y extendido.

Está pensado para que distintas organizaciones e instituciones lo utilicen. Incluso, para que puedan extenderlo.

Palabras clave

Proceso electoral, urna, mesa electoral, puesto de votación, recuento, usabilidad, confidencialidad, integridad, autenticidad, votante, voto.

Abstract

Voting is one of the most important acts in which people can make collective decisions.

In recent years, different electronic voting systems have appeared, but not all have managed to have good usability, guarantee the confidentiality of voters, as well as the integrity and authenticity of the votes.

This paper describes a desktop application for conducting electoral processes that meet all the targets mentioned above.

It is an application developed by the University of Palermo, which has been implemented, studied, internationalized, adapted and extended.

It is designed for different organizations and institutions to use. Even, so that they can extend it.

Keywords

Electoral process, ballot box, polling station, recount, usability, confidentiality, integrity, authenticity, voter, vote.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Capítulo 1 PRESENTACIÓN

1.1 OBJETIVOS DEL PROYECTO

Los objetivos principales del proyecto son los siguientes:

- Buscar un sistema de software libre, implantarlo y que sea funcional. Estudiarlo y documentarlo en profundidad.
- El sistema debe permitir que el voto se almacene de forma segura y se garantice la integridad y anonimidad de los votos.
- Además, otro de los objetivos es que se pueda verificar los resultados del proceso electoral una vez que este finalice, emitiendo informes necesarios.
- El sistema de debe de ser flexible, es decir, que se puedan realizar distintos tipos de votaciones y encuestas. Pudiendo seleccionar una o varias opciones en cada pregunta. Así mismo se deben contabilizar los votos nulos.
- Por otra parte, se debe contemplar que una persona pueda votar de manera remota.

Capítulo 2 PLANIFICACIÓN DEL SISTEMA DE INFORMACIÓN

2.1 INICIO DEL PLAN DE SISTEMAS DE INFORMACIÓN

2.1.1 Análisis de la Necesidad del PSI

Las votaciones reflejan los cambios sociales de las distintas comunidades. En la Antigua Grecia ya se realizaban votaciones levantado las manos o usando piedras. Estos métodos fueron evolucionando a medida que iba pasando el tiempo, mediante la introducción de cabinas de votación o papeletas.

Aun así, parece que todas las mejoras no han sido suficientes. El proceso de votación físico es lento y lleva mucho trabajo. Basta con pensar en cada vez que hay unas elecciones generales, autonómicas, etc. lo que conlleva todo el proceso.

En los próximos capítulos, voy a exponer una solución que mejora la eficiencia y la seguridad de las votaciones. Con las técnicas de seguridad existentes se puede conseguir que el proceso sea totalmente transparente y verificable, acelerar la votación, asegurar la privacidad de los usuarios, así como garantizar la integridad de los votos.

Aparte de lo mencionado, los sistemas de votación electrónica pueden proporcionar apoyo a los usuarios (como asistencia de voz para personas con discapacidad visual) y llegar a un mayor número de personas.

2.1.2 Identificación del Alcance del PSI

Sin embargo, a pesar de sus indudables ventajas, el uso de sistemas de votación electrónicos aún no está claro. La adopción de este sistema implica distintos retos.

Uno de los más relevantes es el proceso de autenticación de los usuarios preservando a su vez su anonimato, garantizando la privacidad y confidencialidad de los votos. Podemos catalogar que

ganarse la confianza de los votantes es uno de los problemas más difíciles a resolver. Después de todo, si los sistemas tradicionales de votación funcionan, ¿por qué debemos cambiarlos?

Por esta razón, teniendo en cuenta que la percepción positiva de los usuarios de un sistema es esencial, nuestro objetivo es crear un sistema de voto electrónico que mantenga las características de las elecciones tradicionales, mejorando la seguridad y usabilidad. Por ejemplo, decidimos mantener la necesidad de votar en un colegio electoral físico, aunque sea de forma digital.

Una característica principal de este proyecto es de código abierto por lo que se puede analizar y verificar.

Todo esto da como resultado los siguientes objetivos estratégicos:

- Evaluación de las distintas alternativas.
- Elección de la mejor solución.
- Análisis profundo de la solución elegida.
- Desarrollar ampliaciones.

2.2 DEFINICIÓN Y ORGANIZACIÓN DEL PSI

2.2.1 Especificación del Ámbito y Alcance

En función de los objetivos estratégicos vistos, el proyecto se divide en las siguientes fases/objetivos generales, con los siguientes objetivos por cada fase:

2.2.1.1 Evaluación de las distintas alternativas

Como ya se comentó, necesitamos una solución que mejore el proceso actual de votación físico, evitando la lentitud y la pesadez que implica. Y asegurándose que el votante confía en la solución electrónica.

Como comentaremos en Estudio de Viabilidad del Sistema, se han considerado varias alternativas.

2.2.1.2 Elección de la mejor solución

Después de un largo periodo de reflexión, el proyecto escogido es SecureBallot, pues garantiza las características en las que habíamos pensado.

En esta fase se procede a un estudio de la viabilidad del proyecto y a la implantación del sistema.

2.2.1.3 Análisis profundo de la solución elegida

Una vez ya con la solución en marcha, se produce una especificación detallada de los requisitos y documentación extensa de las partes del sistema más interesantes.

2.2.1.4 Desarrollo de ampliaciones

A continuación, vendría la fase de implementación de ampliaciones que aportan un valor añadido a la solución inicial, como son:

- Generación de tokens para que los usuarios accedan a los puestos de votación.
- Sistema de usuario-contraseña web.
- Internacionalización del sistema

2.3 ESTUDIO DE LA INFORMACIÓN RELEVANTE

2.3.1 Selección y Análisis de Antecedentes

2.3.1.1 Voto presencial

El voto presencial es la forma más común de votación, consiste en acudir personalmente a la mesa electoral que nos corresponde.

Se puede consultar dónde se ubica la mesa electoral que le corresponde, desde la Web del Instituto Nacional de Estadística, sin necesidad de acreditarse mediante certificado digital, cumplimentando, al menos, los datos de municipio, provincia y letra inicial del primer apellido, que son obligatorios.

La identificación del elector ante la Mesa se realiza mediante:

- Documento nacional de identidad (D.N.I.)
- Pasaporte (con fotografía).
- Permiso (carné) de conducir (con fotografía).
- Tarjeta de residencia, en el caso de ciudadanos de la Unión Europea que la posean.
- Tarjeta de identidad de extranjero, en el caso de nacionales de países con los que España haya suscrito un tratado de reciprocidad para el reconocimiento del derecho de sufragio en las elecciones municipales.

No importa que estos documentos estén caducados, pero deben ser los originales, no siendo válidas las fotocopias.

2.3.1.2 AES

El algoritmo AES (Advanced Encryption Standard) aplica sucesivamente una serie de transformaciones matemáticas a cada bloque de datos de 128 bits. Debido a que la computación es baja, AES se puede utilizar con dispositivos informáticos como portátiles y teléfonos inteligentes, así como para cifrar rápidamente grandes cantidades de datos.

AES es un algoritmo simétrico que utiliza la misma clave de 128, 192 o 256 bits tanto para el cifrado como para el descifrado (la seguridad de un sistema AES aumenta exponencialmente con la longitud de la clave). Incluso con una clave de 128 bits, la tarea de descifrar AES verificando cada uno de los 2128 valores posibles (un ataque de "fuerza bruta") es tan computacionalmente intensiva que incluso la supercomputadora más rápida requeriría más de 100 billones de años para hacerlo.

De hecho, AES nunca se ha descifrado, y según las tendencias tecnológicas actuales, se espera que siga siendo seguro en los próximos años.

2.3.1.3 RSA

RSA lleva el nombre de los científicos del MIT (Rivest, Shamir y Adleman) que lo describieron por primera vez en 1977. Es un algoritmo asimétrico que utiliza una clave pública para el cifrado, pero que también necesita una clave privada para el descifrado.

En este sistema, llamado criptografía de clave pública (PKC), la clave pública es el producto de multiplicar dos enormes números primos juntos. Solo ese producto, 1024, 2048 o 4096 bits de longitud, se hace público. Debido a que no existe un método conocido para calcular los factores primos de números tan grandes, solo el creador de la clave pública puede generar la clave privada para el descifrado.

RSA es computacionalmente más intensivo que AES, y mucho más lento. Normalmente se usa para cifrar solo pequeñas cantidades de datos.

Capítulo 3 ESTUDIO DE VIABILIDAD DEL SISTEMA

3.1 ESTUDIO

Se pueden identificar dos categorías principales de voto electrónico:

- **Votación no supervisada**, también conocida como votación electrónica remota, que permite a los usuarios votar a distancia a través de internet.
- **Votación supervisada**, que requiere centros de votación físicos monitoreados por funcionarios electorales.

El voto electrónico remoto permite a los usuarios votar sin estar físicamente presentes como sí sucede en entornos supervisados. Esta es la mejor opción para los votantes, pero sin embargo tiene dos problemas principales.

En primer lugar, los votantes tienen que confiar en la votación (se aplica tanto a los sistemas a distancia como a los supervisados). A menudo, los usuarios obtienen un recibo virtual a través del cual pueden comprobar que han votado. Pero el uso de los recibos plantea posibles problemas de privacidad: si hay cualquier asociación entre el voto y el votante, se podría llegar a rastrear. Por lo que deberían evitarse.

En segundo lugar, se debe asegurar que los usuarios voten de forma libre sin ninguna influencia externa. Para garantizar este aspecto, es esencial que los votantes estén solos. Esta es una cuestión que no se puede garantizar con un sistema de voto electrónico remoto.

Por otra parte, también es importante garantizar el secreto de los votos.

3.2 VALORACIÓN DE ALTERNATIVAS DE SOLUCIÓN

3.2.1 Helios voting

Helios es uno de los sistemas de voto electrónico de código abierto más famosos. Más de 2 millones de votos fueron emitidos usando Helios.

Los votos en Helios se envían después de ser encriptados por lo que se garantiza el secreto de los votos. Cada votante obtiene un número de seguimiento del voto. Tienen el problema de que no hacen ningún intento para evitar que los votantes pueden ser influenciados a la hora de la votación.

3.2.2 Voto y encuestas telemáticas en la Universitat Jaume I

Se trata de un sistema de encuestas y voto telemático de la Universitat Jaume I.

Tiene como objetivo, la realización de votaciones y encuestas de forma anónima y no trazables a través de un sistema realizado por ellos denominado eSurvey.

El sistema ofrece las máximas garantías de integridad, unicidad, anonimato y auditabilidad.

No obstante, no se puede garantizar que los votantes expresen sus preferencias de forma libre sin ninguna influencia externa.

Pese a todos los aspectos positivos que tiene este sistema, tuve que descartarlo debido a que está sin mantener por parte de los responsables y, por ende, parado.

3.2.3 Kuorum

Kuorum es una plataforma de votación online donde el voto telemático es secreto, libre y directo. A la hora de realizar una votación se puede gestionar a los votantes utilizando distintos permisos de voto. Otra característica llamativa es que se puede monitorizar las estadísticas de participación en tiempo real, filtrando los datos por género, área geográfica, etc.

La desventaja que tiene es que es software propietario y que se asigna un recibo virtual a cada votante.

3.2.4 SecureBallot

SecureBallot es un sistema que no mantiene un vínculo entre los votantes y los votos, por tanto, no se entrega un recibo a los votantes para que estos puedan verificar su voto.

Es un sistema supervisado, por tanto, no hay lugar a que ningún agente externo interfiera en la votación de una persona.

También, se debe mencionar que es un proyecto bastante reciente, de 2021.

Por último, cabe destacar que es de código abierto. Por ello, me he decantado por esta solución.

3.3 SELECCIÓN DE LA ALTERNATIVA FINAL

A continuación, se muestra una tabla con las características de los sistemas anteriormente valorados:

Características	Helios	Universitat Jaume I	Kuorum	Secureballot
Código abierto	X	X		X
Voto secreto	X	X	X	X
Voto no trazable		X		X
Votante no influenciable				X
Está mantenido	X		X	X

Tabla 1. Características sistemas

El sistema SecureBallot, recoge todas las características que me resultan interesantes por lo que es mi elección.

Capítulo 4 PLANIFICACIÓN Y GESTIÓN DEL TFG

4.1 PLANIFICACIÓN DEL PROYECTO

4.1.1 Identificación de Interesados

Los distintos interesados en el proyecto son los siguientes:

- Miembros del equipo del proyecto: personal que conforma el equipo de desarrollo del proyecto.
- Personal que interviene en la realización del proceso electoral: usuario raíz, supervisores y técnicos.
- Candidatos que se presentan a las elecciones.
- Votantes.
- Instituciones y organizaciones que deseen implantar el proyecto.

4.1.2 Planificación

En este apartado, se presenta la planificación del proyecto.

Se estimó que se trabajaría 8 horas al día.

A continuación, se muestren las etapas que componen la planificación:

- Estudio de viabilidad
- Arranque del proyecto
- Análisis
- Diseño
- Implementación
- Pruebas
- Documentación
- Despliegue
- Cierre del proyecto
- Reuniones con el cliente

Debemos distinguir entre una planificación inicial y otra final, pues se produjeron retrasos que se comentarán a continuación.

4.1.2.1 Planificación inicial

4.1.2.1.1 Estudio de viabilidad

La etapa "Estudio de la viabilidad" es la inicial del proyecto. Se estimó que la duración sería de algo menos de 7 días.

Núm.	Nombre de tarea	Duración	Comienzo	Fin
1.1	Estudio de viabilidad	6,88 días	mar 15/02/22	mié 23/02/22
1.1.1	Estudio del arte	3 horas	mar 15/02/22	mar 15/02/22
1.1.2	Contacto con responsables	2 horas	mar 15/02/22	mar 15/02/22
1.1.3	Plan de viabilidad	6 horas	mar 15/02/22	mié 16/02/22
1.1.4	Estudio de alternativas	2 días	mié 16/02/22	vie 18/02/22
1.1.5	Planificación inicial	1 día	vie 18/02/22	lun 21/02/22
1.1.6	Elaboración presupuesto inicial	2 días	lun 21/02/22	mié 23/02/22
1.1.7	Requisitos iniciales	4 horas	mié 23/02/22	mié 23/02/22

Tabla 2. Estudio de viabilidad

4.1.2.1.2 Arranque del proyecto

La etapa "Arranque del proyecto" es la segunda del proyecto, donde ya se profundiza más en este. Se estimó que la duración sería de algo más de 5 días.

Núm.	Nombre de tarea	Duración	Comienzo	Fin
1.2	Arranque del proyecto	5,19 días	mié 23/02/22	jue 03/03/22
1.2.1	Revisión de objetivos	1 día	mié 23/02/22	jue 24/02/22
1.2.2	Revisión de requisitos	0,5 horas	jue 24/02/22	jue 24/02/22
1.2.3	Preparación del entorno de desarrollo y pruebas	2 días	vie 25/02/22	lun 28/02/22
1.2.4	Configuración del entorno de desarrollo	2 días	mar 01/03/22	mié 02/03/22
1.2.5	Revisión de la planificación	0,5 horas	jue 03/03/22	jue 03/03/22
1.2.6	Cierre presupuesto inicial	0,5 horas	jue 03/03/22	jue 03/03/22

Tabla 3. Arranque del proyecto

4.1.2.1.3 Análisis

La fase "Análisis" es la siguiente del proyecto. Se definen y se especifican los requisitos con detalle y se elabora el presupuesto de cliente inicial.

Se estimó que la duración sería de 6 días.

Núm.	Nombre de tarea	Duración	Comienzo	Fin
1.3	Análisis	6 días	jue 03/03/22	vie 11/03/22
1.3.1	Definir requisitos con detalle	1 día	jue 03/03/22	vie 04/03/22
1.3.2	Especificación detallada de requisitos	3 días	vie 04/03/22	mié 09/03/22
1.3.3	Elaboración de presupuesto de cliente inicial	2 días	mié 09/03/22	vie 11/03/22
1.4	Hito – fin de análisis			

Tabla 4. Análisis

4.1.2.1.4 Diseño

La fase "Diseño" es la siguiente del proyecto. En la planificación inicial, se estimó que la duración sería ligeramente superior a los 6 días.

Núm.	Nombre de tarea	Duración	Comienzo	Fin
1.5	Diseño	6,06 días	vie 11/03/22	lun 21/03/22
1.5.1	Definición de la arquitectura	1 día	vie 11/03/22	lun 14/03/22
1.5.2	Diseño de clases	2 días	lun 14/03/22	mié 16/03/22
1.5.3	Especificación del modelo de datos	1 día	mié 16/03/22	jue 17/03/22
1.5.4	Especificación de las interfaces de comunicación	0,5 horas	jue 17/03/22	jue 17/03/22
1.5.5	Diseño de interfaces de usuario	2 días	jue 17/03/22	lun 21/03/22
1.6	Hito – fin de diseño			

Tabla 5. Diseño

4.1.2.1.5 Implementación

La etapa "Implementación" es la siguiente del proyecto. En la planificación inicial, se estimó que la duración sería de 14 días.

Núm.	Nombre de tarea	Duración	Comienzo	Fin
1.7	Implementación	14 días	lun 21/03/22	vie 08/04/22
1.7.1	Nuevas mejoras del sistema	14 días	lun 21/03/22	vie 08/04/22

Tabla 6. Implementación

4.1.2.1.6 Pruebas

La etapa "Pruebas" es la siguiente del proyecto. En la planificación inicial, se estimó que la duración sería de 5 días.

Núm.	Nombre de tarea	Duración	Comienzo	Fin
1.8	Pruebas	5 días	vie 08/04/22	vie 15/04/22

1.8.1	Implementación de pruebas unitarias	1 día	vie 08/04/22	lun 11/04/22
1.8.2	Pruebas de integración	4 días	lun 11/04/22	vie 15/04/22
1.8.2.1	Diseño	1 día	lun 11/04/22	mar 12/04/22
1.8.2.2	Implementación	1 día	mar 12/04/22	mié 13/04/22
1.8.2.3	Ejecución	1 día	mié 13/04/22	jue 14/04/22
1.8.2.4	Documentación	1 día	jue 14/04/22	vie 15/04/22

Tabla 7. Pruebas

4.1.2.1.7 Documentación

La fase "Documentación" es la siguiente del proyecto. En la planificación inicial, se estimó que la duración sería de 6 días.

Núm.	Nombre de tarea	Duración	Comienzo	Fin
1.9	Documentación	6 días	vie 15/04/22	lun 25/04/22
1.9.1	Realizar la documentación y manuales de instalación	2 días	vie 15/04/22	mar 19/04/22
1.9.2	Realizar la documentación y manuales de configuración del sistema	2 días	mar 19/04/22	jue 21/04/22
1.9.3	Realizar la documentación y manuales de ejecución del sistema	2 días	jue 21/04/22	lun 25/04/22

Tabla 8. Documentación

4.1.2.1.8 Despliegue

La etapa "Despliegue" es la siguiente del proyecto. En la planificación inicial, se estimó que la duración sería de 3 días.

Núm.	Nombre de tarea	Duración	Comienzo	Fin
1.10	Despliegue	3 días	lun 25/04/22	jue 28/04/22
1.10.1	Instalar el sistema en los servidores de prueba y producción de la empresa contratante	1 día	lun 25/04/22	mar 26/04/22
1.10.2	Desplegar el sistema en los servidores de prueba y producción de la empresa contratante	1 día	mar 26/04/22	mié 27/04/22
1.10.3	Ejecución de pruebas de integración en los servidores de prueba y producción de la empresa contratante	1 día	mié 27/04/22	jue 28/04/22

Tabla 9. Despliegue

4.1.2.1.9 Cierre de proyecto

La etapa “Cierre de proyecto” es la siguiente del proyecto. En la planificación inicial, se estimó que la duración sería de casi 35 días. Se debe resaltar que entre las fases “Cierre memoria” y “Defensa TFG”, existe una diferencia de fechas sustancial.

Núm.	Nombre de tarea	Duración	Comienzo	Fin
1.11	Cierre de proyecto	34,75 días	jue 28/04/22	jue 16/06/22
1.11.1	Cierre del presupuesto de cliente	0,5 horas	jue 28/04/22	jue 28/04/22
1.11.2	Definición de ampliaciones futuras	1 día	jue 28/04/22	vie 29/04/22
1.11.3	Cambios en la documentación	1 día	vie 29/04/22	lun 02/05/22
1.11.4	Guardar copia de código y documentación para consultas futuras	0,2 horas	lun 02/05/22	lun 02/05/22
1.11.5	Cierre memoria	3 horas	lun 02/05/22	lun 02/05/22
1.11.6	Defensa TFG	0,5 horas	jue 16/06/22	jue 16/06/22

Tabla 10. Cierre de proyecto

4.1.2.1.10 Reuniones con el cliente

La fase de “Reuniones con el cliente” es la siguiente del proyecto. En la planificación inicial, se estimó que la duración sería de algo más de 97 días. Cada tarea se desarrolla cada cierto tiempo.

Núm.	Nombre de tarea	Duración	Comienzo	Fin
1.13	Reuniones con el cliente	97,31 días	mié 24/11/21	vie 08/04/22
1.13.1	Reunión - Toma de contacto	0,5 horas	mié 24/11/21	mié 24/11/21
1.13.2	Reunión - Estudio de viabilidad	0,5 horas	vie 04/02/22	vie 04/02/22
1.13.3	Reunión - Arranque de proyecto	0,5 horas	mié 23/02/22	mié 23/02/22
1.13.4	Reunión - Principio de Análisis	0,5 horas	jue 03/03/22	jue 03/03/22
1.13.5	Reunión - Fin de Análisis	0,5 horas	vie 11/03/22	vie 11/03/22
1.13.6	Reunión - Fin de Diseño	0,5 horas	lun 21/03/22	lun 21/03/22
1.13.7	Reunión - Fin implementación	0,5 horas	vie 08/04/22	vie 08/04/22

Tabla 11. Reuniones con el cliente

4.1.2.2 Planificación final

4.1.2.2.1 Estudio de viabilidad

En este caso, no hay distinción entre la planificación inicial y la final. Ver Estudio de viabilidad

4.1.2.2.2 Arranque del proyecto

En este caso, no hay distinción entre la planificación inicial y la final. Ver Arranque del proyecto

4.1.2.2.3 Análisis

En este caso, no hay distinción entre la planificación inicial y la final. Ver Análisis

4.1.2.2.4 Diseño

En la planificación final, se produjeron retrasos en las siguientes tareas:

- Diseño de clases.
- Especificación del modelo de datos.
- Especificación del modelo de datos.
- Especificación de las interfaces de comunicación.
- Diseño de interfaces de usuario

La duración fue de algo más de 11 días.

Núm.	Nombre de tarea	Duración	Comienzo	Fin
1.5	Diseño	11,25 días	vie 11/03/22	lun 28/03/22
1.5.1	Definición de la arquitectura	1 día	vie 11/03/22	lun 14/03/22
1.5.2	Diseño de clases	3 días	lun 14/03/22	jue 17/03/22
1.5.3	Especificación del modelo de datos	2 días	jue 17/03/22	lun 21/03/22
1.5.4	Especificación de las interfaces de comunicación	2 horas	lun 21/03/22	lun 21/03/22
1.5.5	Diseño de interfaces de usuario	5 días	lun 21/03/22	lun 28/03/22
1.6	Hito – fin de diseño			

Tabla 12. Diseño final

4.1.2.2.5 Implementación

En la planificación final, se produjo un retraso en la tarea “Nuevas mejoras del sistema”. La duración fue de 27 días.

Núm.	Nombre de tarea	Duración	Comienzo	Fin
1.7	Implementación	27 días	lun 28/03/22	mié 04/05/22
1.7.1	Nuevas mejoras del sistema	27 días	lun 28/03/22	mié 04/05/22

Tabla 13. Implementación final

4.1.2.2.6 Pruebas

En la planificación final, se produjo un retraso en las tareas:

- Implementación de pruebas unitarias.
- Diseño.

La duración fue de 9 días, 4 más que en la planificación inicial.

Núm.	Nombre de tarea	Duración	Comienzo	Fin
1.8	Pruebas	9 días	mié 04/05/22	mar 17/05/22
1.8.1	Implementación de pruebas unitarias	3 días	mié 04/05/22	lun 09/05/22
1.8.2	Pruebas de integración	6 días	lun 09/05/22	mar 17/05/22
1.8.2.1	Diseño	3 días	lun 09/05/22	jue 12/05/22
1.8.2.2	Implementación	1 día	jue 12/05/22	vie 13/05/22
1.8.2.3	Ejecución	1 día	vie 13/05/22	lun 16/05/22
1.8.2.4	Documentación	1 día	lun 16/05/22	mar 17/05/22

Tabla 14. Pruebas final

4.1.2.2.7 Documentación

En la planificación final, se produjo retraso en todas las tareas.

La duración fue de 14 días, 8 más que en la planificación inicial.

Núm.	Nombre de tarea	Duración	Comienzo	Fin
1.9	Documentación	14 días	mar 17/05/22	lun 06/06/22
1.9.1	Realizar la documentación y manuales de instalación	4 días	mar 17/05/22	lun 23/05/22
1.9.2	Realizar la documentación y manuales de configuración del sistema	5 días	lun 23/05/22	lun 30/05/22
1.9.3	Realizar la documentación y manuales de ejecución del sistema	5 días	lun 30/05/22	lun 06/06/22

Tabla 15. Documentación final

4.1.2.2.8 Despliegue

En la planificación final, como podemos observar, la duración no ha cambiado. Sin embargo, cabe destacar que tanto la fecha de comienzo como de fin, son posteriores a las respectivas de la planificación inicial.

Núm.	Nombre de tarea	Duración	Comienzo	Fin
1.10	Despliegue	3 días	lun 06/06/22	jue 09/06/22
1.10.1	Instalar el sistema en los servidores de prueba y	1 día	lun 06/06/22	mar 07/06/22

	producción de la empresa contratante			
1.10.2	Desplegar el sistema en los servidores de prueba y producción de la empresa contratante	1 día	mar 07/06/22	mié 08/06/22
1.10.3	Ejecución de pruebas de integración en los servidores de prueba y producción de la empresa contratante	1 día	mié 08/06/22	jue 09/06/22

Tabla 16. Despliegue final

4.1.2.2.9 Cierre del proyecto

En la fase final, tiene una duración de casi 27 días. La fecha de comienzo y de fin de "Cierre de proyecto" son posteriores a las respectivas de la planificación inicial debido a los retrasos acumulados.

Núm.	Nombre de tarea	Duración	Comienzo	Fin
1.11	Cierre de proyecto	26,56 días	jue 09/06/22	lun 18/07/22
1.11.1	Cierre del presupuesto de cliente	0,5 horas	jue 09/06/22	jue 09/06/22
1.11.2	Definición de ampliaciones futuras	1 día	jue 09/06/22	vie 10/06/22
1.11.3	Cambios en la documentación	1 día	vie 10/06/22	lun 13/06/22
1.11.4	Guardar copia de código y documentación para consultas futuras	0,2 horas	lun 13/06/22	lun 13/06/22
1.11.5	Cierre memoria	3 horas	lun 13/06/22	lun 13/06/22
1.11.6	Defensa TFG	0,5 horas	lun 18/07/22	lun 18/07/22

Tabla 17. Cierre de proyecto final

4.1.2.2.10 Reuniones con el cliente

En la fase final, tiene una duración de casi 116 días.

Núm.	Nombre de tarea	Duración	Comienzo	Fin
1.13	Reuniones con el cliente	115,5 días	mié 24/11/21	mié 04/05/22
1.13.1	Reunión - Toma de contacto	0,5 horas	mié 24/11/21	mié 24/11/21
1.13.2	Reunión - Estudio de viabilidad	0,5 horas	vie 04/02/22	vie 04/02/22
1.13.3	Reunión - Arranque de proyecto	0,5 horas	mié 23/02/22	mié 23/02/22
1.13.4	Reunión - Principio de Análisis	0,5 horas	jue 03/03/22	jue 03/03/22
1.13.5	Reunión - Fin de Análisis	0,5 horas	vie 11/03/22	vie 11/03/22
1.13.6	Reunión - Fin de Diseño	0,5 horas	lun 28/03/22	lun 28/03/22

1.13.7	Reunión - Fin implementación	0,5 horas	mié 04/05/22	mié 04/05/22

Tabla 18. Reuniones con el cliente final

4.1.2.3 Conclusión

A continuación, haremos un resumen de la comparativa entre la planificación inicial y la final.

Durante las etapas iniciales: "Estudio de viabilidad", "Arranque del proyecto" y "Análisis", no existe diferencia alguna en la duración de la planificación y por tanto en las fechas de comienzo y fin.

No obstante, en la etapa de "Diseño" se produce una demora entre la duración planificada inicialmente y la final. También se produce en la "Implementación", las "Pruebas" y la "Documentación".

Sin embargo, en el "Despliegue" y en el "Cierre de proyecto" no se produce ningún retraso en la duración, es más hasta el "Cierre de proyecto" dura menos que la planificada en un principio, pero debido a los retrasos acumulados, las fechas van con retraso.

No he incluido en el siguiente gráfico, la fase "Reunión con el cliente" porque se desarrolla de forma uniforme durante todo el proyecto.

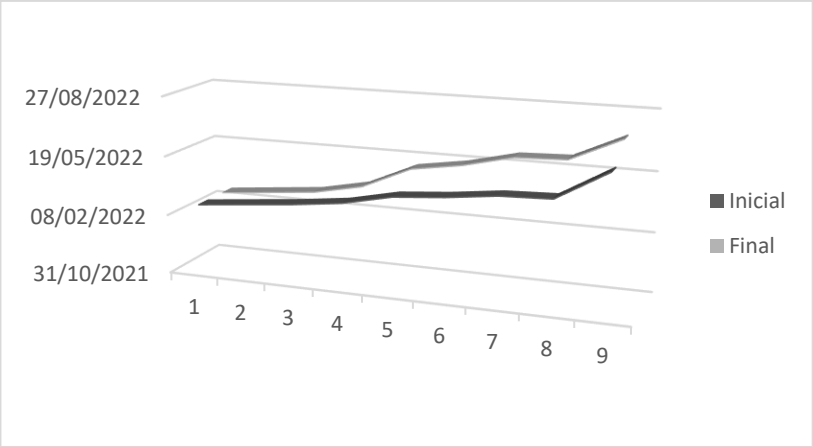

Ilustración 1. Conclusión planificación

4.1.3 Resumen del presupuesto

En este apartado, se muestran los recursos de trabajo, el resumen del presupuesto de costes y el presupuesto de cliente.

4.1.3.1 Recursos de trabajo

Los recursos de trabajo son los que se muestran en la siguiente tabla.

Nombre del recurso	Precio/hora (sin beneficios)
Jefe de proyecto	56,00 €
Arquitecto de software	45,00 €
Analista	43,00 €
Desarrollador SW	34,00 €
Tester	29,00 €
Administrador de Sistemas	32,00 €

Tabla 19. Tasas recursos de trabajo

El precio/hora (sin beneficios) para cada recurso de trabajo se ha escogido siguiendo la Guía de Aprendizaje de la asignatura de Dirección y Planificación de Proyectos Informáticos. Concretamente en el apartado 15.5 “Precio hora” del “Anexo VI. Modelo de Empresa”. Ver [23].

En caso de que un perfil de este proyecto no apareciera en ese apartado de la guía, realicé una estimación.

4.1.3.2 Resumen del presupuesto de costes

El desarrollo del proyecto es la fase que tiene un mayor coste, seguido del hardware y de los costes indirectos.

El presupuesto de costes es el conjunto de todas las partidas del proyecto. Se puede ver el detalle en Presupuesto de costes.

I1	I2		Subtotal
Proyecto		Desarrollo del proyecto	*39.306,20 €*
	1	Estudio de viabilidad	11.550,00 €
	2	Arranque del proyecto	1.979,00 €
	3	Análisis	2.272,00 €
	4	Diseño	4.050,00 €
	5	Implementación	7.344,00 €

	6	Pruebas	2.088,00 €
	7	Documentación	7.392,00 €
	8	Despliegue	1.208,00 €
	9	Cierre del proyecto	1.227,20 €
	10	Reuniones	196,00 €
HW	1	Hardware	*2.353,00 €*
CI	1	Costes indirectos	*471,02 €*
Coste total			**42.130,22 €**

Tabla 20. Presupuesto. Resumen del presupuesto de costes

4.1.3.3 Presupuesto de cliente

El presupuesto de cliente incluye un coste extra (beneficio del 20% del coste del desarrollo del proyecto y los costes indirectos).

El coste extra es de 8.332,26€ y se dividirá de forma prorrateada para cada partida del proyecto.

La fase de diseño se incrementará un 25% del coste extra. El análisis, un 20%. La implementación, las pruebas, la documentación y el despliegue un 10%. El estudio de la viabilidad, el arranque del proyecto y el cierre del proyecto un 5%. Mientras que las reuniones y el hardware no se incrementarán.

I1	**I2**		**Porcentaje**	**Cantidad añadida**	**Cantidad añadida total**
Proyecto		Desarrollo del proyecto			8.332,26 €
	1	Estudio de viabilidad	5%	416,61 €	
	2	Arranque del proyecto	5%	416,61 €	
	3	Análisis	20%	1.666,45 €	
	4	Diseño	25%	2.083,06 €	
	5	Implementación	10%	833,23 €	
	6	Pruebas	10%	833,23 €	

	7	Documentación	10%	833,23 €	
	8	Despliegue	10%	833,23 €	
	9	Cierre de proyecto	5%	416,61 €	
	10	Reuniones	0%	- €	
HW	1	Hardware	0%	- €	

Tabla 21. Presupuesto de cliente

El coste total es la suma del presupuesto de costes (42.130,22 €) y la suma de la cantidad añadida (8.332,26 €), es decir, **50.462,47 €.**

Capítulo 5 ANÁLISIS DEL SISTEMA DE INFORMACIÓN

5.1 DEFINICIÓN DEL SISTEMA

5.1.1 Determinación del Alcance del Sistema

5.1.1.1 Aplicación de escritorio

El objetivo de este proyecto es analizar el sistema SecureBallot, implantarlo e implementar nuevas mejoras para adaptarlo a nuestras necesidades. El sistema sirve para realizar votaciones.

El usuario root o el técnico se encargan de introducir los datos de un proceso electoral y de asignárselo a un supervisor.

El supervisor puede ver los resultados de la votación, pero una vez acabado el proceso electoral.

El supervisor se encarga de activar la urna, la mesa electoral y habilitar los puestos de votación.

El votante se dirige a un puesto de votación con el token generado por el supervisor.

El votante realiza la votación y una vez finalizada, devuelve el token al supervisor para enviar el voto con éxito.

5.1.1.2 Aplicación web

Algunos procesos electorales podrán recibir los votos desde una aplicación web para lo cual los usuarios deben registrarse y proporcionar un usuario y contraseña con el que se identificarán.

Esos usuarios pasarán a ser votantes y elegirán sus preferencias.

El voto enviado será así mismo encriptado siguiendo el proceso de encriptación del sistema de votación.

5.2 ESTABLECIMIENTO DE REQUISITOS

5.2.1 Obtención de los Requisitos del Sistema

5.2.1.1 Aplicación de escritorio

5.2.1.1.1 Proceso Electoral

RProcesoElectoral1 El sistema debe permitir que los usuarios del staff se encarguen de la gestión de los procesos electorales.

RProcesoElectoral1.1 El sistema debe permitir a los usuarios raíz crear nuevos usuarios.

RProcesoElectoral1.1.1 Deben especificar los siguientes datos:

RProcesoElectoral1.1.1.1 Nombre de usuario.

RProcesoElectoral1.1.1.1.1 Obligatorio.

RProcesoElectoral1.1.1.2 Contraseña.

RProcesoElectoral1.1.1.2.1 Obligatorio.

RProcesoElectoral1.1.1.3 Repetición de la contraseña.

RProcesoElectoral1.1.1.3.1. Obligatorio.

RProcesoElectoral1.1.1.4 Rol.

RProcesoElectoral1.1.1.4.1 Obligatorio.

RProcesoElectoral1.1.1.4.2 El sistema debe permitir escoger entre los siguientes roles:

RProcesoElectoral1.1.1.4.2.1 Técnico.

RProcesoElectoral1.1.1.4.2.2 Supervisor.

RProcesoElectoral1.1.1.4.3 La lista de roles indicados en RProcesoElectoral1.1.1.4.2 podrá ser modificada por el administrador del sistema.

RProcesoElectoral1.1.2 El sistema debe almacenar en la base de datos, los de datos de creación del usuario (contraseña cifrada, nombre de usuario, tipo de usuario).

RProcesoElectoral1.1.3 Los datos solicitados en los requisitos RProcesoElectoral1.1.1.1, RProcesoElectoral1.1.1.2, RProcesoElectoral1.1.1.3, RProcesoElectoral1.1.1.4 podrán ser modificados por el administrador del sistema.

RProcesoElectoral2 El sistema debe permitir la creación de procesos electorales.

RProcesoElectoral2.1 El usuario raíz o el técnico pueden crearlos.

RProcesoElectoral2.2 El sistema debe solicitar los siguientes datos:

RProcesoElectoral2.2.1 Nombre del proceso electoral.

RProcesoElectoral2.2.1.1 Obligatorio.

RProcesoElectoral2.2.2 Fecha de inicio.

RProcesoElectoral2.2.2.1 Obligatorio.

RProcesoElectoral2.2.3 Fecha de fin.

RProcesoElectoral2.2.3.1 Obligatorio.

RProcesoElectoral2.2.4 Número de tarjetas.

RProcesoElectoral2.2.4.1 Obligatorio.

RProcesoElectoral2.2.5 Supervisor.

RProcesoElectoral2.2.5.1 Obligatorio.

RProcesoElectoral2.3 La lista de roles indicados en RProcesoElectoral2.2.1, RProcesoElectoral2.2.2, RProcesoElectoral2.2.3, RProcesoElectoral2.2.4, RProcesoElectoral2.2.5 podrá ser modificada por el administrador del sistema.

RProcesoElectoral2.4 El sistema debe permitir cargar los siguientes ficheros:

RProcesoElectoral2.4.1. Sesión.

RProcesoElectoral2.4.1.1. Obligatorio.

RProcesoElectoral2.4.2. Candidatos.

RProcesoElectoral2.4.2.1. Obligatorio.

RProcesoElectoral2.4.3. Tarjetas.

RProcesoElectoral2.4.3.1. Obligatorio.

RProcesoElectoral2.4.4. Votantes.

RProcesoElectoral2.4.4.1. Obligatorio.

RProcesoElectoral2.5 La lista de roles indicados en RProcesoElectoral2.4.1, RProcesoElectoral2.4.2, RProcesoElectoral2.4.3, RProcesoElectoral2.4.4, RProcesoElectoral2.4.5 podrá ser modificada por el administrador del sistema.

RProcesoElectoral3. El sistema debe permitir el a acceso a una ventana de verificación.

RProcesoElectoral3.1 El sistema debe permitir el acceso a los supervisores.

5.2.1.1.2 Encuesta

REncuesta1. El sistema debe efectuar el recuento del proceso electoral.

REncuesta1.1. El supervisor tiene acceso a los servicios de la encuesta.

REncuesta1.2. Tanto el usuario raíz como los técnicos no tienen acceso a los servicios de la encuesta.

REncuesta1.3 El supervisor debe seleccionar el proceso.

REncuesta1.3.1 El sistema debe controlar que el proceso haya finalizado.

REncuesta1.4 El supervisor debe iniciar el recuento.

REncuesta1.5 El supervisor puede exportar el resultado en distintos formatos.

REncuesta1.5.1 Excel

REncuesta1.5.1 PDF

REncuesta1.6 La lista descrita en REncuesta1.5 puede ser modificada por el administrador del sistema.

5.2.1.1.3 Urna

RUrna1. El sistema debe mantener la urna activa.

RUrna1.1. El supervisor tiene acceso a los servicios de la urna.

RUrna1.2. Tanto el usuario raíz como los técnicos no tienen acceso a los servicios de la urna.

RUrna1.3. El supervisor debe seleccionar una sesión.

RUrna1.4. La urna debe mostrar estadísticas.

RUrna1.4.1. Terminales autentificados

RUrna1.4.1.1. Mesa electoral

RUrna1.4.1.2. Mesa electoral auxiliar

RUrna1.4.1.3. Puesto

RUrna1.4.2. Votantes

RUrna1.4.2.1. Habilitados

RUrna1.2.2.1. No habilitados

RUrna1.5. El supervisor puede desactivar los siguientes terminales.

RUrna1.3.1 Mesa electoral

RUrna1.3.2 Mesa electoral auxiliar

RUrna1.3.3 Puesto

5.2.1.1.4 Mesa Electoral

RMesaElectoral1. El sistema debe mantener activa la mesa electoral.

RMesaElectoral1.1. El supervisor tiene acceso a los servicios de la mesa electoral.

RMesaElectoral1.2. Tanto el usuario raíz como los técnicos no tienen acceso a los servicios de la mesa electoral.

RMesaElectoral1.3 El sistema debe comprobar que se introduce un clave de sesión.

RMesaElectoral1.3.1 El sistema debe comprobar que el formato de la clave de sesión es válido.

RMesaElectoral1.3.1.1 La clave debe tener contener caracteres y/o números.

RMesaElectoral1.3.1.2 La clave debe tener longitud

RMesaElectoral1.3.2 El administrador del sistema puede cambiar las características del formato de la clave de sesión descritas en RMesaElectoral1.3.1.1 y RMesaElectoral1.3.1.2

RMesaElectoral1.4. El sistema debe comprobar que la mesa electoral pide a la urna autenticarse.

RMesaElectoral1.4.1 Si se autentica con éxito, el sistema debe mostrar la pantalla principal de la mesa electoral.

RMesaElectoral1.4.1.1 Se muestra la lista de puestos asociados con la mesa electoral.

RMesaElectoral1.4.1.2 Se puede acceder a las siguientes pantallas:

RMesaElectoral1.4.1.2.1 Actualizar votante.

RMesaElectoral1.4.1.2.2 Añadir votante.

RMesaElectoral1.4.1.2.3 Buscar votante.

RMesaElectoral1.4.2 Si no se autentica con éxito, se muestra un mensaje de error.

5.2.1.1.5 Puesto

RPuesto1. El sistema debe mantener activo el puesto de votación.

RPuesto1.1. El supervisor tiene acceso a los servicios del puesto.

RPuesto1.2. Tanto el usuario raíz como los técnicos no tienen acceso a los servicios del puesto.

RPuesto1.3. El sistema debe comprobar que se introduce un clave de sesión.

RPuesto1.3.1 El sistema debe comprobar que el formato de la clave de sesión es válido.

RPuesto1.3.1.1 La clave debe tener contener caracteres y/o números.

RPuesto1.3.1.2 La clave debe tener longitud SESION_TOKEN_LENGTH

RPuesto1.3.2 El administrador del sistema puede cambiar las características del formato de la clave de sesión descritas en RPuesto1.3.1.1 y RPuesto1.3.1.2

RPuesto1.4. El sistema debe comprobar que la mesa electoral pide a la urna autenticarse.

RPuesto1.4.1 Si se autentica con éxito, el sistema debe mostrar la pantalla principal del puesto.

RPuesto1.4.1.1 Se indica que el puesto está activado.

5.2.1.1.6 Requisitos no funcionales

RNF1 El sistema permite que sea utilizado en distintos idiomas.

RNF1.1 Inicialmente en castellano, inglés e italiano.

RNF2 El sistema garantiza la confidencialidad y seguridad de los datos de los usuarios.

RNF2.1 Inicialmente se utilizarán los algoritmos AES y RSA.

RNF3 Los votantes necesitarán tener un conocimiento mínimo de cómo funciona el proceso de votación.

5.2.1.2 Aplicación web

5.2.1.2.1 Login

RLogin1. El sistema debe permitir el que un usuario inicie sesión.

RLogin1.1 El usuario tiene que haberse registrado con anterioridad. Ver Registro.

RLogin1.2. El sistema debe solicitar los siguientes datos:

RRegistro1.2.1. Usuario.

RRegistro1.1.1.1. Obligatorio.

RRegistro1.1.2. Contraseña.

RRegistro1.1.2.1. Obligatorio.

RLogin1.3 El sistema debe comprobar que los datos del usuario y de la contraseña estén en la base de datos

RLogin1.4. El usuario debe confirmar el inicio de sesión.

RLogin1.5 El sistema debe permitir el acceso a la pantalla de registro

5.2.1.2.2 Registro

RRegistro1. El sistema debe permitir el registro de usuarios nuevos.

RRegistro1.1. El sistema debe solicitar los siguientes datos:

RRegistro1.1.1. Usuario.

RRegistro1.1.1.1. Obligatorio.

RRegistro1.1.1.2. Debe tener longitud mayor o igual que USUARIO_LENGTH

RRegistro1.1.2. Nombre.

RRegistro1.1.2.1. Obligatorio.

RRegistro1.1.3. Apellidos.

RRegistro1.1.3.1. Obligatorio.

RRegistro1.1.4. Email.

RRegistro1.1.4.1 Obligatorio.

RRegistro1.1.4. Email.

RRegistro1.1.4.1 Obligatorio.

RRegistro1.1.4.2 Debe cumplir con

RRegistro1.1.5. Contraseña.

RRegistro1.1.5.1 Obligatorio.

RRegistro1.1.5.2 Debe tener longitud mayor o igual que PASSWORD_LENGTH.

RRegistro1.1.6. Proceso electoral.

RRegistro1.1.6.1 Obligatorio.

RRegistro1.1.6.2 El sistema debe garantizar que el proceso electoral exista en la base de datos.

RRegistro1.2 El sistema debe almacenar en la base de datos, los datos del usuario, nombre, apellidos, email, contraseña y proceso electoral.

RRegistro1.3. El usuario debe confirmar el registro.

RRegistro1.4 El sistema debe permitir el acceso a la pantalla de inicio de sesión.

5.2.1.2.3 Votación

RVotación1. El sistema debe permitir que el usuario realice la votación.

RVotación1.1 El usuario debe haber realizado el proceso de inicio de sesión. Ver Login

RVotación1.2 El usuario debe escoger sus preferencias.

RVotación1.2.1 El sistema debe permitir dos mostrar distintos tipos de preguntas.

RVotación1.2.1.1 Elección única

RVotación1.2.1.2 Elección múltiple

RVotación1.3 El usuario debe confirmar la votación.

RVotación1.4 El sistema debe almacenar la votación en la base de datos.

5.2.1.3 Parametrización

SESION_TOKEN_LENGTH = 32.
USUARIO_LENGTH = 4.

PASSWORD_LENGTH = 4.

5.2.2 Identificación de Actores del Sistema

En este apartado, describiremos los actores principales que interactuarán con el sistema.

- Usuario raíz.
- Técnico.
- Supervisor.
- Votante.

5.2.3 Especificación de Casos de Uso

A continuación, se muestran los casos de usos de la aplicación. Simplemente se muestra una pequeña descripción de cada uno, se entrará en más detalle en capítulos posteriores. Ver Análisis de los Casos de Uso

5.2.3.1 Aplicación de escritorio

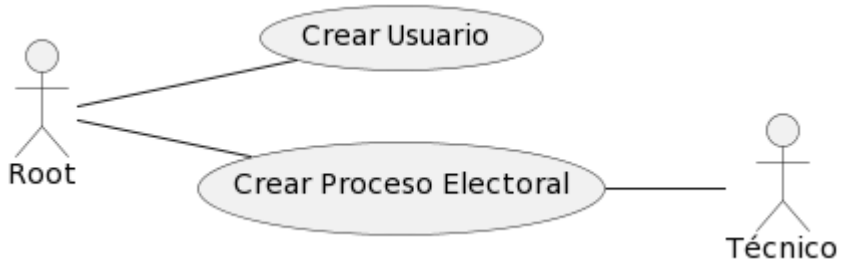

Ilustración 2. Casos de uso root

Nombre del caso de uso
Crear usuario
Descripción
El usuario raíz puede crear nuevos usuarios en el sistema que pueden tener rol de supervisor o técnico.

Tabla 22. Casos de uso root. Crear usuario

Nombre del caso de uso
Crear proceso electoral
Descripción
El usuario raíz o el técnico pueden crear nuevos procesos electorales.

Tabla 23. Casos de uso root. Crear proceso electoral

Ilustración 3. Casos de uso supervisor I

Nombre del caso de uso
Mostrar resultados
Descripción
El usuario supervisor puede mostrar los resultados del recuento.

Tabla 24. Casos de uso supervisor. Mostrar resultados

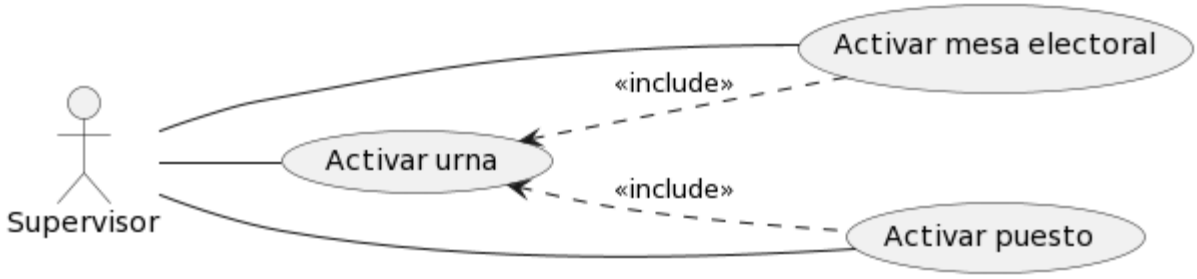

Ilustración 4. Casos de uso supervisor II

Nombre del caso de uso
Activar urna
Descripción
El usuario supervisor tiene que arrancar la urna para continuar con el proceso de votación.

Tabla 25. Casos de uso supervisor. Activar urna

Nombre del caso de uso
Activar mesa electoral
Descripción
El usuario supervisor tiene que activar la mesa electoral. Es imprescindible haber iniciado la urna.

Tabla 26. Casos de uso supervisor. Activar mesa

Nombre del caso de uso
Activar puesto
Descripción
El usuario supervisor tiene que activar el puesto de votación. Es imprescindible haber iniciado la urna.

Tabla 27. Casos de uso supervisor. Activar puesto

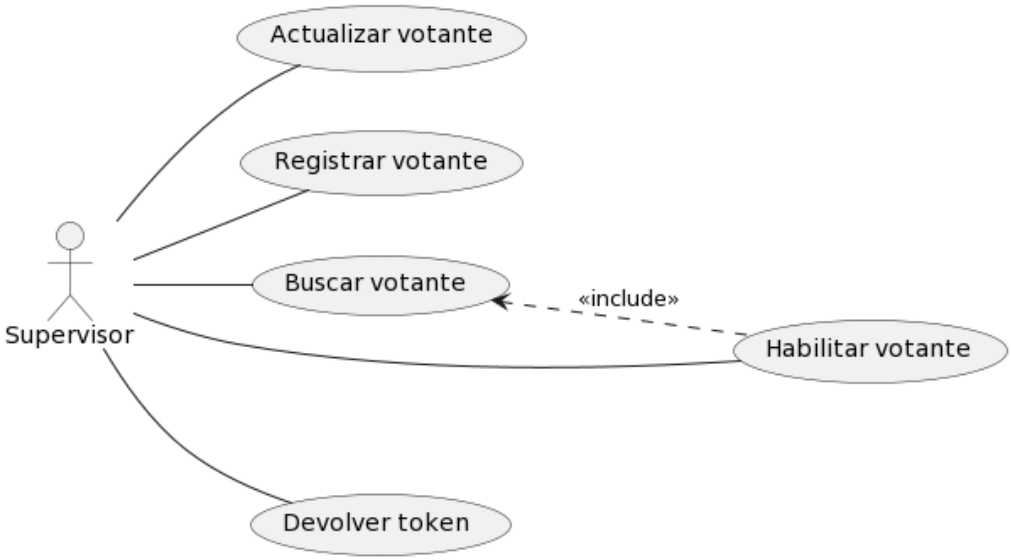

Ilustración 5. Casos de uso de supervisor III

Nombre del caso de uso
Actualizar votante
Descripción
El supervisor tiene que encargarse de la actualización de un votante.

Tabla 28. Casos de uso supervisor. Actualizar votante

Nombre del caso de uso
Registrar votante
Descripción
El supervisor tiene que encargarse del registro de un votante.

Tabla 29. Casos de uso supervisor. Registrar votante

Nombre del caso de uso
Buscar votante
Descripción
El supervisor tiene que encargarse de la búsqueda de un votante.

Tabla 30. Casos de uso supervisor. Buscar votante

Nombre del caso de uso
Habilitar votante
Descripción
El supervisor tiene que habilitar al votante para la votación.

Tabla 31. Casos de uso supervisor. Habilitar votante

Nombre del caso de uso
Devolver token
Descripción
El supervisor debe encargarse de devolver el token para confirmar la votación.

Tabla 32. Casos de uso supervisor. Gestión token

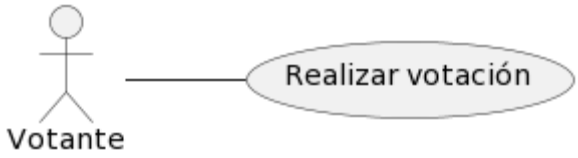

Ilustración 6. Casos de uso Votante. Realizar votación

Nombre del caso de uso
Realizar votación
Descripción
El votante realiza la votación

Tabla 33. Casos de uso Votante. Realizar votación

5.2.3.2 Aplicación web

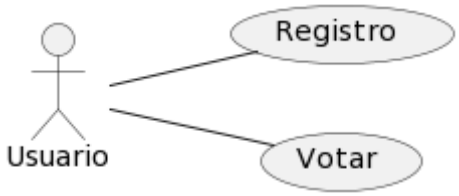

Ilustración 7. Casos de uso Votante

Nombre del caso de uso
Registro
Descripción
El usuario se podrá registrar en la aplicación web.

Ilustración 8. Casos de uso Votante. Registro

Nombre del caso de uso
Votar
Descripción
El usuario muestra sus preferencias.

Ilustración 9. Casos de uso Votante. Votar

5.3 IDENTIFICACIÓN DE SUBSISTEMAS DE ANÁLISIS

5.3.1 Aplicación de escritorio

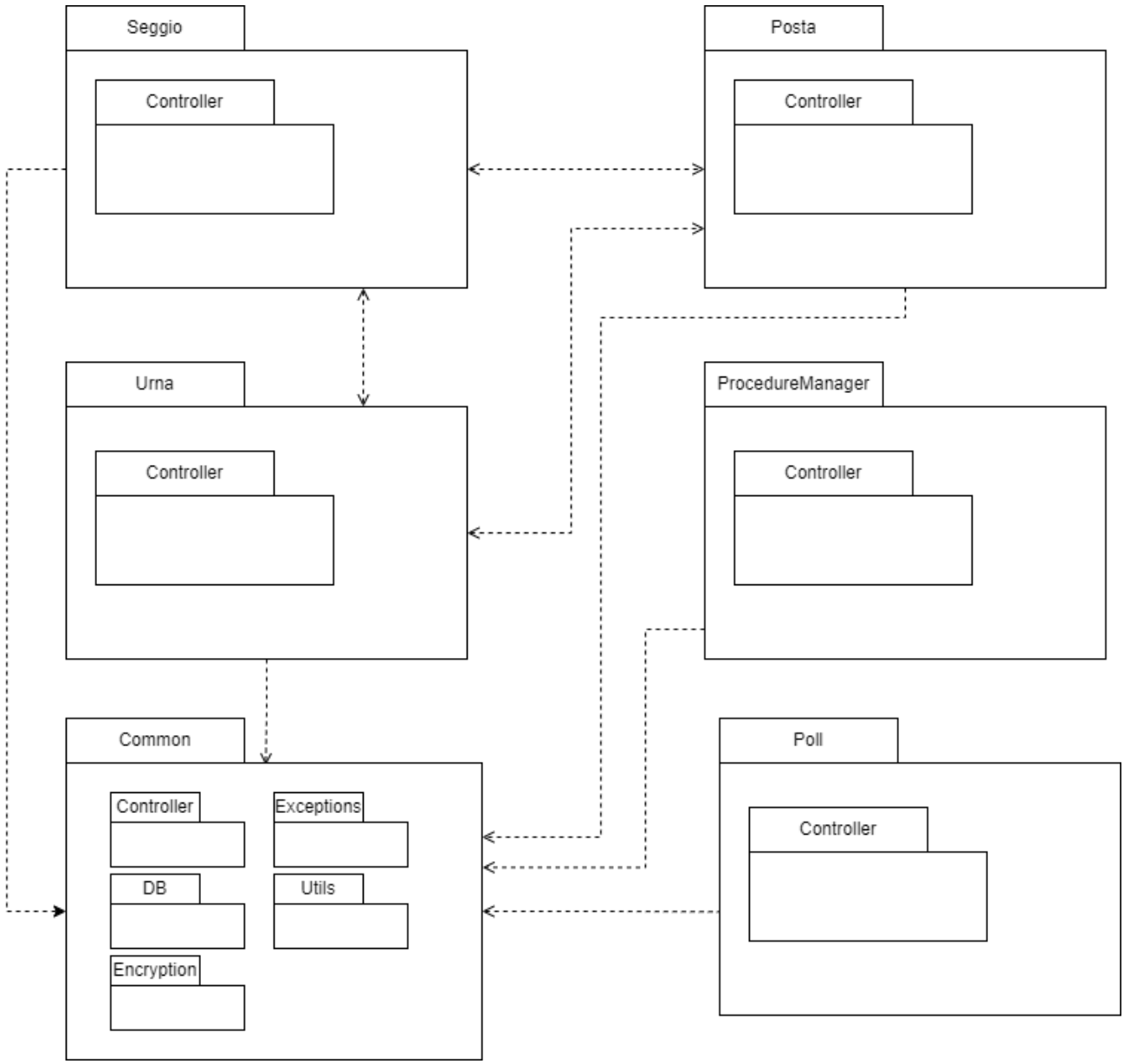

Ilustración 10. Subsistemas de análisis

Se han mantenido los nombres originales del sistema implantado. Si se tuviera alguna duda con alguno de ellos, ver Glosario.

Todos los subsistemas utilizan el Modelo Vista Controlador (MVC). Además, en el caso de Common, se encuentran paquetes para conectarse a la base de datos, para realizar tareas de encriptación, manejar excepciones u otro de utilidades.

Como cabe esperar, los paquetes Seggio, Posta, Urna, ProcedureManager y Poll tienen que estar conectados con Common.

También, debe haber conexiones entre el Seggio, Posta y Urna, pues si no estuvieran conectados, no se podría efectuar el proceso de votación.

A continuación, se mostrarán los mensajes de comunicación entre la Urna, el Seggio y el Post:

Protocol	**Descripción**
<<StationAuthenticationPhase1>>	Mensaje correspondiente a la primera fase de autenticación de una mesa electoral.
<<StationAuthenticationPhase2>>	Mensaje correspondiente a la segunda fase de autenticación de una mesa electoral.
<<SubStationAuthenticationPhase1>>	Mensaje correspondiente a la primera fase de autenticación de una mesa electoral alternativa.
<<SubStationAuthenticationPhase2>>	Mensaje correspondiente a la segunda fase de autenticación de una mesa electoral alternativa.
<<PostAuthenticationPhase1>>	Mensaje correspondiente a la primera fase de autenticación de un puesto.
<<PostAuthenticationPhase2>>	Mensaje correspondiente a la segunda fase de autenticación de un puesto.
<<validAuthentication>	Mensaje de autenticación válida.
<<authenticationFailed>>	Mensaje de autenticación fallida.
<<checkTerminalAuthentication>>	Mensaje enviado desde cualquier terminal a la urna para verificar que esta reconozca al terminal como autenticado.
<< authenticatedAck>>	Mensaje enviado desde la urna cuando esta solicita verificar autenticación de un terminal y tiene éxito.
<<authenticatedNack>>	Mensaje enviado desde la urna cuando esta solicita verificar autenticación de un terminal y no tiene éxito.
<<urnShutDown>>	Mensaje utilizado por la urna para informar de su desactivación.
<<stationShutDown>>	Mensaje utilizado por la mesa electoral para informar de su desactivación.
<<subStationShutDown>>	Mensaje utilizado por la mesa electoral alternativa para informar de su desactivación.
<<postShutDown>>	Mensaje utilizado por el puesto para informar de su desactivación.

<<retrieveStatePost>>	Mensaje enviado desde la mesa electoral a la urna para conocer el estado de todos los puestos asociados a él.
<<informStatePost>>	Mensaje enviado desde los puestos a la mesa electoral, comunicando el estado actual de cada uno de los puestos.
<<checkUnreachablePost>>	Mensaje enviado desde la mesa electoral para comprobar si los puestos asociados son alcanzables.
<<resetPostReq>>	Mensaje enviado desde la mesa electoral uno de los puestos para solicitar el reinicio.
<<resetPostGranted>>	Mensaje enviado desde el puesto a la mesa electoral. Informa que se produce el reinicio y que el puesto vuelve al estado ACTIVO, eliminado cualquier asociación.
<<resetPostDenied>>	Mensaje enviado desde el puesto a la mesa electoral. Informa que no se ha producido el reinicio. Suele suceder cuando la estación está en estados como NO ACTIVO o REINICIABLE
<<associationReq>>	Mensaje utilizado por la mesa electoral para solicitar a los puestos una nueva asociación. La asociación permite ocupar un puesto y permitir la votación.
<<associationAck>>	Mensaje de respuesta de éxito enviado desde el puesto a la mesa electoral.
<<associationNack>>	Mensaje de respuesta de fracaso enviado desde el puesto a la mesa electoral
<<postEndVoteReq>>	Mensaje enviado desde la mesa electoral al puesto para confirmar la operación de votación.
<<postEndVoteAck>>	Mensaje de respuesta del puesto a la mesa electoral, para confirmar la destrucción de la asociación y su retorno a estado ACTIVO.
<<postEndVoteNack>>	Mensaje de respuesta del puesto a la mesa electoral, para informar que no se ha podido destruir la asociación.
<<nonceReq>>	Mensaje utilizado por el puesto para solicitar a la urna, al final de la fase de votación, generar un cierto número de nonce dependiendo del número de preferencias del votante.
<<nonceAck>>	Mensaje de respuesta enviado desde la urna al puesto para confirmar el envío del nonce.
<<nonceNack>>	Mensaje de respuesta enviado desde la urna al puesto para señalar que ha habido algún error durante la generación del nonce.

<<tokensAck>>	Mensaje de respuesta enviado desde la urna a la mesa electoral para señalar que la devolución de tokens se ha hecho correctamente.
<<tokensNack>>	Mensaje de respuesta enviado desde la urna a la mesa electoral para señalar que la devolución de tokens no se ha hecho correctamente.
<<sendVoteToStation>>	Mensaje enviado por el puesto a la mesa electoral para enviar el paquete de votación.
<<sendVoteToUrn>>	Mensaje enviado por la mesa electoral a la urna para enviar el paquete de votación. Se debe haber recibido antes <<sendVoteToStation>>
<<votesReceivedAck>>	Mensaje utilizado por la mesa electoral y la urna para confirmar la recepción de los votos.
<<votesReceivedNack>>	Mensaje utilizado por la mesa electoral y la urna para informar de un error en la recepción de los votos.
<<registerNewUserReq>>	Mensaje utilizado por la mesa electoral para solicitar a la urna el registro de un nuevo usuario en el proceso electoral actual.
<<registerNewUserAck>>	Mensaje enviado desde la urna a la mesa electoral para confirmar el registro de un nuevo usuario en la base de datos.
<<registerNewUserNack>>	Mensaje enviado desde la urna a la mesa electoral para informar de errores en el registro de un nuevo usuario en la base de datos.
<<updateExistingUserReq>>	Mensaje utilizado por la mesa electoral para solicitar a la urna la actualización de un usuario en el proceso electoral actual.
<<updateExistingUserAck>>	Mensaje enviado desde la urna a la mesa electoral para confirmar la actualización de un usuario en la base de datos.
<<updateExistingUserNack>>	Mensaje enviado desde la urna a la mesa electoral para informar de errores en la actualización de un usuario en la base de datos.
<<changePostState>>	Mensaje utilizado por la mesa electoral para comunicar a un puesto su nuevo estado.
<<updateSubStation>>	Mensaje utilizado por la mesa electoral para comunicarse con la mesa electoral alternativa e informarle el nuevo estado de los puestos.
<<searchPersonReq>>	Mensaje utilizado por la mesa electoral para enviar una solicitud de búsqueda de votantes a la urna.
<<getTokensReq>>	Mensaje para comprobar si el token es de los que han sido enviados por email a un votante a

	la hora de devolver el token en la mesa electoral.
<<searchPersonSubStationReq>>	Mensaje utilizado por la mesa electoral alternativa para enviar una solicitud de búsqueda de los votantes.
<<searchPersonAck>>	Mensaje enviado desde la urna a la mesa electoral para confirmar la búsqueda de votantes en la base de datos y el envío de estos.
<<searchPersonNack>>	Mensaje enviado desde la urna a la mesa electoral para informar de errores en la búsqueda de votantes en la base de datos.
<<success>>	Mensaje genérico de éxito.
<<error>>	Mensaje genérico para informar de un error.

Tabla 34. Mensaje protocolos

5.3.2 Aplicación web

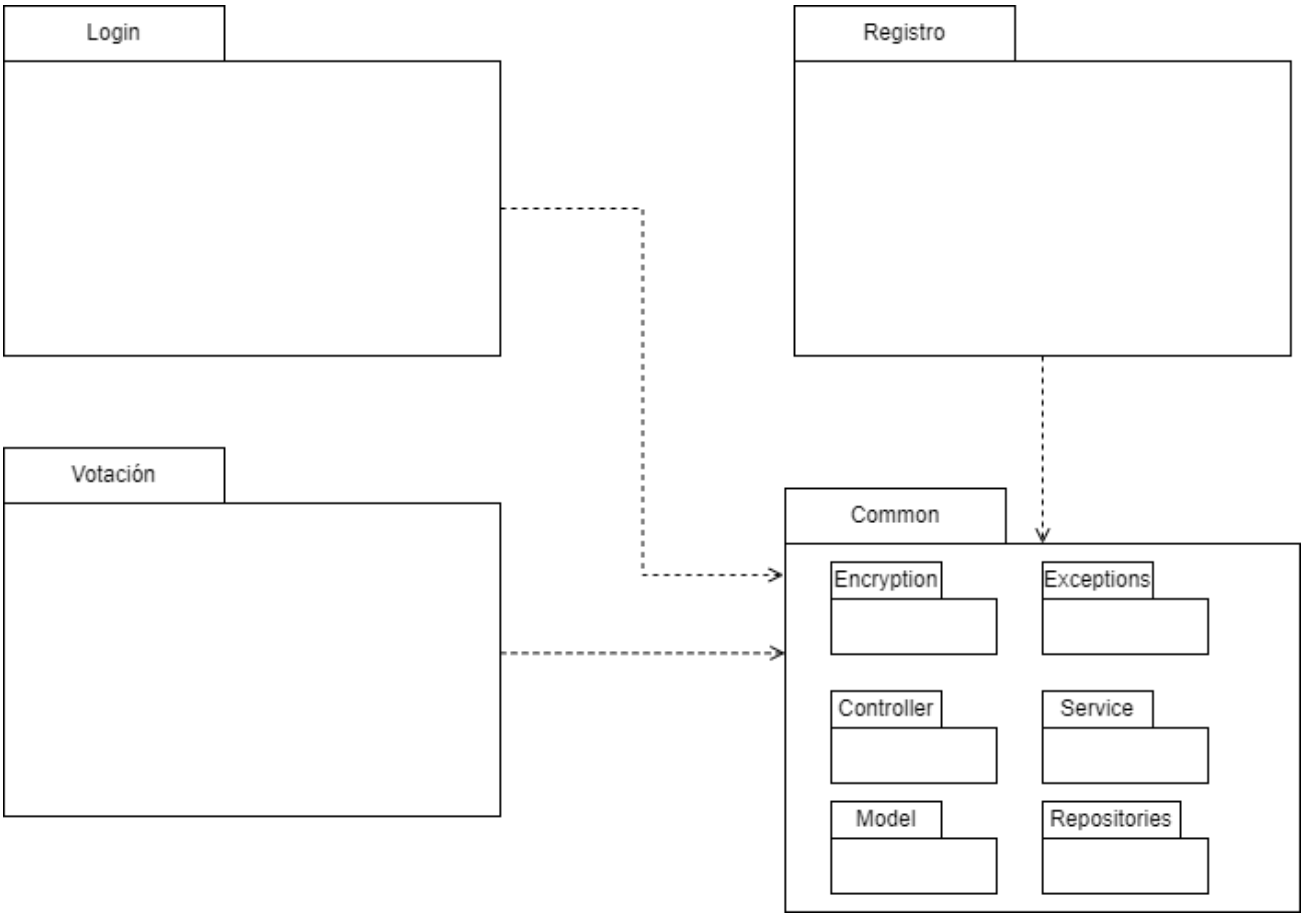

Ilustración 11. Subsistemas de Análisis Web

Los subsistemas Login, Registro y Votación realizan tareas de encriptación, manejan excepciones, y utilizan controladores, distintos servicios, modelos y repositorios.

5.4 ANÁLISIS DE LOS CASOS DE USO

5.4.1 Aplicación de escritorio

5.4.1.1 Crear usuario

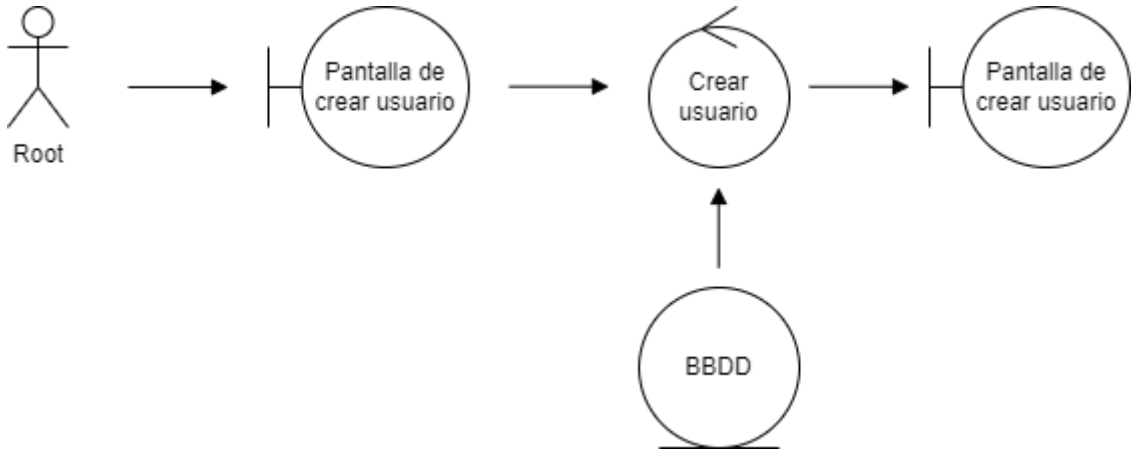

Ilustración 12. Análisis casos de uso. Crear usuario

Caso de Uso 1. Crear usuario	
Precondiciones	El usuario no debe estar registrado en la base de datos
Actores	Root y usuario a crear
Descripción	El usuario raíz puede crear nuevos usuarios en el sistema que pueden tener rol de supervisor o técnico.
Postcondiciones	
Excepciones	El nombre de usuario ya existe en la base de datos.

Tabla 35. Análisis casos de uso. Crear usuario

5.4.1.2 Crear proceso electoral

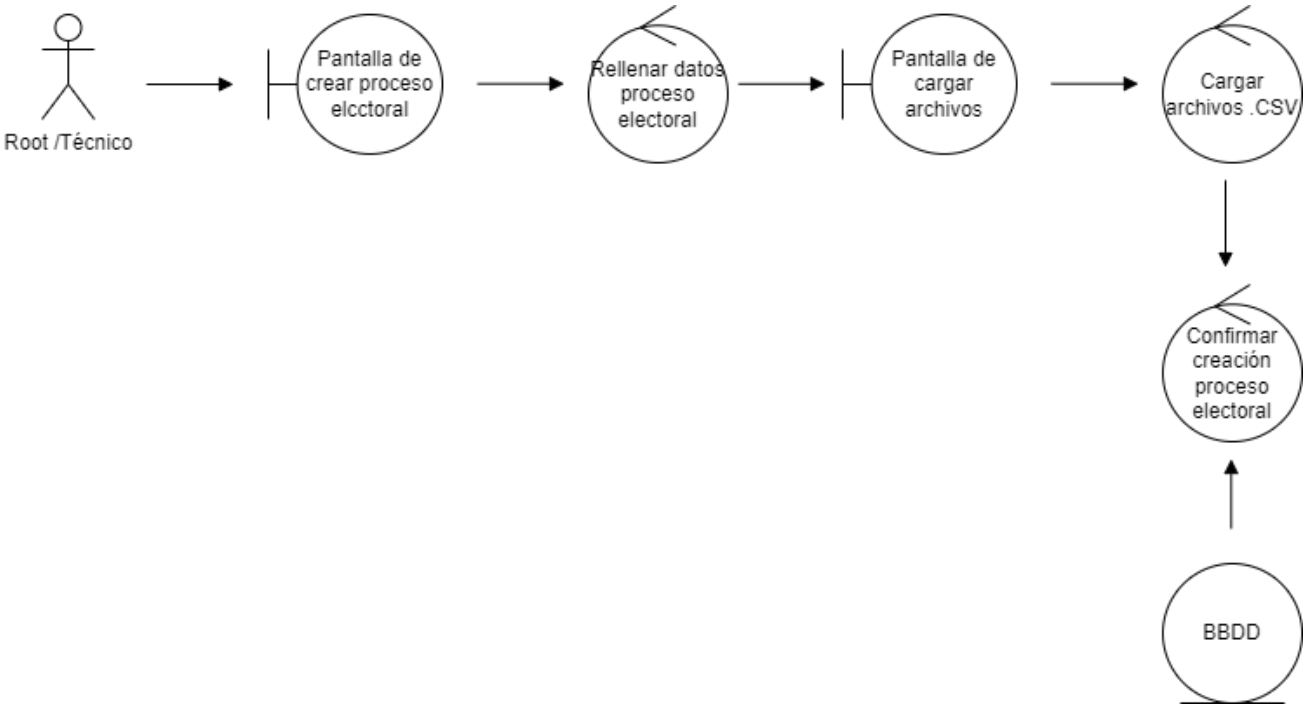

Ilustración 13. Análisis casos de uso. Crear proceso electoral

Caso de Uso 2. Crear proceso electoral	
Precondiciones	No puede haber un proceso electoral con el mismo identificador en la BD.
Actores	Root o Técnico
Descripción	El usuario raíz o el técnico pueden crear nuevos procesos electorales.
Postcondiciones	
Excepciones	La fecha de inicio del procedimiento sea posterior a la fecha de finalización.

Tabla 36. Análisis casos de uso. Crear proceso electoral

5.4.1.3 Mostrar resultados

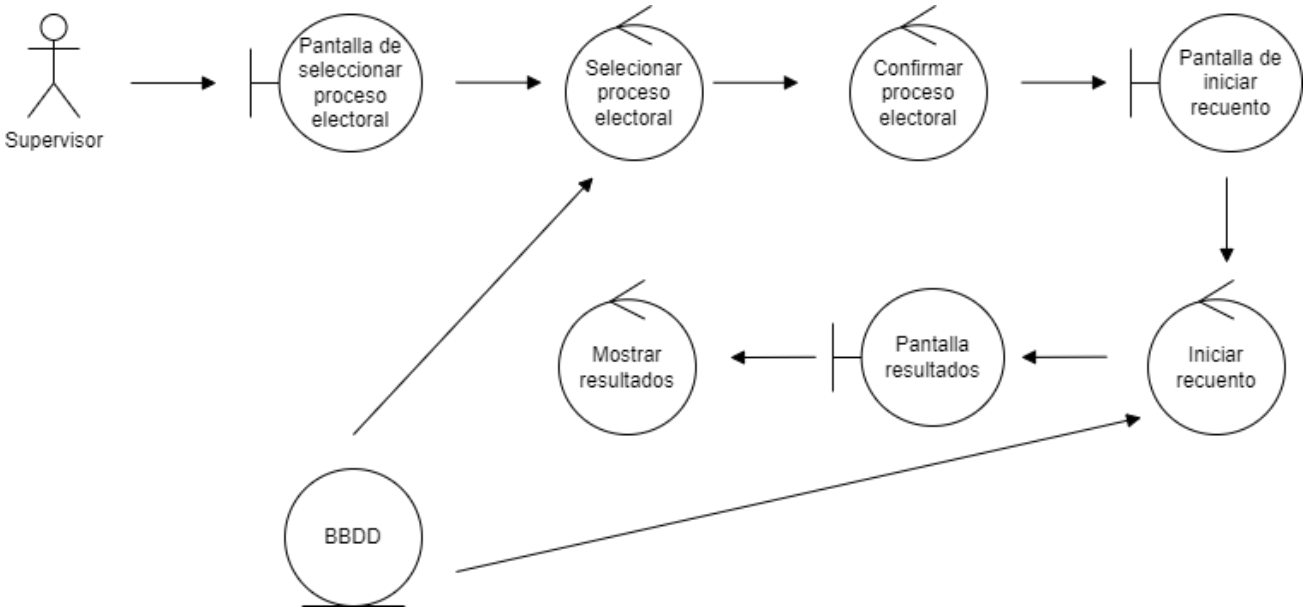

Ilustración 14. Análisis casos de uso. Mostrar resultados

Caso de Uso 3. Mostrar resultados	
Precondiciones	El proceso electoral tiene que haber finalizado.
Actores	Supervisor
Descripción	El usuario supervisor puede mostrar los resultados del recuento. Para ello se debe elegir el proceso electoral deseado. Los resultados electorales se pueden ver tanto en la pantalla de resultados como en un archivo .pdf o .csv
Postcondiciones	
Excepciones	• No se haya seleccionado ningún proceso electoral antes de confirmar. • El proceso electoral no haya finalizado.

Tabla 37. Análisis casos de uso. Mostrar resultados

5.4.1.4 Activar urna

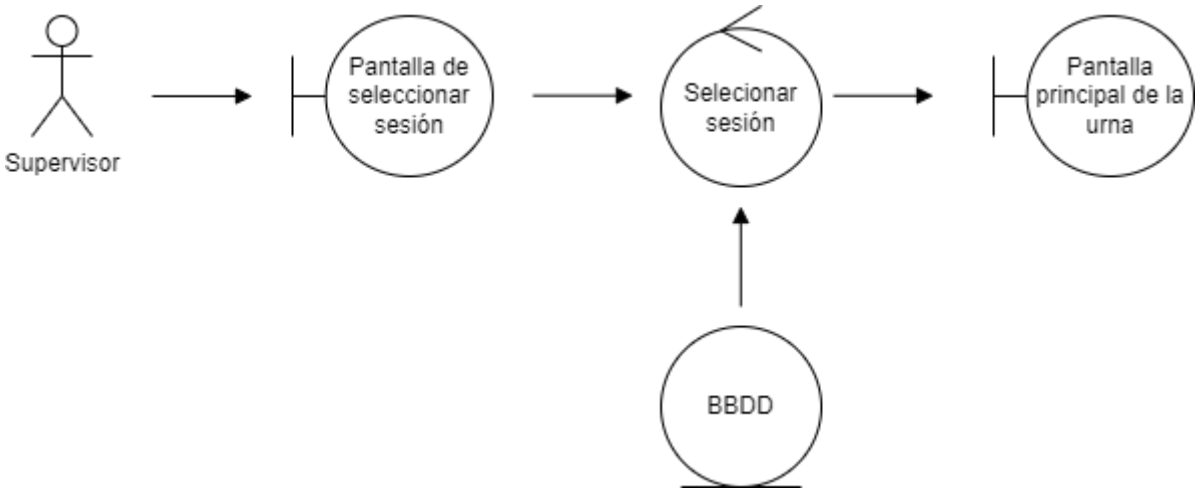

Ilustración 15. Análisis casos de uso. Activar urna

Caso de Uso 4. Activar urna	
Precondiciones	El supervisor debe tener asignado el proceso electoral.
Actores	Supervisor
Descripción	El usuario supervisor tiene que arrancar la urna para continuar con el proceso de votación.
Postcondiciones	
Excepciones	

Tabla 38. Análisis casos de uso. Activar urna

5.4.1.5 Activar mesa electoral

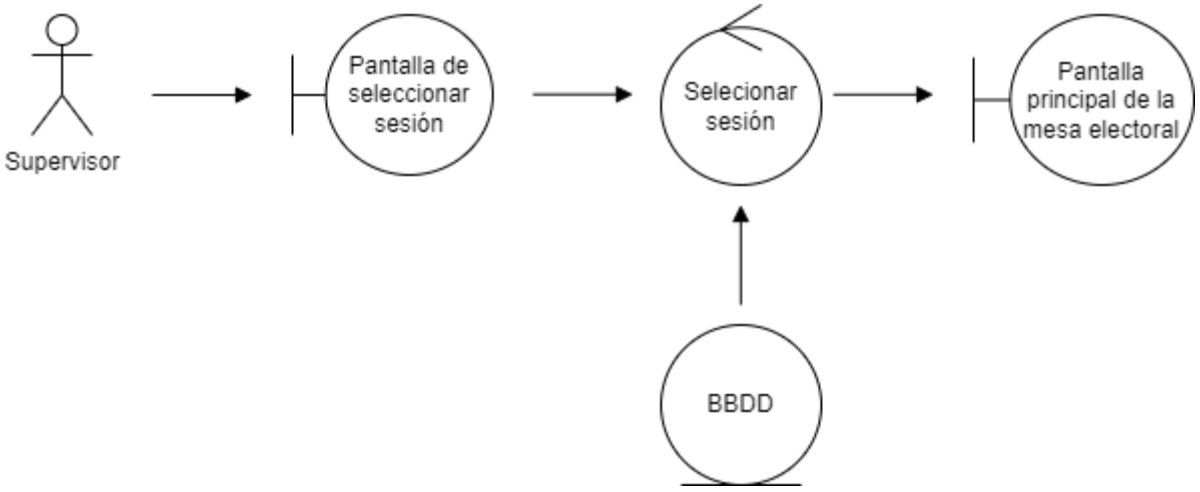

Ilustración 16. Análisis Casos de Uso. Activar mesa electoral

Caso de Uso 5. Activar mesa electoral	
Precondiciones	Es condición indispensable haber iniciado la urna antes.
Actores	Supervisor
Descripción	El usuario supervisor tiene que activar la mesa electoral.
Postcondiciones	
Excepciones	No se encuentra la clave de sesión.

Ilustración 17. Análisis Casos de Uso. Activar mesa electoral

5.4.1.6 Activar puesto

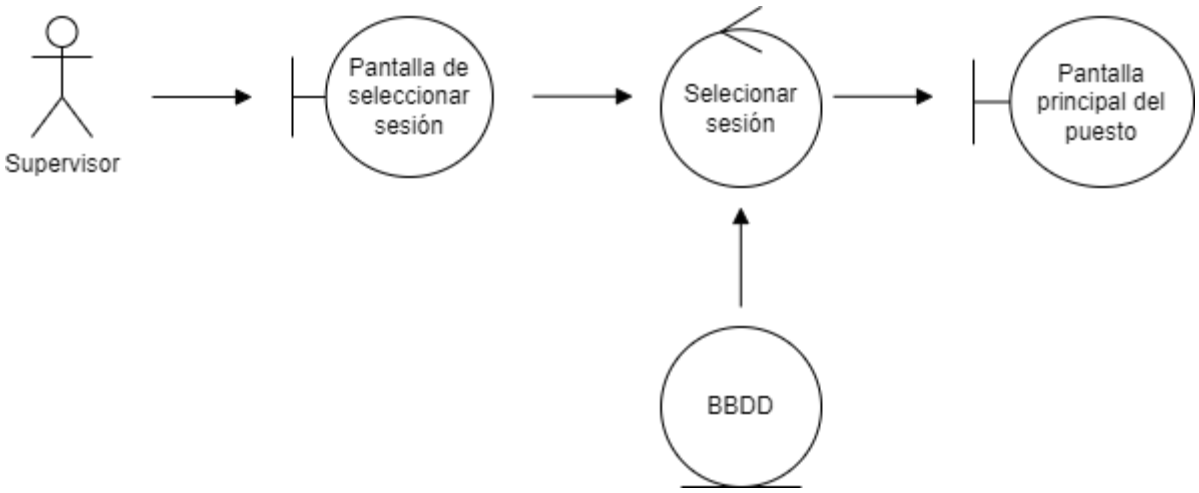

Ilustración 18. Análisis Casos de Uso. Activar puesto

Caso de Uso 6. Activar puesto	
Precondiciones	Es condición indispensable haber iniciado la urna antes.
Actores	Supervisor
Descripción	El usuario supervisor tiene que activar el puesto de votación.
Postcondiciones	
Excepciones	No se encuentra la clave de sesión.

Ilustración 19. Análisis Casos de Uso. Activar puesto

5.4.1.7 Actualizar votante

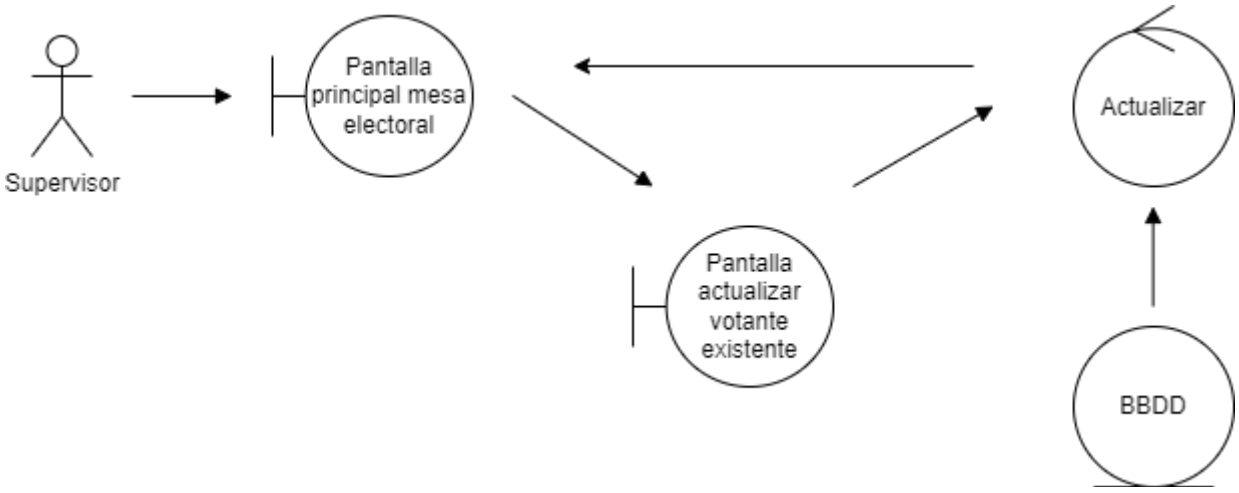

Ilustración 20. Análisis Casos de Uso. Actualizar votante

Caso de Uso 7. Actualizar votante	
Precondiciones	El votante debe existir en la BD.
Actores	Supervisor
Descripción	El usuario supervisor tiene que encargarse de actualizar votante.
Postcondiciones	
Excepciones	El votante no existe en la BD.

Tabla 39. Análisis Casos de Uso. Actualizar votante

5.4.1.8 Registrar votante

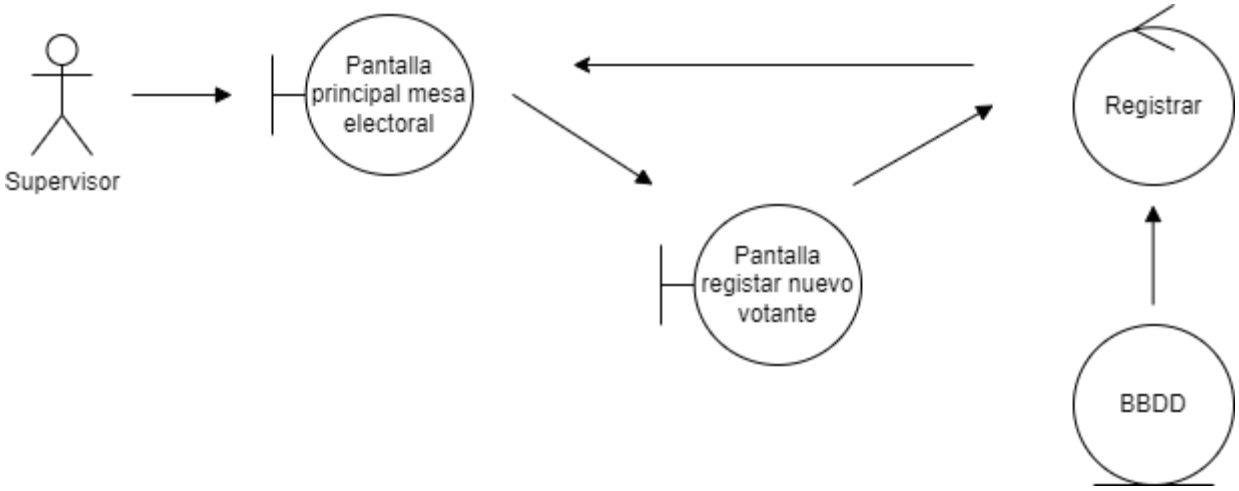

Ilustración 21. Análisis Casos de Uso. Registrar votante

Caso de Uso 8. Registrar votante	
Precondiciones	El votante no debe existir en la BD.
Actores	Supervisor
Descripción	El usuario supervisor tiene que encargarse del registro de nuevos votantes.
Postcondiciones	
Excepciones	El votante ya existe en la BD.

Tabla 40. Análisis Casos de Uso. Registrar votante

5.4.1.9 Buscar votante

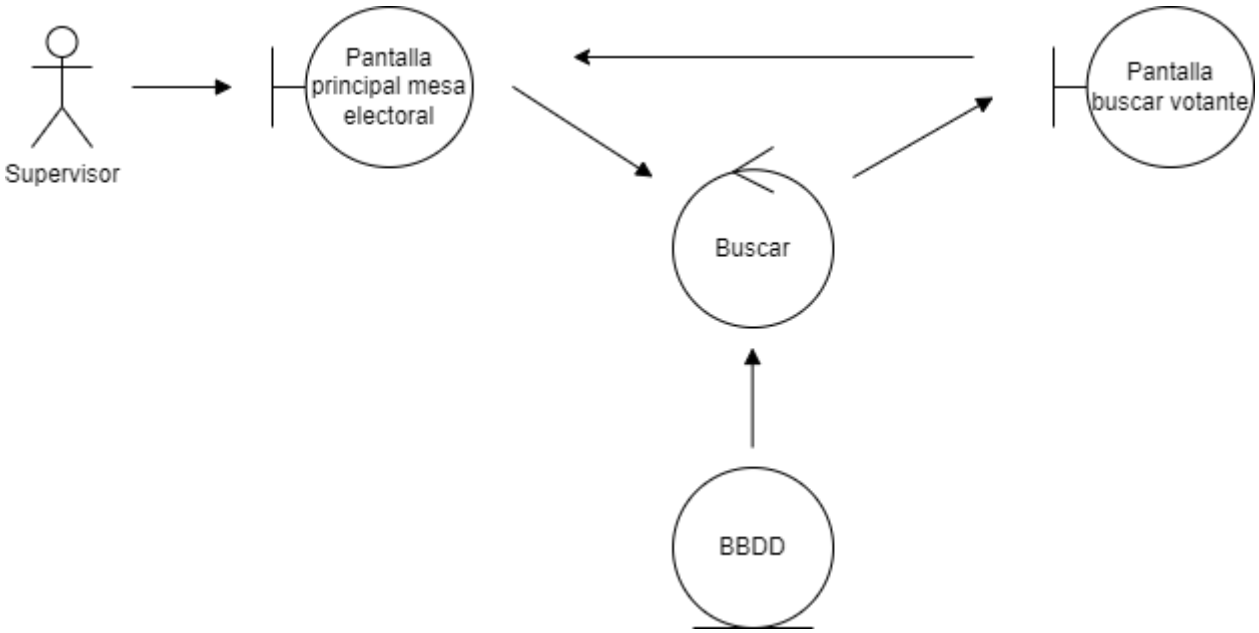

Ilustración 22. Análisis Casos de Uso. Buscar votante

Caso de Uso 9. Buscar votante	
Precondiciones	El votante debe existir en la BD.
Actores	Supervisor
Descripción	El usuario supervisor tiene que encargarse de buscar un votante.
Postcondiciones	
Excepciones	El votante no existe en la BD.

Tabla 41. Análisis Casos de Uso. Buscar votante

5.4.1.10 Habilitar votante

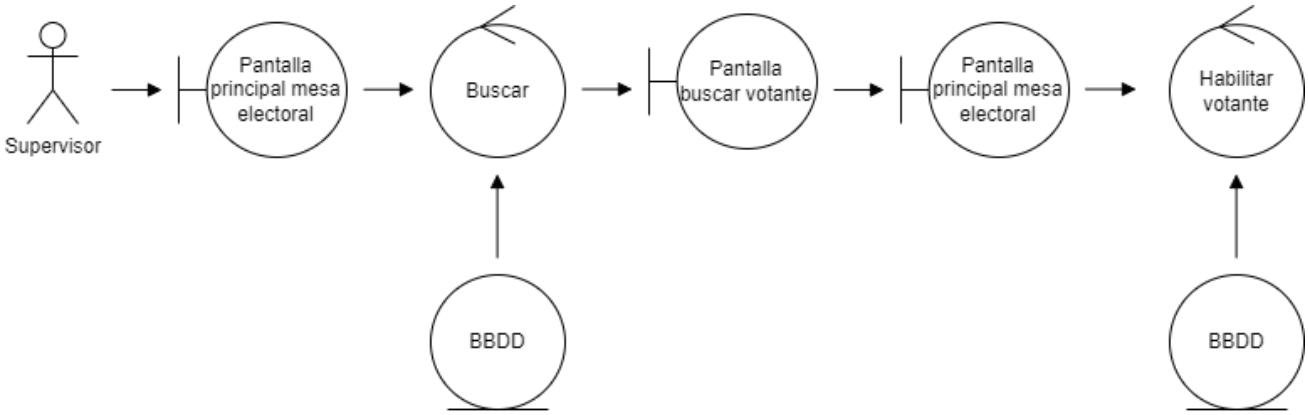

Ilustración 23. Análisis Casos de Uso. Habilitar votante

Caso de Uso 10. Habilitar votante	
Precondiciones	El votante debe existir en la BD.
Actores	Supervisor
Descripción	El usuario supervisor tiene que encargarse de habilitar a un votante existente para que pueda votar. 1. Se tiene que buscar. 2. Se tiene que habilitar. El supervisor genera un token para el usuario.
Postcondiciones	
Excepciones	El votante no existe en la BD.

Tabla 42. Análisis Casos de Uso. Habilitar votante

5.4.1.11 Devolver token

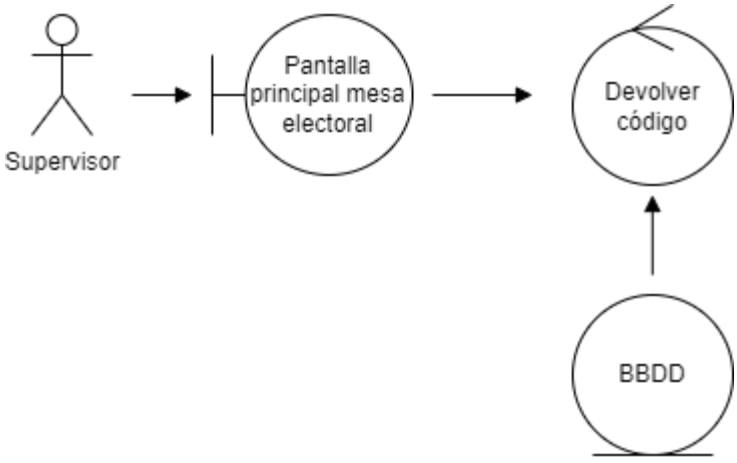

Ilustración 24. Análisis Casos de Uso. Devolver token

Caso de Uso 11. Devolver token	
Precondiciones	El votante tiene que haber acabado de votar y entregar el token al supervisor.
Actores	Supervisor
Descripción	El supervisor devuelve el token para confirmar el envío del voto
Postcondiciones	
Excepciones	Devolver el token cuando el puesto tenga un estado distinto a VOTO_ENVIADO

Tabla 43. Análisis Casos de Uso. Devolver token

5.4.1.12 Realizar votación

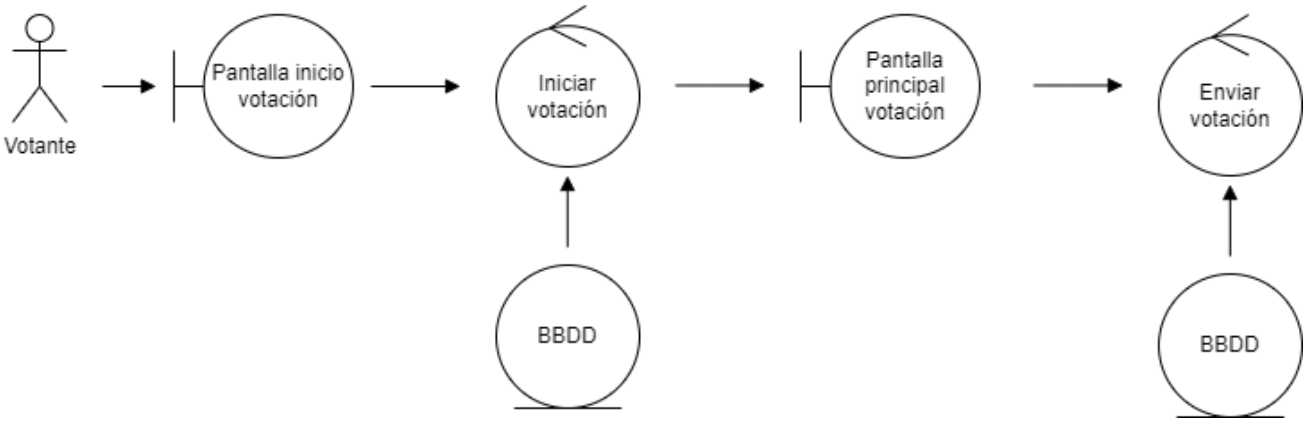

Ilustración 25. Análisis Casos de Uso. Realizar votación

Caso de Uso 12. Realizar votación	
Precondiciones	El votante debe estar habilitado.
Actores	Votante
Descripción	El votante realiza la votación. Tiene que iniciar la votación y a continuación, se muestran las pantallas de votación donde debe mostrar sus preferencias.
Postcondiciones	
Excepciones	

Tabla 44. Análisis Casos de Uso. Realizar votación

5.4.2 Aplicación web

5.4.2.1 Registro

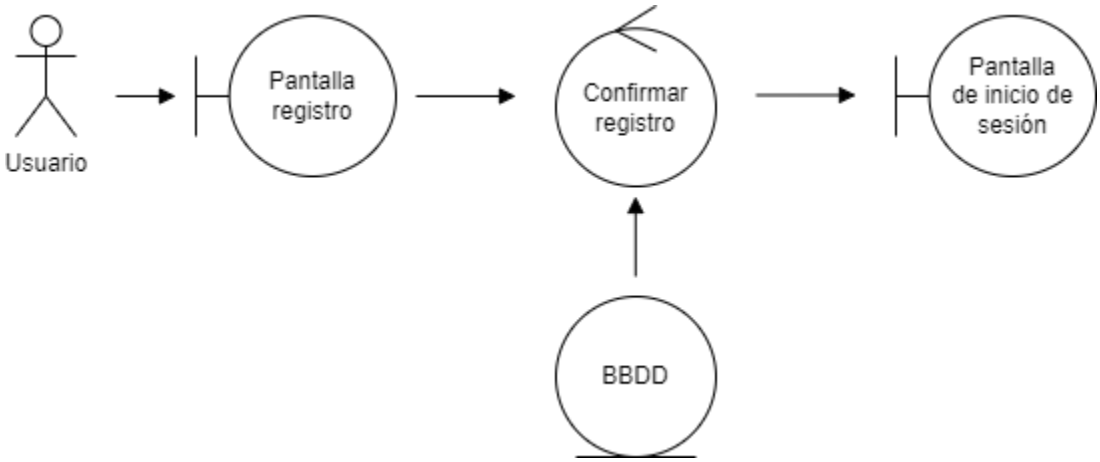

Ilustración 26. Análisis Casos de Uso. Registro web

Caso de Uso 13. Registro	
Precondiciones	El proceso electoral debe existir. El usuario no debe estar registrado en la base de datos.
Actores	Usuario
Descripción	El usuario se podrá registrar en la aplicación web.
Postcondiciones	
Excepciones	El proceso electoral no existe El usuario ya existe en la base de datos.

Tabla 45. Análisis Casos de Uso. Registro web

5.4.2.2 Votar

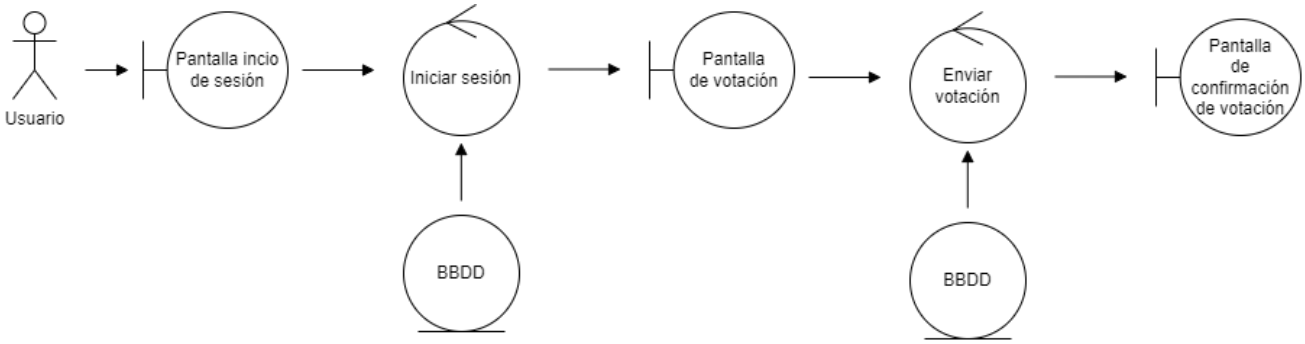

Ilustración 27. Análisis Casos de Uso. Votar web

Caso de Uso 13. Votar	
Precondiciones	El usuario debe existir.
Actores	Usuario
Descripción	El usuario muestra sus preferencias.
Postcondiciones	
Excepciones	El usuario ya ha votado. El proceso electoral está cerrado. El usuario escoger más preferencias para una pregunta.

Tabla 46. Análisis Casos de Uso. Votar web

5.5 ANÁLISIS DE CLASES

5.5.1 Aplicación de escritorio

5.5.1.1 Diagrama de clases

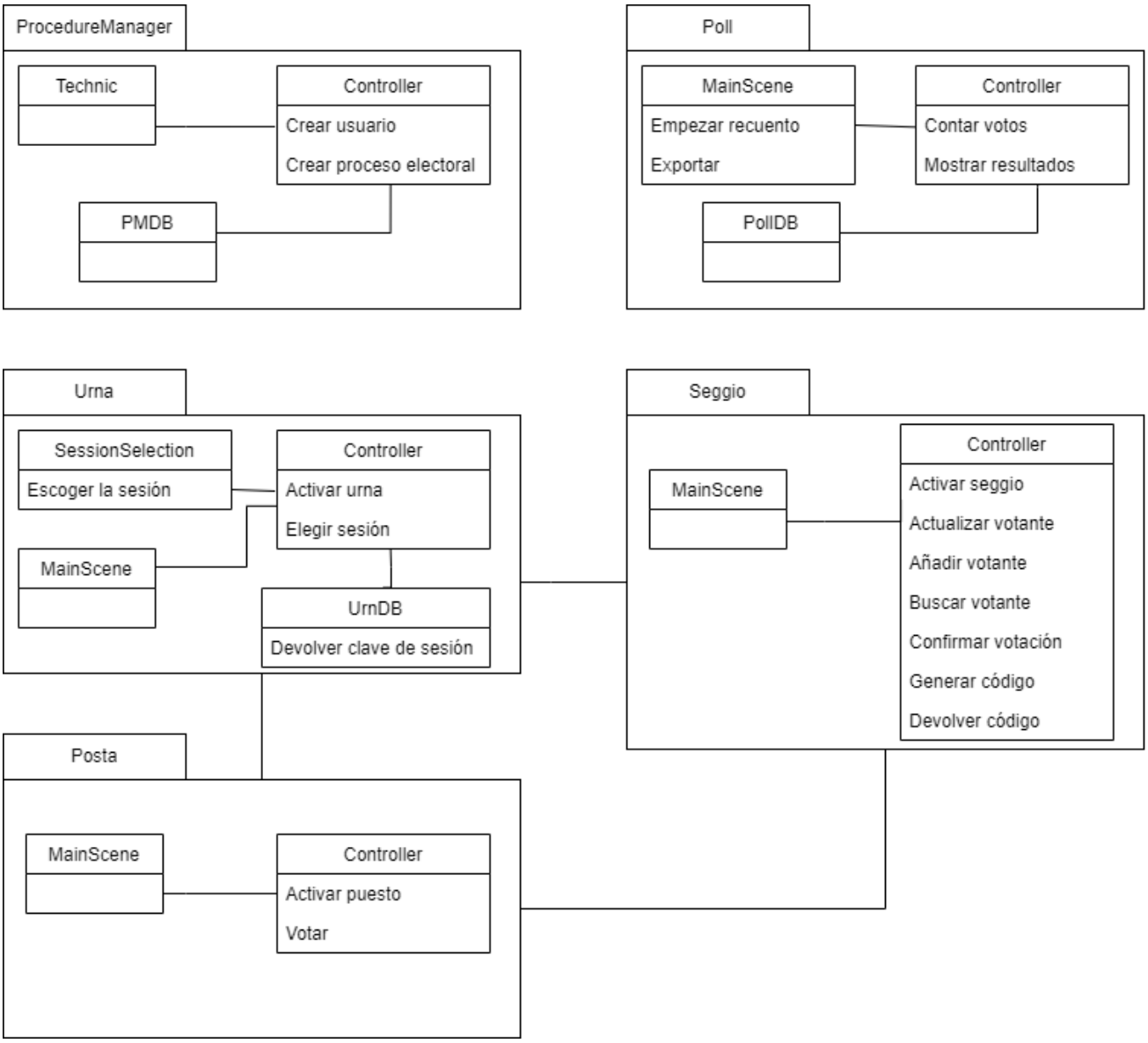

Ilustración 28. Análisis de clases. Diagrama de clases

5.5.1.2 Descripción de las clases

5.5.1.2.1 Proceso electoral

Nombre de la clase
Technic
Descripción
Pantalla para crear usuarios y procesos electorales.
Responsabilidades
Insertar en la base de datos los nuevos usuarios y procesos electorales.
Atributos propuestos
Métodos propuestos

Tabla 47. Análisis de clases. Technic

Nombre de la clase
PMDB
Descripción
Base de datos de ProcedureManager
Responsabilidades
Insertar en la base de datos los nuevos usuarios y procesos electorales.
Atributos propuestos
Métodos propuestos

Tabla 48. Análisis de clases. PMDB

Nombre de la clase
Controller
Descripción
Controller de ProcedureManager
Responsabilidades
Crear usuarios Crear procesos electorales
Atributos propuestos
Métodos propuestos

Tabla 49. Análisis de clases. Controller_PM

5.5.1.2.2 Encuesta

Nombre de la clase
MainScene
Descripción
La vista que muestra los resultados del proceso electoral.
Responsabilidades
Iniciar el recuento Exportar los resultados, dos formatos .pdf y .csv
Atributos propuestos
Métodos propuestos

Tabla 50. Análisis de clases. MainScene_Encuesta

Nombre de la clase
PollDB
Descripción
Base de datos de Poll
Responsabilidades
Mostrar los resultados del proceso electoral
Atributos propuestos
Métodos propuestos

Tabla 51. Análisis de clases. PollDB

Nombre de la clase
Controller
Descripción
Controlador de Poll
Responsabilidades
Se encarga de hacer el recuento de los votos y mostrar los resultados.
Atributos propuestos
Métodos propuestos

Tabla 52. Análisis de clases. Controller_Encuesta

5.5.1.2.3 Urna

Nombre de la clase
SessionSelection
Descripción
Pantalla de selección de sesión
Responsabilidades
Escoger la sesión
Atributos propuestos
Métodos propuestos

Tabla 53. Análisis de clases. SessionSelection

Nombre de la clase
MainScene
Descripción
Pantalla principal de la urna donde se ven los mensajes enviados entre terminales.
Responsabilidades
Mostrar mensajes entre terminales
Atributos propuestos
Métodos propuestos

Tabla 54. Análisis de clases. MainScene_Urna

Nombre de la clase
UrnaDB
Descripción
Base de datos de Urna
Responsabilidades
Devuelve clave de sesión de un terminal.
Atributos propuestos
Métodos propuestos

Tabla 55. Análisis de clases. UrnaDB

Nombre de la clase
Controller
Descripción
Controlador de la urna
Responsabilidades
Se encarga de activar la urna y elegir la sesión deseada.
Atributos propuestos
Métodos propuestos

Tabla 56. Análisis de clases. Controller_Urna

5.5.1.2.4 Mesa electoral

Nombre de la clase
MainScene
Descripción
Vista de la mesa electoral
Responsabilidades
Atributos propuestos
Métodos propuestos

Tabla 57. Análisis de clases. MainScene_Mesa

Nombre de la clase
Controller
Descripción
Controlador de la mesa electoral
Responsabilidades
Se encarga de activar el Seggio, actualizar votante, añadir votante, buscar votante, confirmar la votación, generar código y devolver código.
Atributos propuestos
Métodos propuestos

Tabla 58. Análisis de clases. Controller_Mesa

5.5.1.2.5 Puesto de votación

Nombre de la clase
MainScene
Descripción

Vista del puesto de votación
Responsabilidades
Atributos propuestos
Métodos propuestos

Tabla 59. Análisis de clases. MainScene_Puesto de votación

Nombre de la clase
Controller
Descripción
Controlador del puesto de votación.
Responsabilidades
Activar puesto y votar
Atributos propuestos
Métodos propuestos

Tabla 60. Análisis de clases. MainScene_Controller

5.5.2 Aplicación web

5.5.2.1 Diagrama de clases

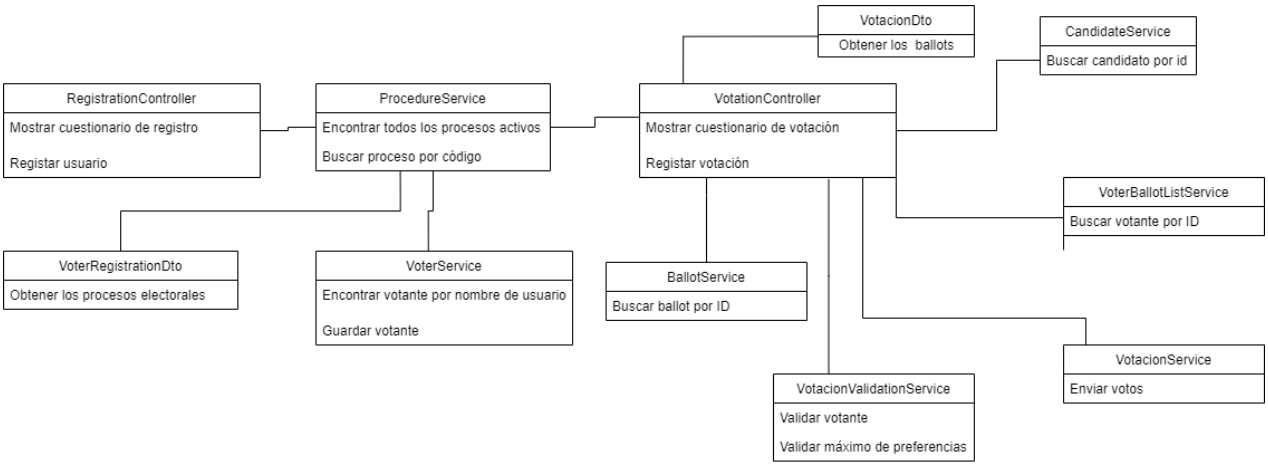

Ilustración 29. Diagrama de clases. App web

5.5.2.2 Descripción de las clases

Nombre de la clase
RegistrationController
Descripción
Controlador encargado del registro de usuarios.
Responsabilidades
Mostrar cuestionario de registro y registrar el usuario
Atributos propuestos
Métodos propuestos

Tabla 61. Análisis de clases. RegistrationController

Nombre de la clase
ProcedureService
Descripción
Servicio del proceso electoral
Responsabilidades
Encontrar todos los procesos activos y buscar procesos por código
Atributos propuestos
Métodos propuestos

Tabla 62. Análisis de clases. ProcedureService

Nombre de la clase

VoterRegistrationDto
Descripción
Dto de Registro de votantes
Responsabilidades
Obtener los procesos electorales
Atributos propuestos
Métodos propuestos

Tabla 63. Análisis de clases. VoterRegistrationDto

Nombre de la clase
VoterService
Descripción
Servicio de votante
Responsabilidades
Encontrar votante por nombre de usuario y guardar votante.
Atributos propuestos
Métodos propuestos

Tabla 64. Análisis de clases. VoterService

Nombre de la clase
VotationController
Descripción
Controlador de votación
Responsabilidades
Mostrar cuestionarios de votación y registrar votación.
Atributos propuestos
Métodos propuestos

Tabla 65. Análisis de clases. VotationController

Nombre de la clase
BallotService
Descripción
Servicio de ballots
Responsabilidades
Buscar ballots por identificador.
Atributos propuestos
Métodos propuestos

Tabla 66. Análisis de clases. BallotService

Nombre de la clase
VotationValidationService
Descripción
Servicio de validación de votación.
Responsabilidades
Validar votante y validar máximo de preferencias.
Atributos propuestos
Métodos propuestos

Tabla 67. Análisis de clases. VotationValidationService

Nombre de la clase
VotationService
Descripción
Servicio de votación.
Responsabilidades
Enviar votos.
Atributos propuestos
Métodos propuestos

Tabla 68. Análisis de clases. VotationService

Nombre de la clase
VoterBallotListService
Descripción
Servicio de lista de ballots.
Responsabilidades
Buscar votante por identificador.
Atributos propuestos
Métodos propuestos

Tabla 69. Análisis de clases. VoterBallotListService

Nombre de la clase
CandidateService
Descripción
Servicio de candidatos
Responsabilidades
Buscar candidato por identificador.
Atributos propuestos
Métodos propuestos

Tabla 70. Análisis de clases. CandidateService

Nombre de la clase
VotationDto
Descripción
Dto de votación
Responsabilidades
Obtener los ballots.
Atributos propuestos
Métodos propuestos

Tabla 71. Análisis de clases. VotationDto

5.6 DEFINICIÓN DE INTERFACES DE USUARIO

5.6.1 Descripción de la Interfaz

5.6.1.1 Aplicación de escritorio

5.6.1.1.1 Login

Se muestra la pantalla de login típica para los paquetes: ProcedureManager, Poll y Urna.

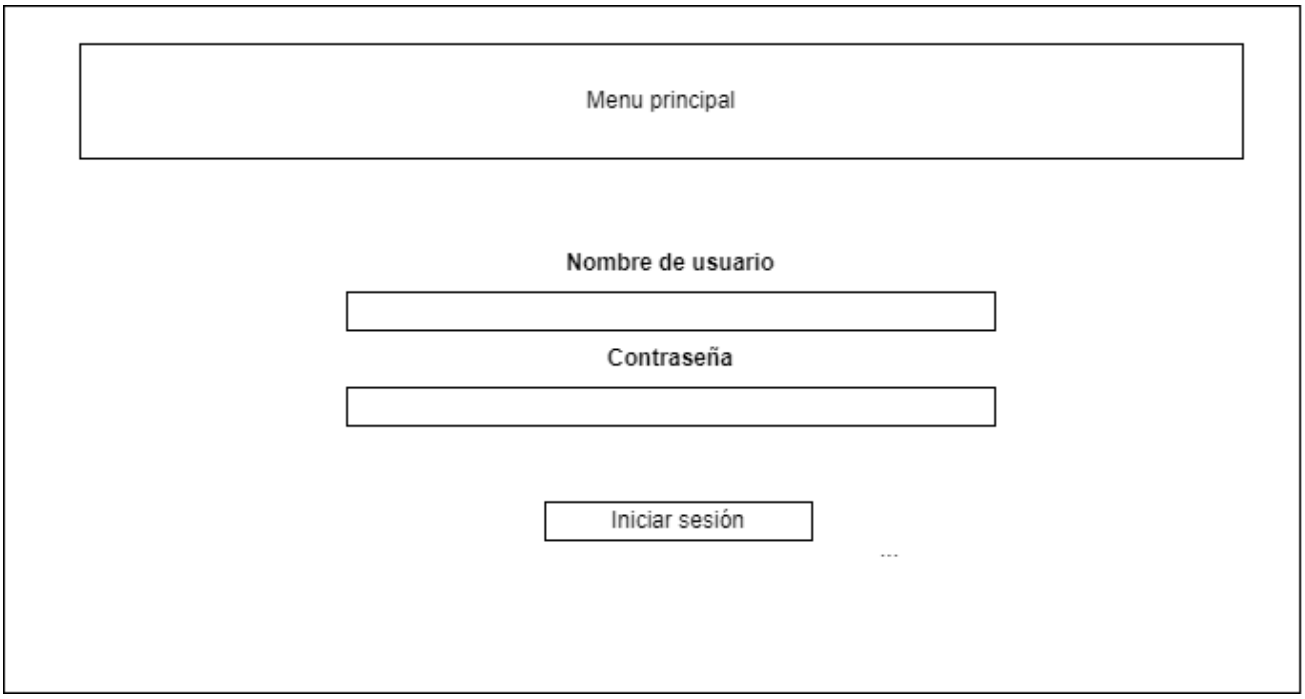

Ilustración 30. Login. App Escritorio

5.6.1.1.2 Proceso electoral

Se presentan las pantallas necesarias para el paquete “proceso electoral”

5.6.1.1.2.1 Crear usuario

Se muestra la pantalla de creación de usuario.

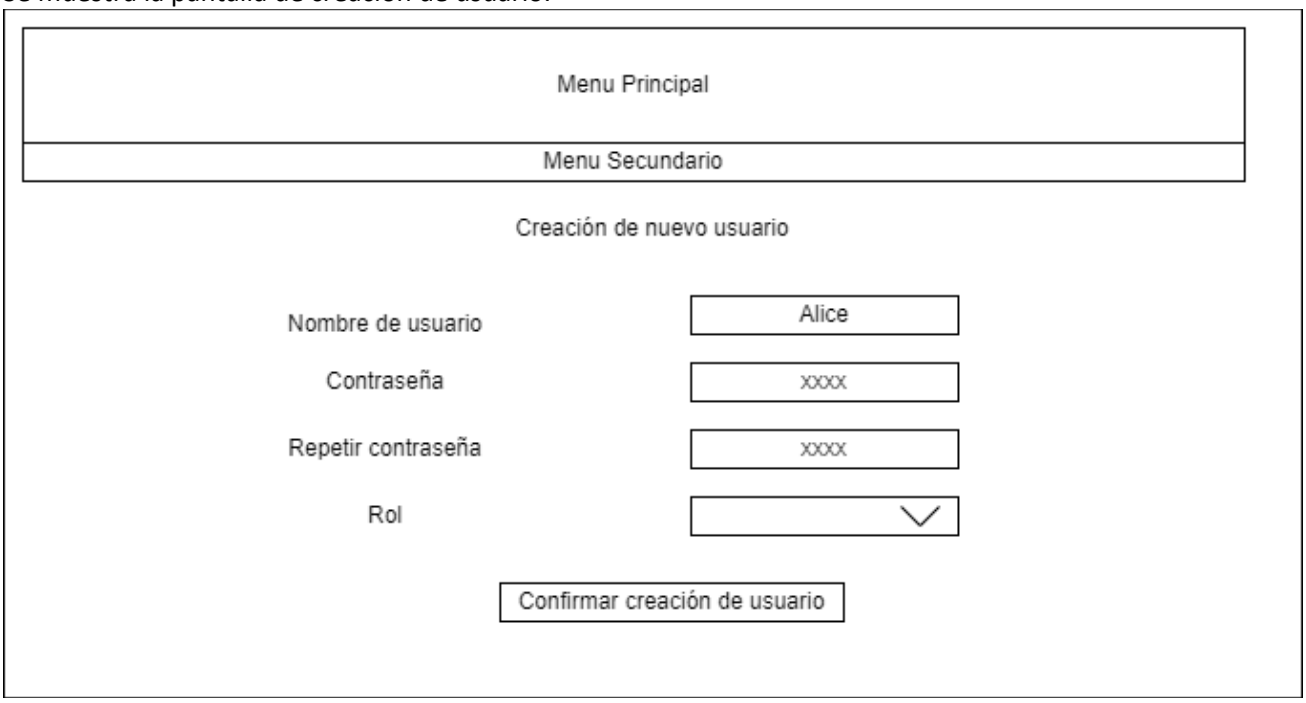

Ilustración 31. App Escritorio. Crear usuario

5.6.1.1.2.2 Crear nuevo proceso electoral

Esta es la pantalla para crear nuevos procesos electorales.

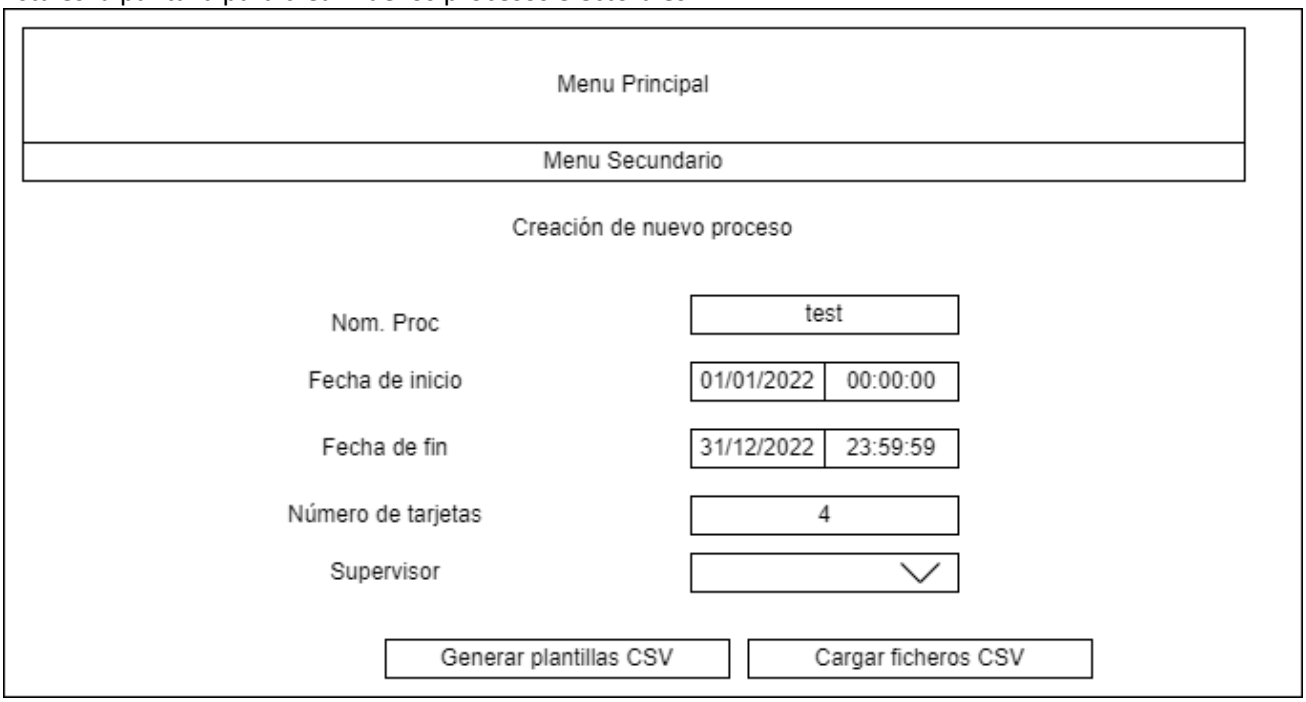

Ilustración 32. App Escritorio. Nuevo Proceso

5.6.1.1.2.3 Archivos de sesión

Esta es la pantalla de cargar archivos, necesaria para crear el proceso electoral.

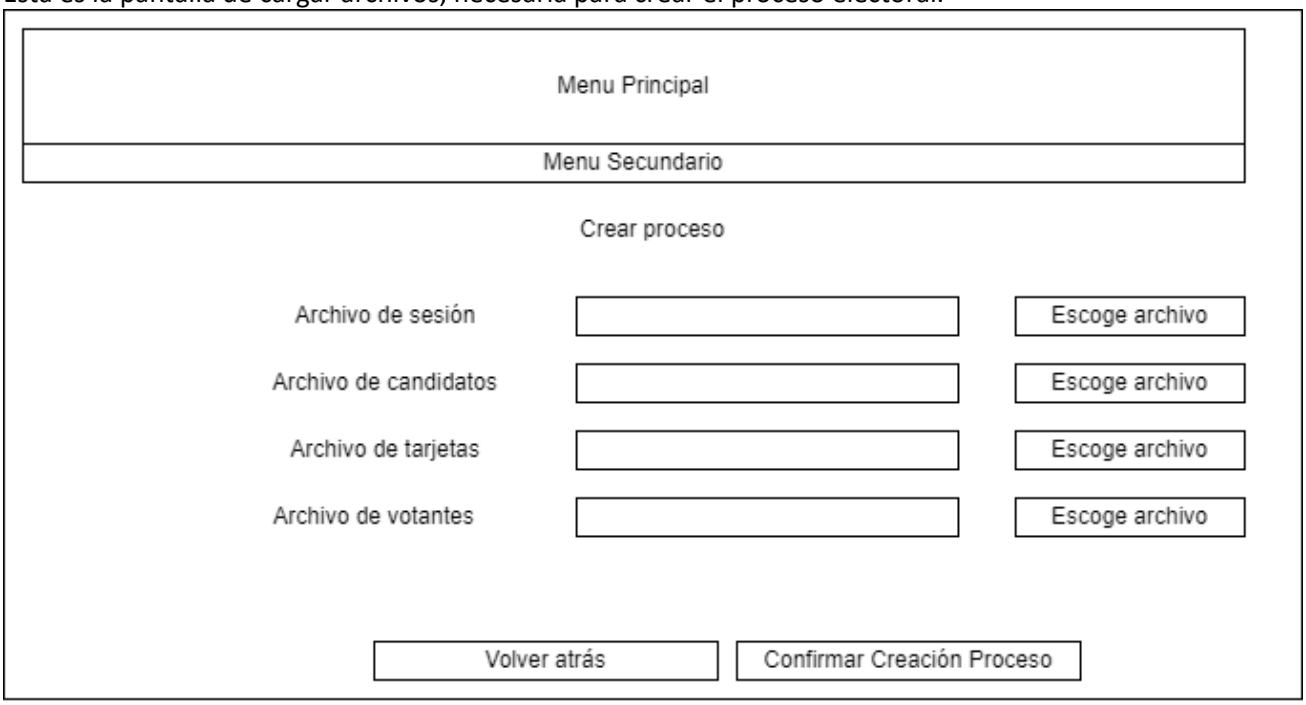

Ilustración 33. App Escritorio. Archivo de sesión

5.6.1.1.3 Escutinio

Se presentan las pantallas necesarias para el paquete “Poll”.

5.6.1.1.3.1 Seleccionar proceso

Esta es la pantalla de selección de proceso.

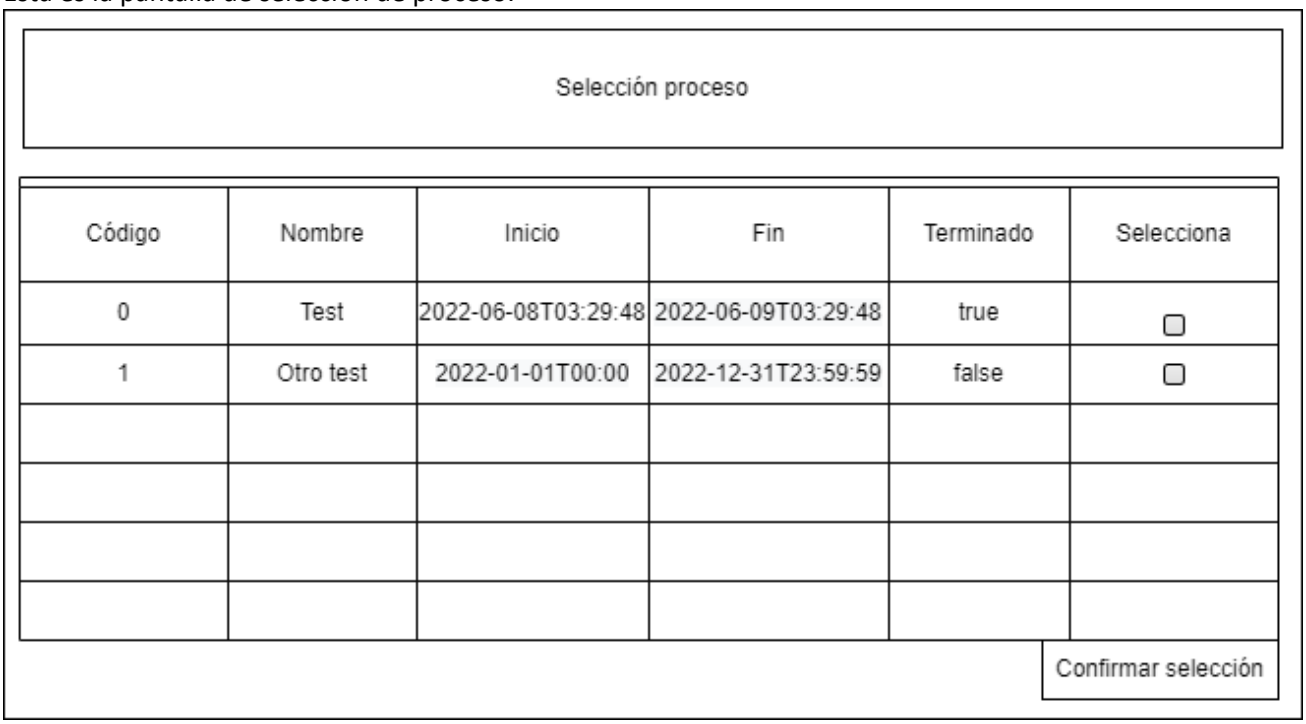

Ilustración 34. App Escritorio. Seleccionar proceso

5.6.1.1.3.2 Resultados

La pantalla o pantallas donde se muestran los resultados de la elección escogida

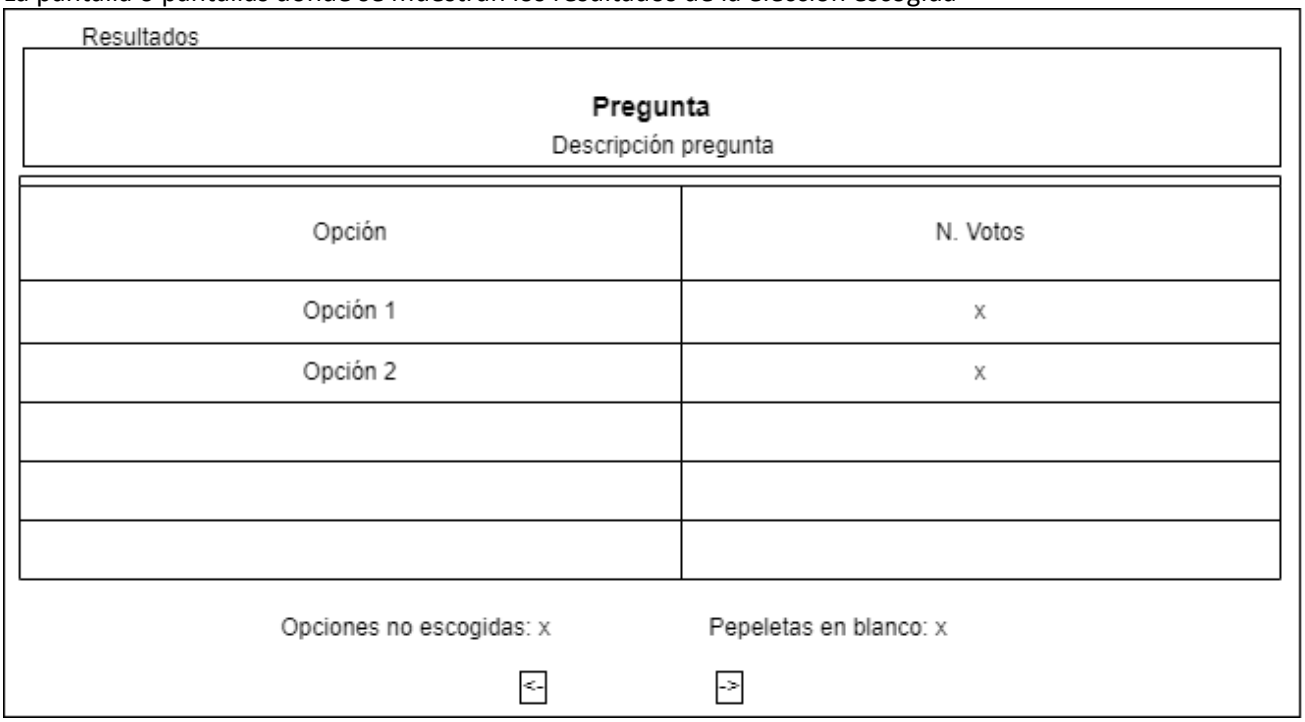

Ilustración 35. App Escritorio. Resultados

5.6.1.1.4 Urna

Se presentan las pantallas necesarias para el paquete “Urna”.

5.6.1.1.4.1 Seleccionar sesión

Esta es la pantalla de elección de la sesión.

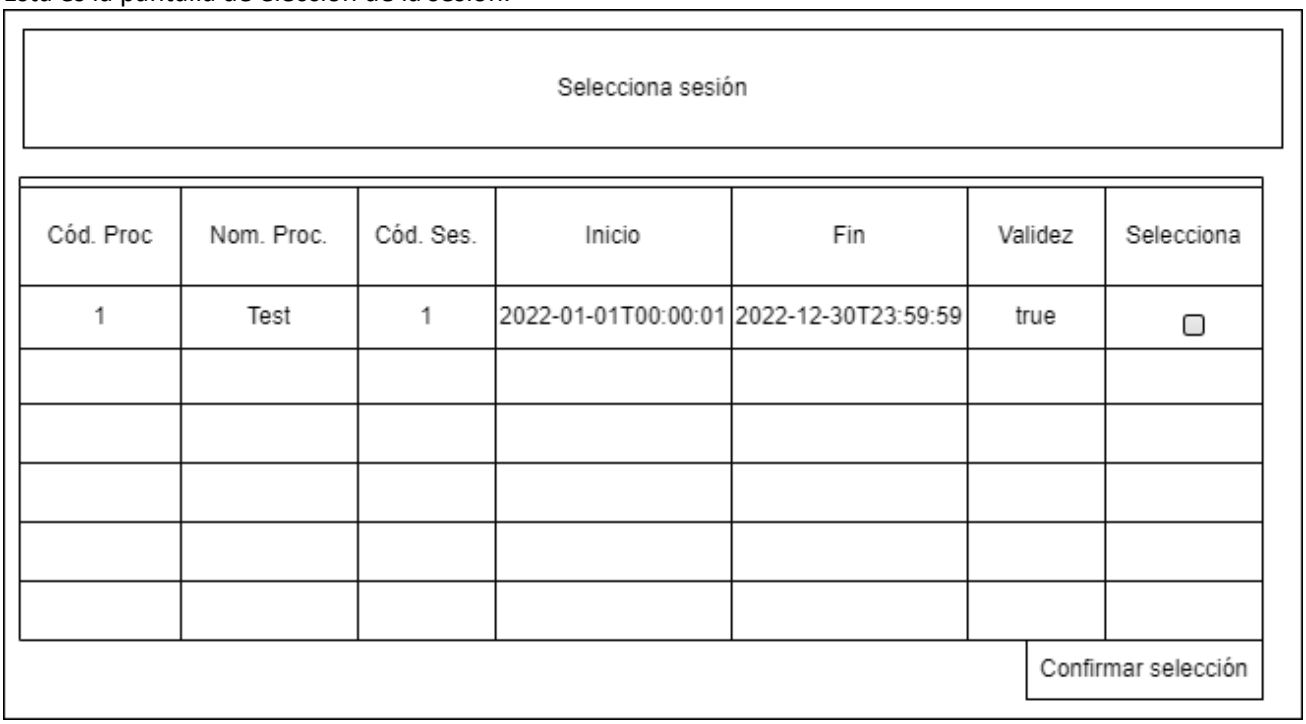

Ilustración 36. App Escritorio. Seleccionar sesión

5.6.1.1.4.2 Mensaje urna

Esta es la pantalla donde se muestran los mensajes enviados entre la Urna y los terminales.

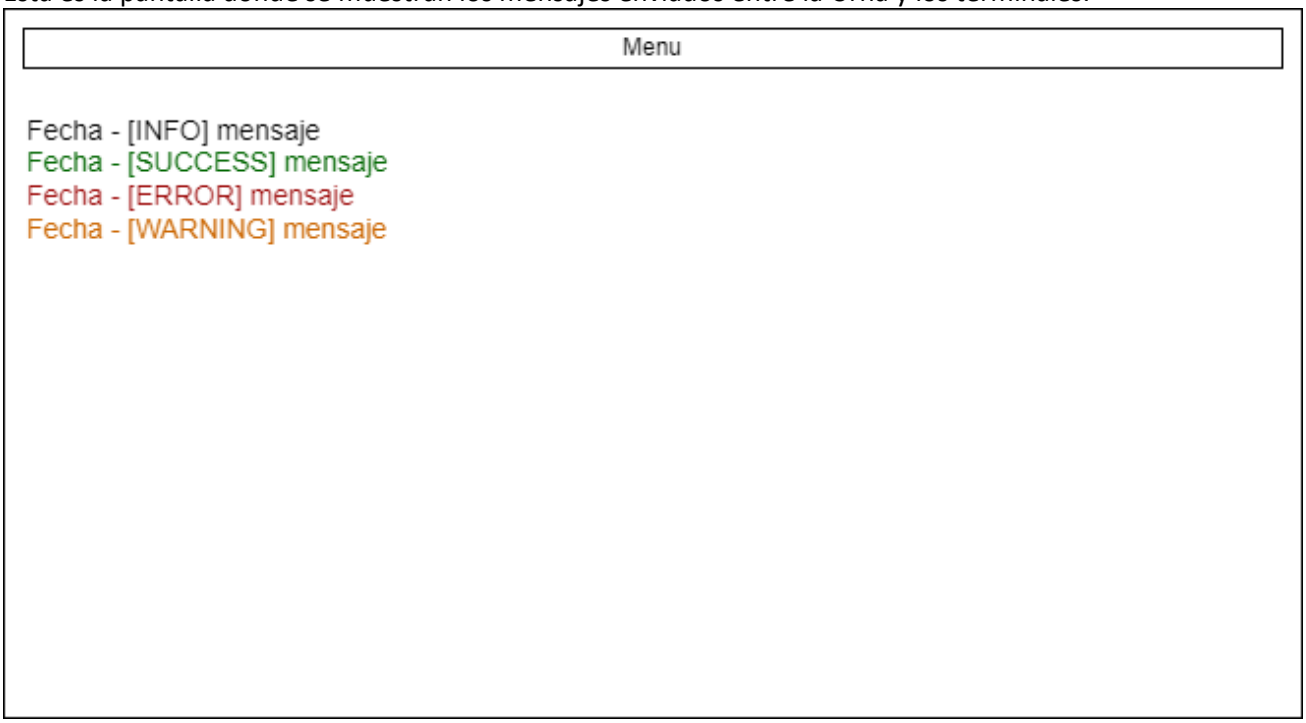

Ilustración 37. App Escritorio. Mensaje urna

5.6.1.1.5 Mesa electoral

Se presentan las pantallas necesarias para el paquete “Seggio”.

5.6.1.1.5.1 Clave de sesión

Esta es la pantalla necesaria para introducir la clave de sesión.

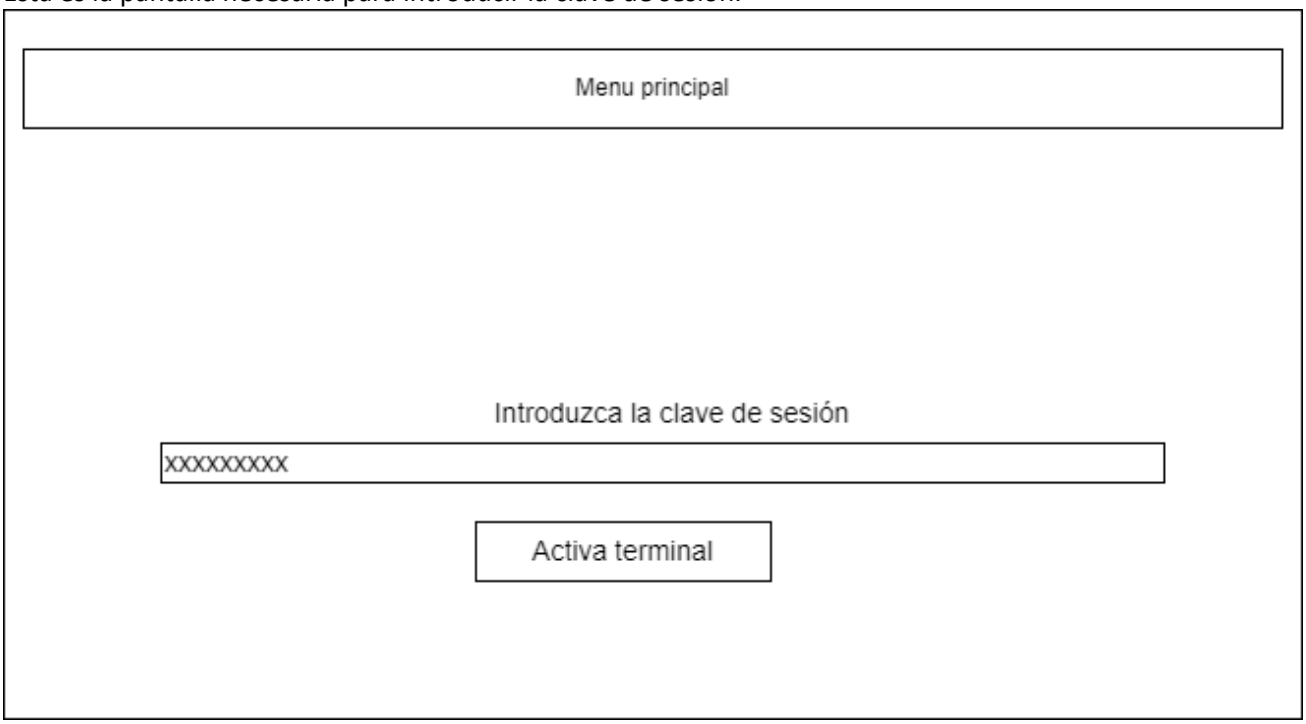

Ilustración 38. App Escritorio. Mesa_Clave sesión

5.6.1.1.5.2 Lista de puestos

Esta es la pantalla donde se muestra la lista de puestos y las opciones para actualizar, registrar y buscar votantes.

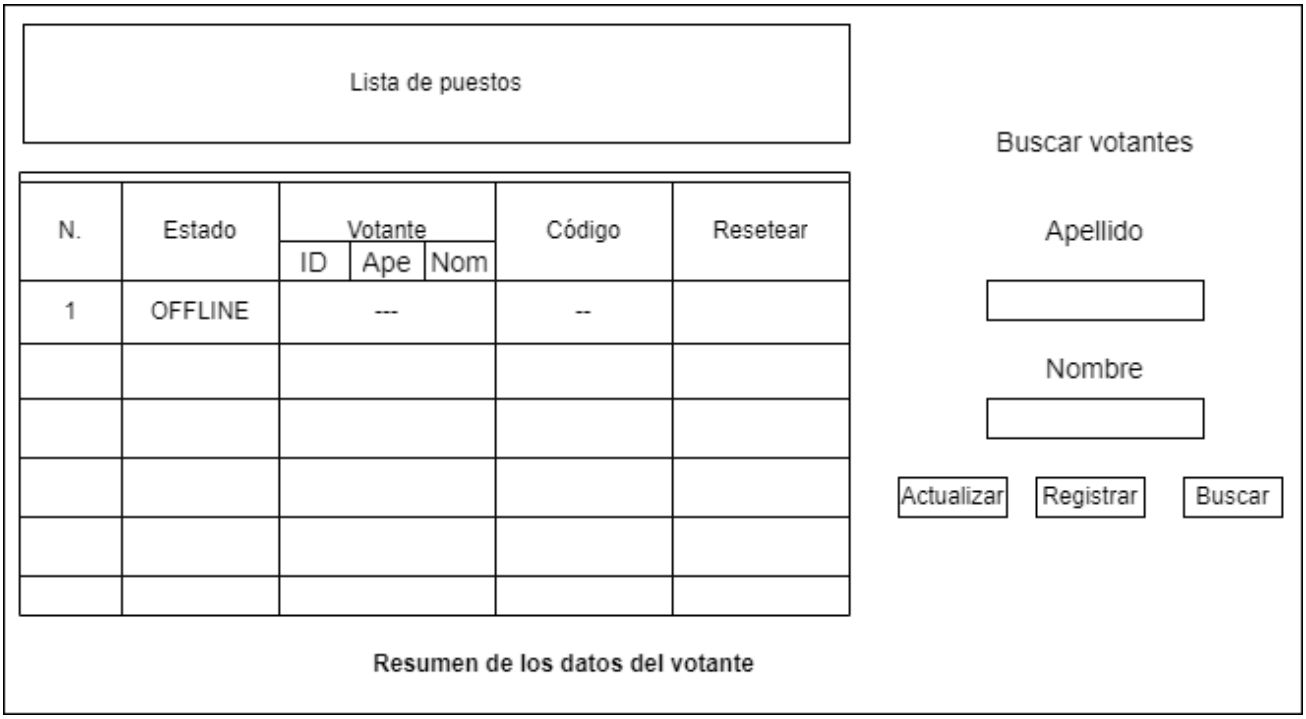

Ilustración 39. App Escritorio. Lista de puestos

5.6.1.1.5.3 Actualizar

Esta es la pantalla para actualizar un votante existente.

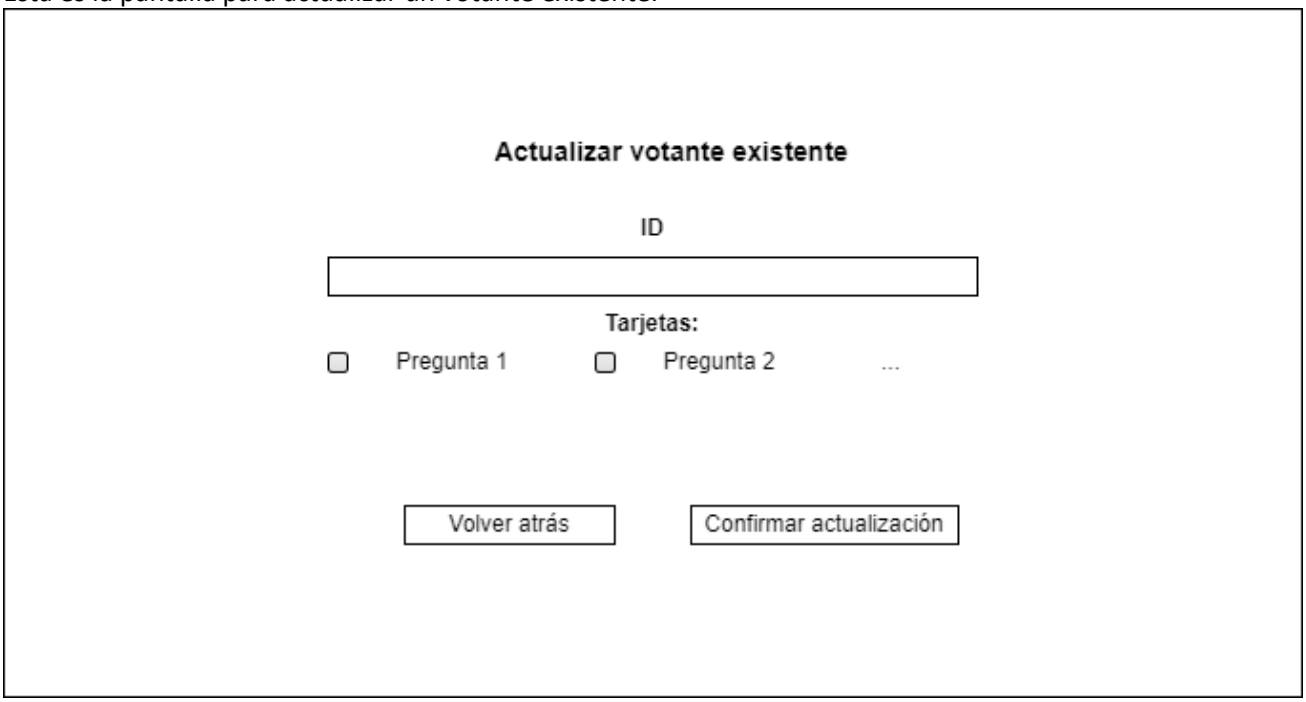

Ilustración 40. App Escritorio. Actualizar

5.6.1.1.5.4 Registrar

Esta es la pantalla para registrar un nuevo votante.

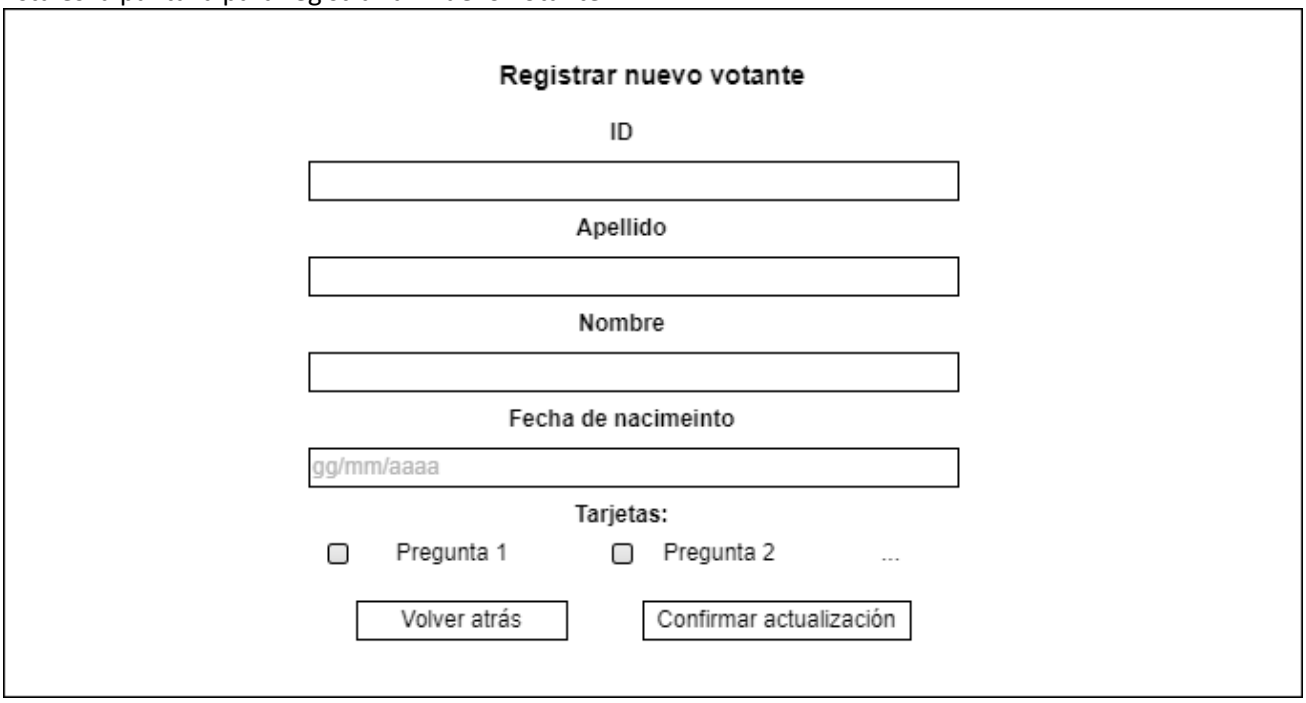

Ilustración 41. App Escritorio. Registrar

5.6.1.1.5.5 Buscar

Esta es la pantalla para buscar un votante.

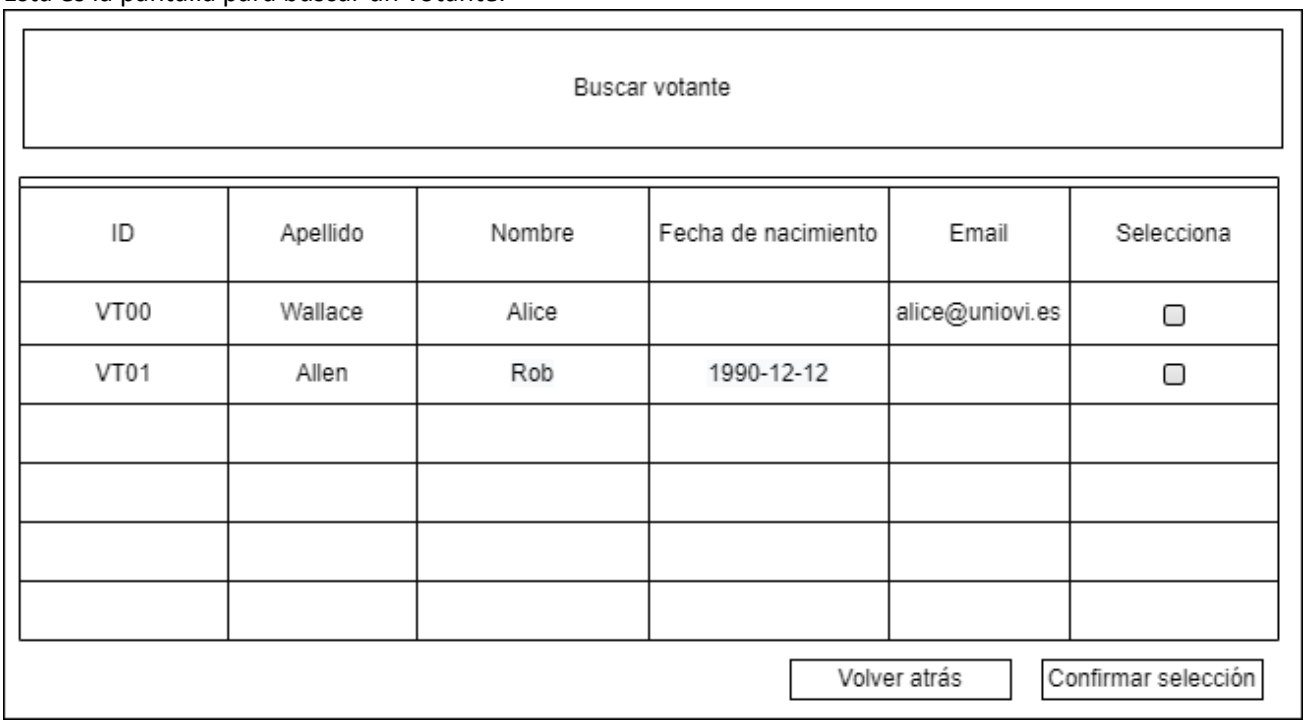

Ilustración 42. App Escritorio. Buscar

5.6.1.1.5.6 Resumen de datos del votante

En esta pantalla se muestran los datos del votante y se muestra el puesto activo. Solo falta generar el código.

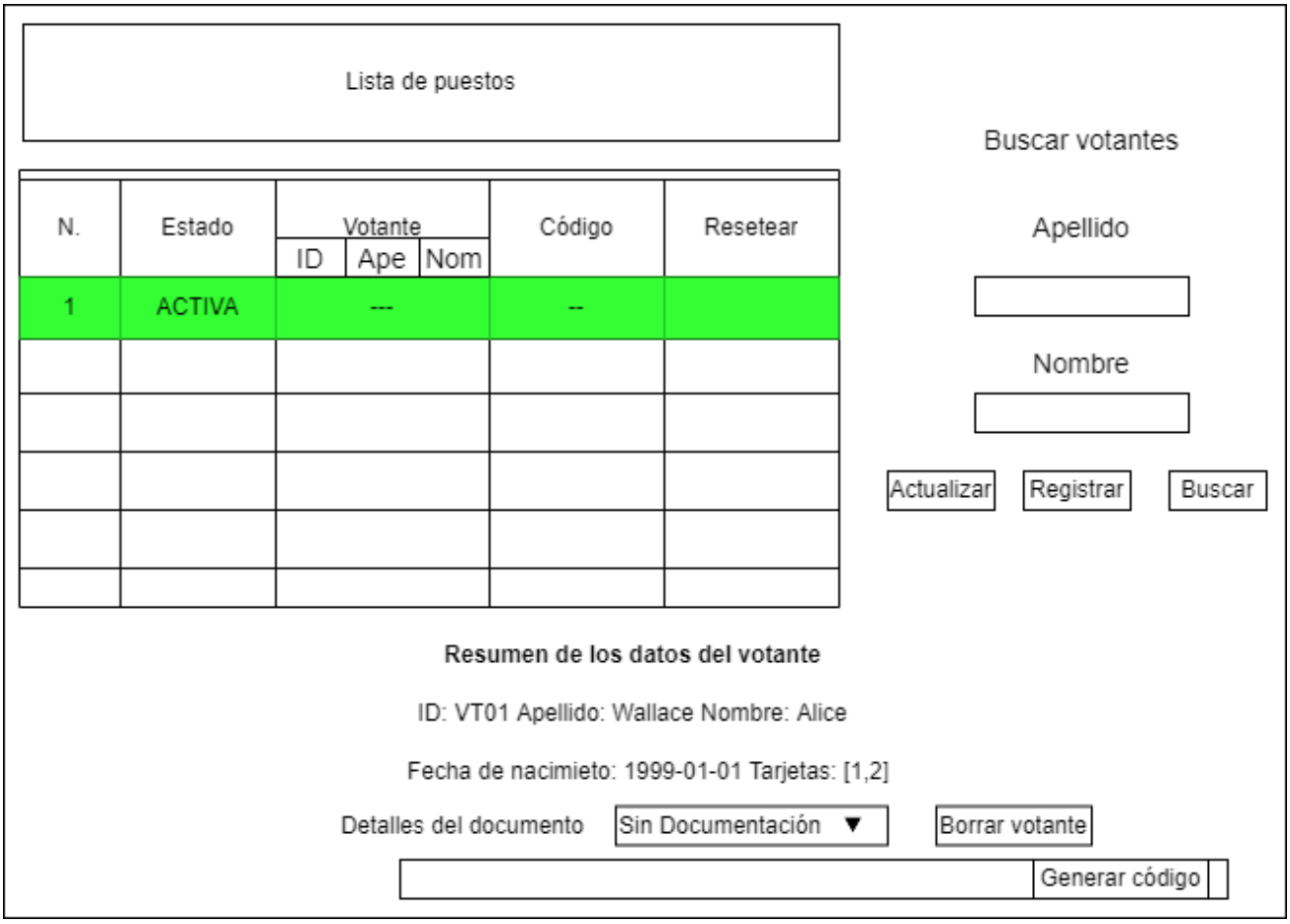

Ilustración 43. Resumen de datos del votante

5.6.1.1.5.7 Lista de puestos, asociado

Una vez se genere el código, el puesto pasa a estar en estado ASOCIADA.

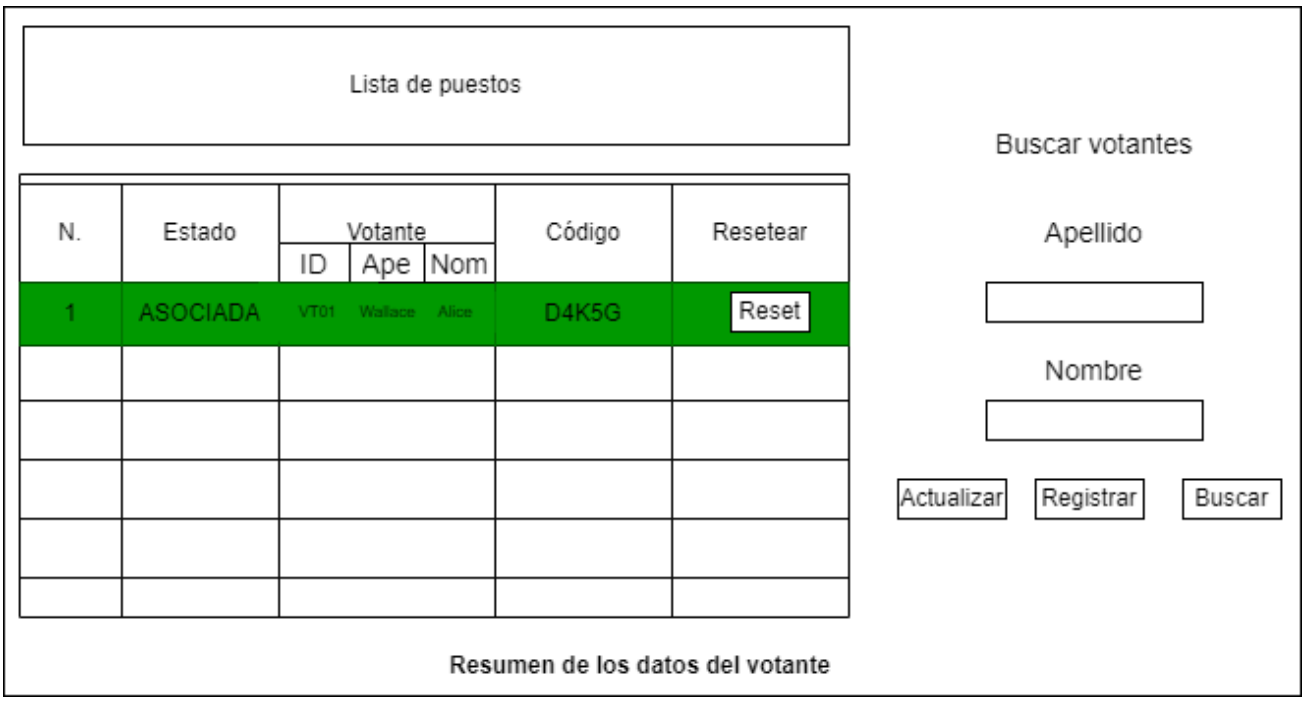

Ilustración 44. Lista de puestos. Asociado

5.6.1.1.5.8 Lista de puesto, en uso

Una vez, el votante inicie la votación, el puesto estará en estado EN USO.

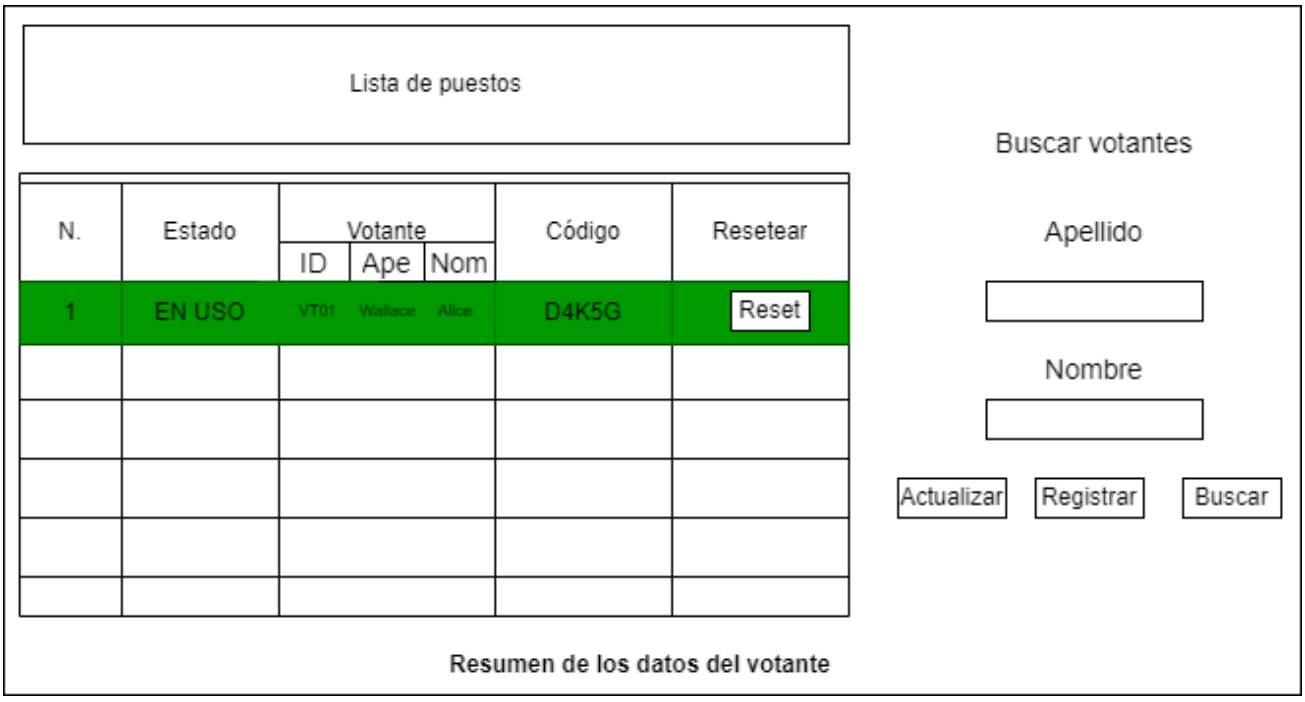

Ilustración 45. Lista de puestos. En uso

5.6.1.1.5.9 Voto enviado

Cuando el votante finalice la votación en el puesto, se mostrará el puesto tendrá estado VOTO ENVIADO.

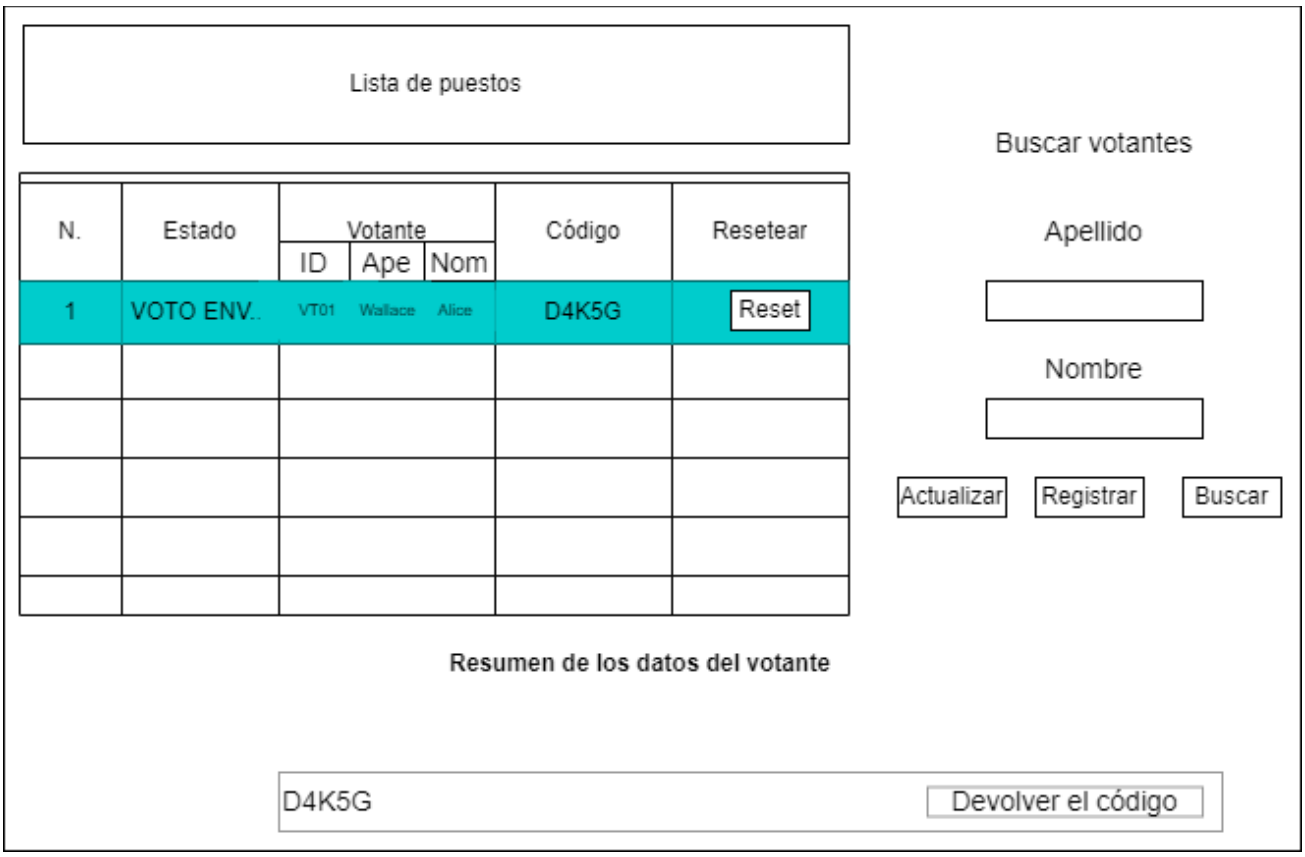

Ilustración 46. Voto enviado

5.6.1.1.6 Puesto de votación

5.6.1.1.6.1 Clave de sesión

Esta es la pantalla necesaria para introducir la clave de sesión.

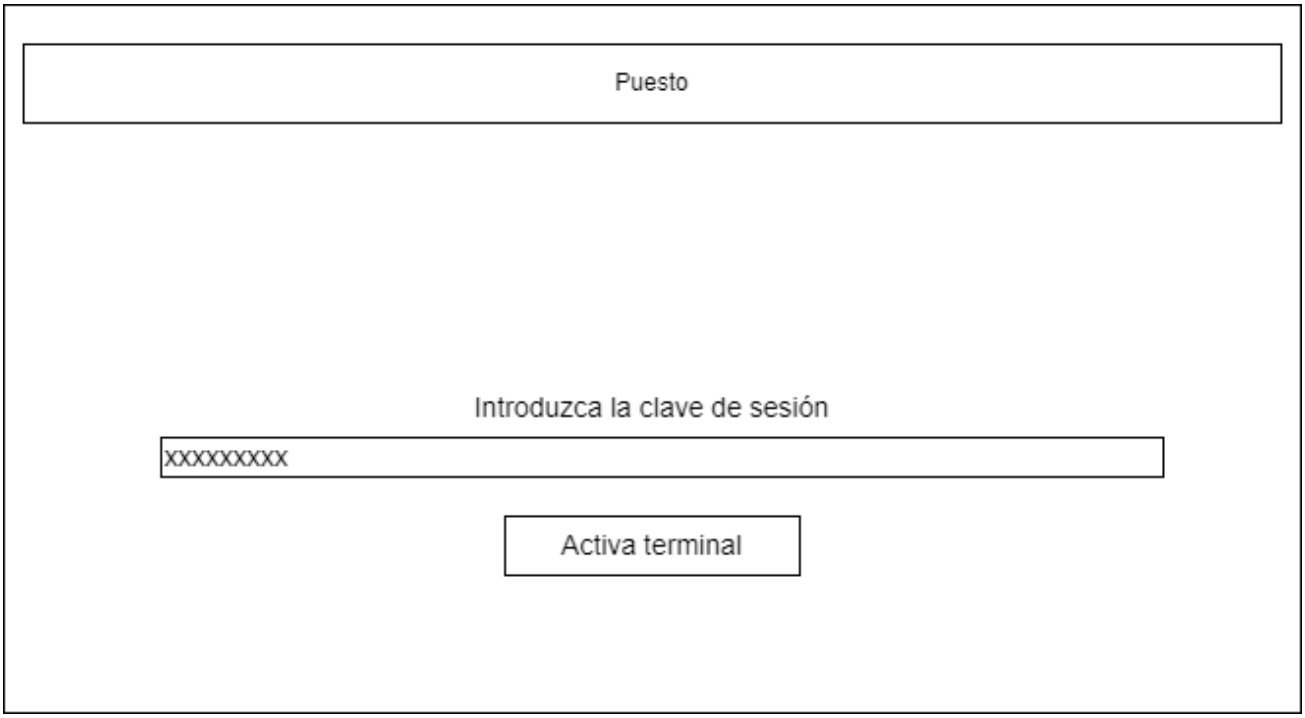

Ilustración 47. Puesto de votación. Clave de sesión

5.6.1.1.6.2 Puesto activado

Ilustración 48. Puesto activado

5.6.1.1.6.3 Puesto asociado

Se debe introducir el código generado por el supervisor en la Mesa electoral.

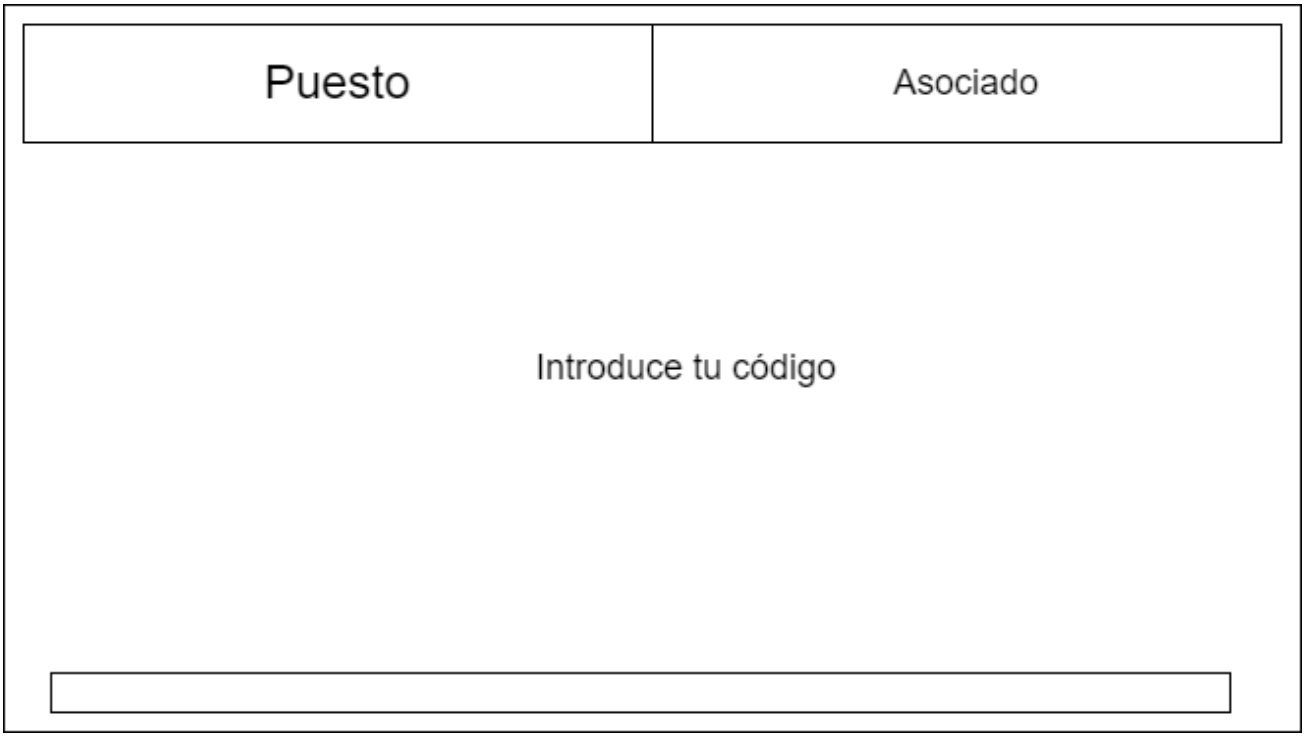

Ilustración 49. Puesto asociado

5.6.1.1.6.4 Iniciar votación

Pantalla de iniciar votación.

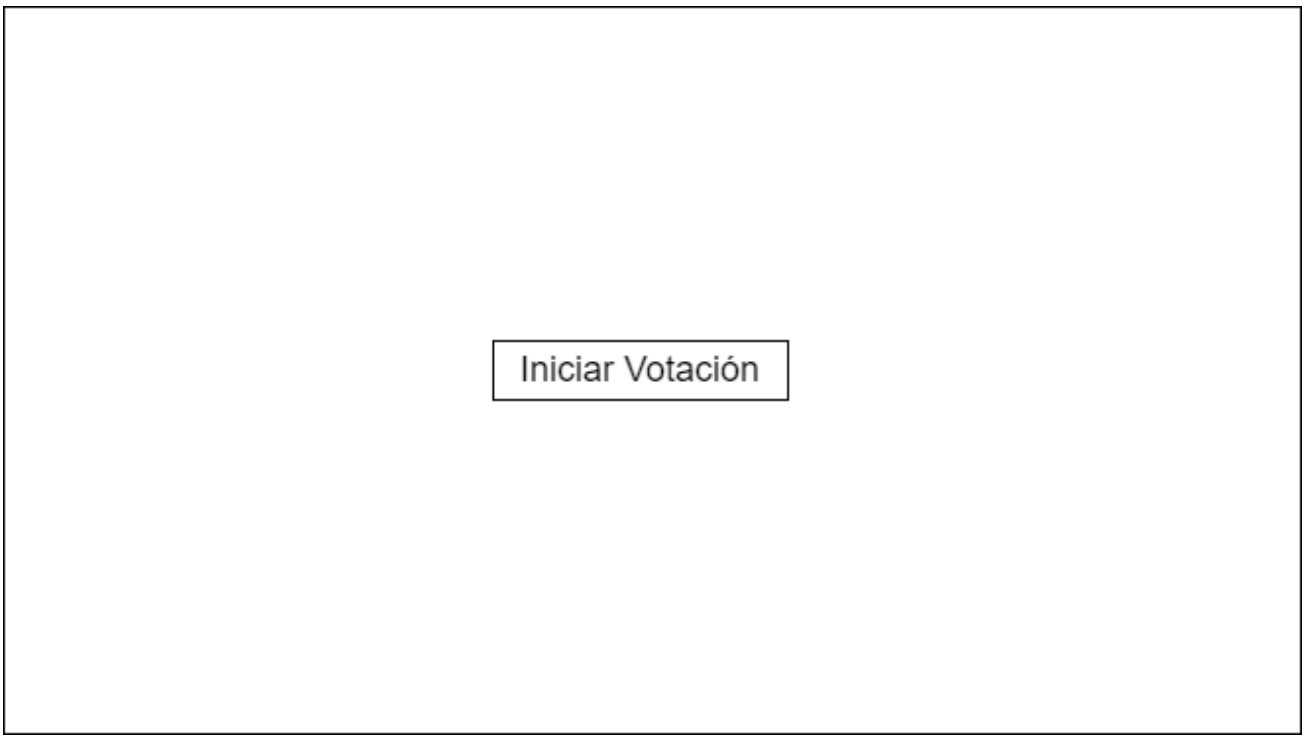

Ilustración 50. Iniciar votación

5.6.1.1.6.5 Referéndum

Preguntas de tipo referéndum (no se votan a candidatos):

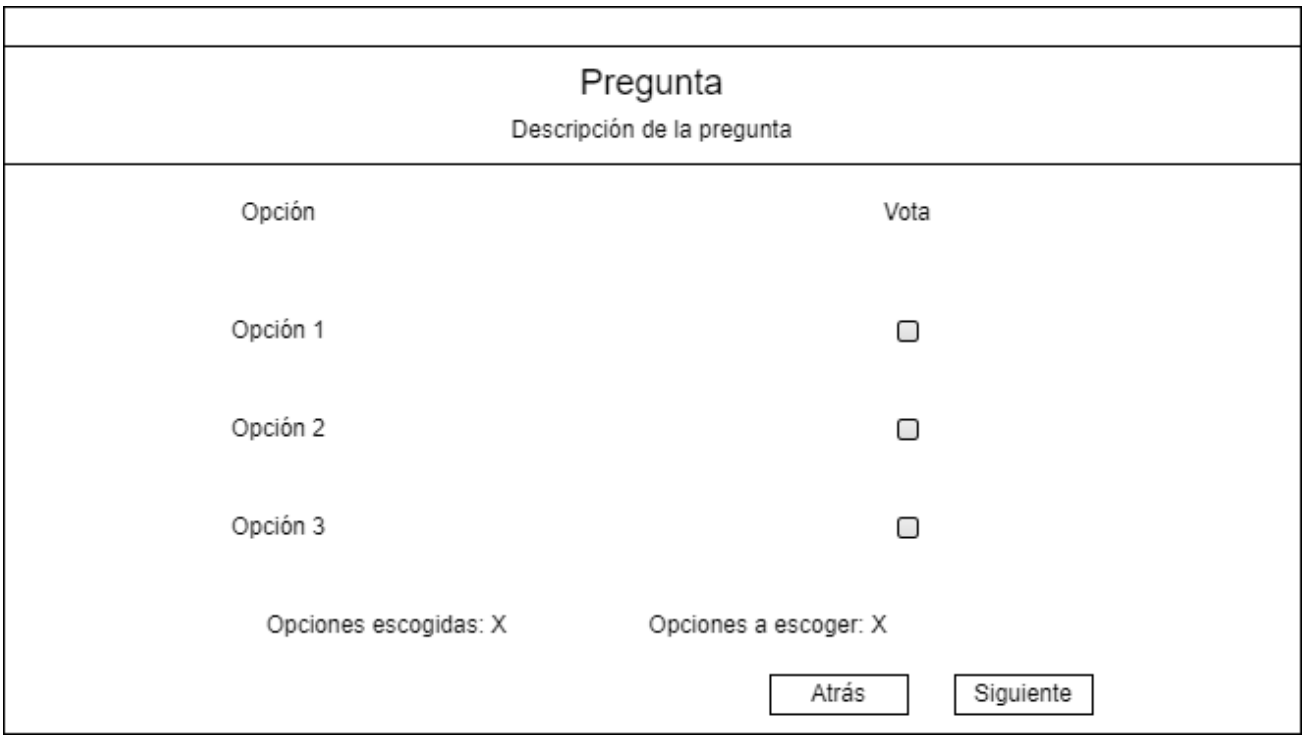

Ilustración 51. Referéndum

5.6.1.1.6.6 Candidatos

Preguntas donde se votan a candidatos:

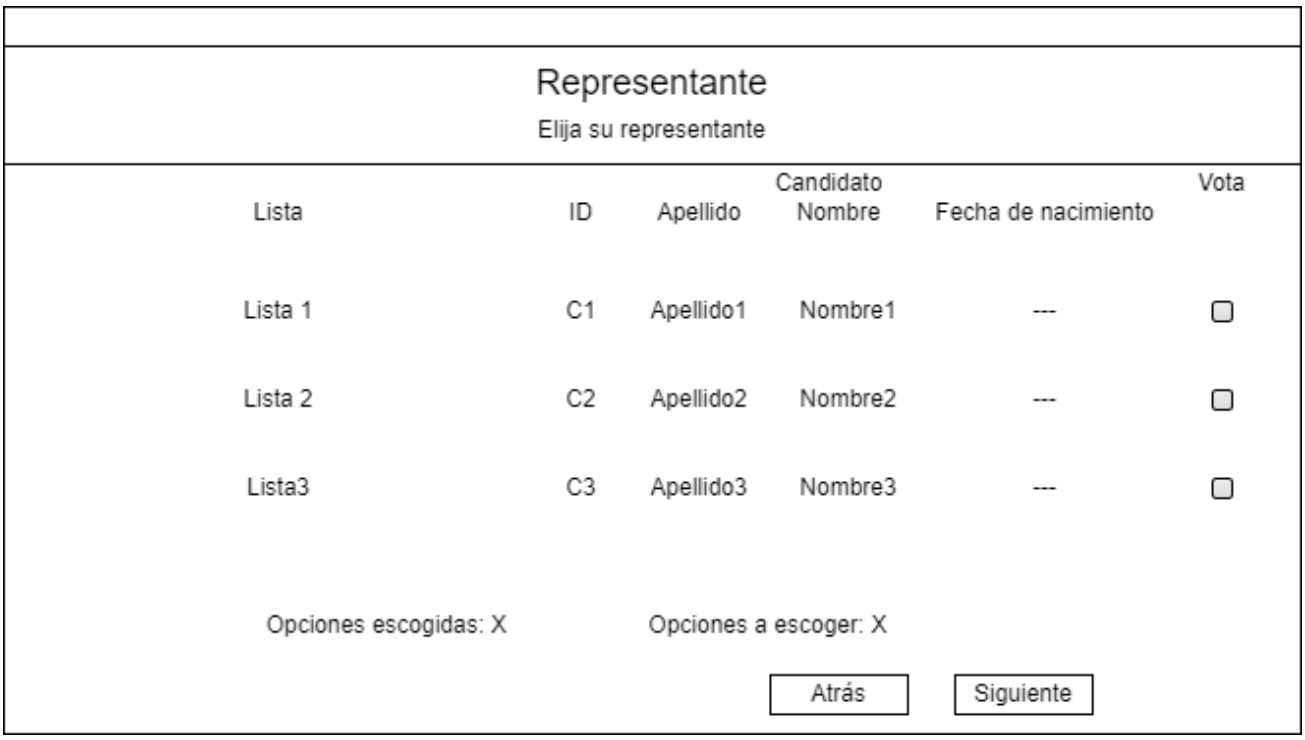

Ilustración 52. Candidatos

5.6.1.1.6.7 Resumen de votación

Se muestra el resumen de la votación y se puede proceder a enviar los votos:

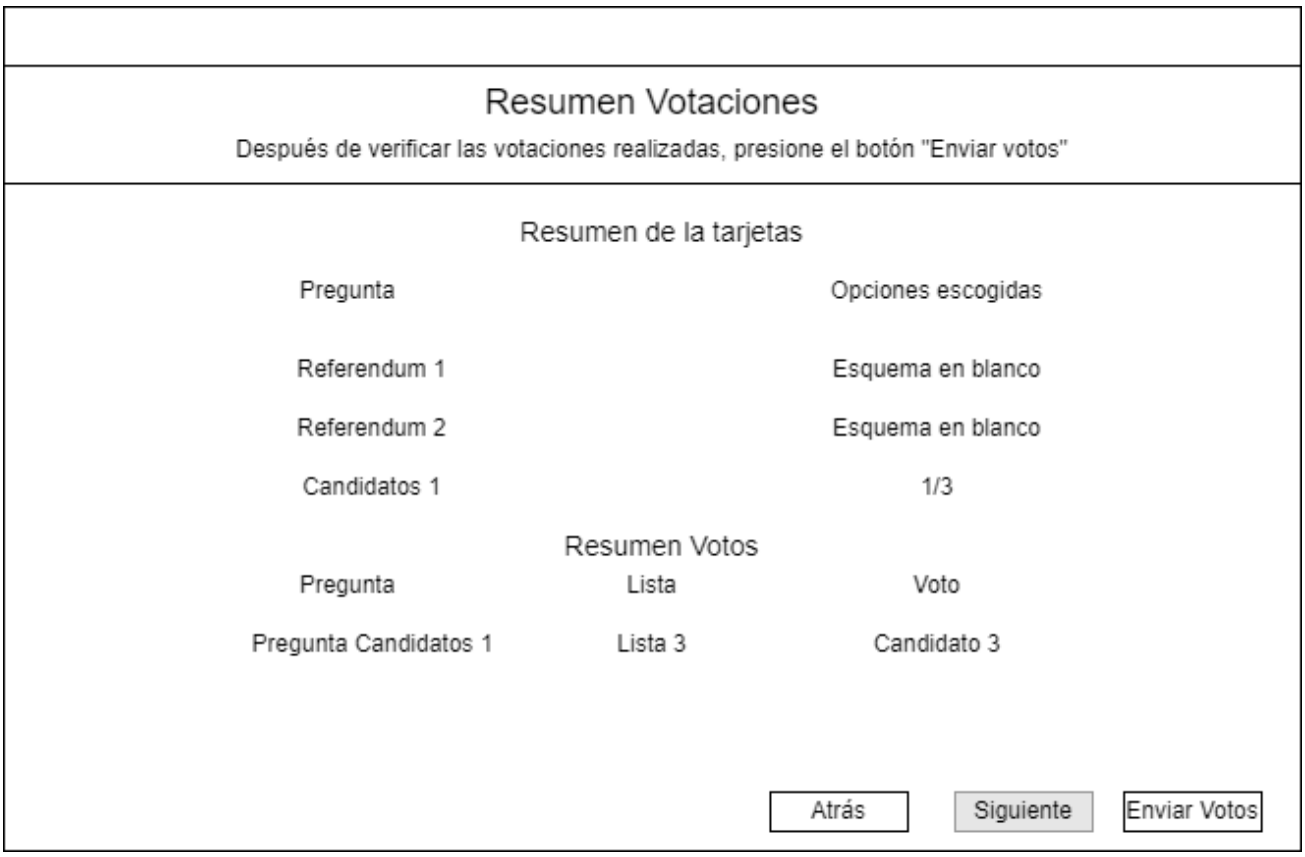

Ilustración 53. Resumen de votación

5.6.1.1.6.8 Entregar el token

Pantalla donde se indica al votante que se debe avisar/entregar el token al supervisor para que confirme la devolución del token:

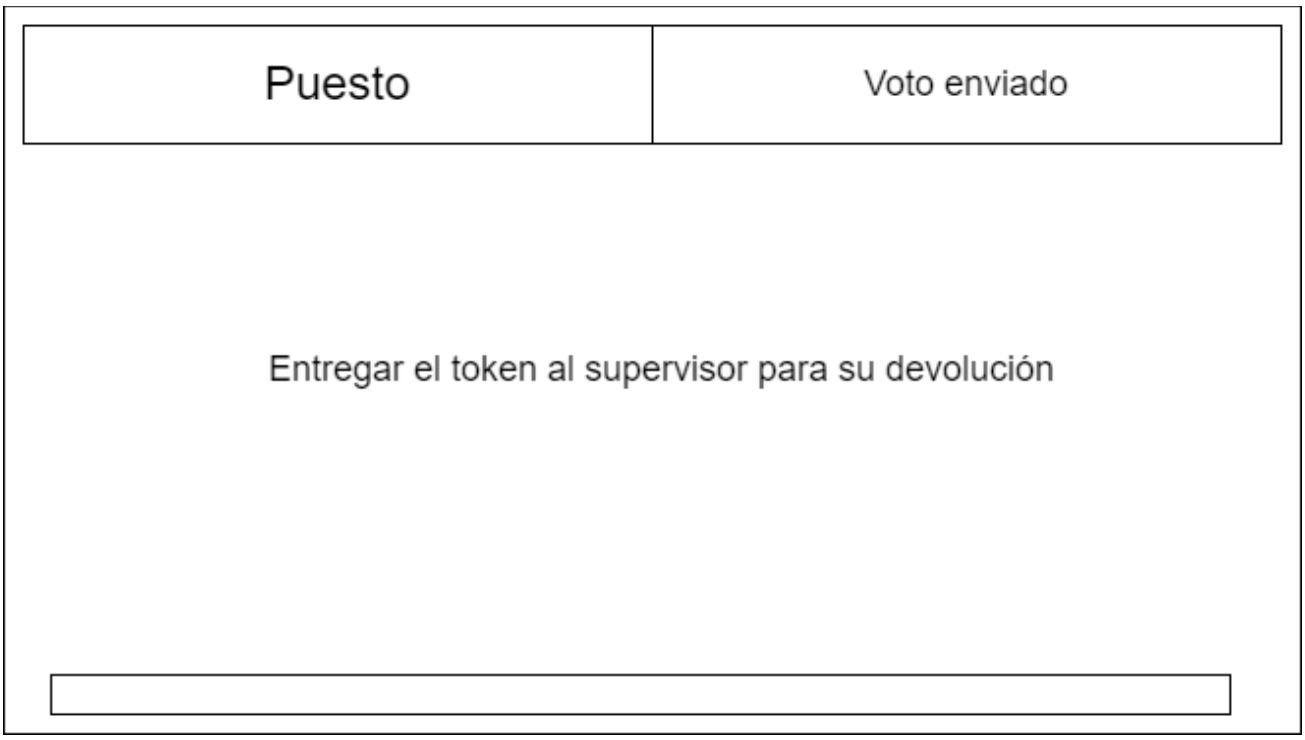

Ilustración 54. Voto enviado

5.6.1.1.6.9 Voto enviado con éxito

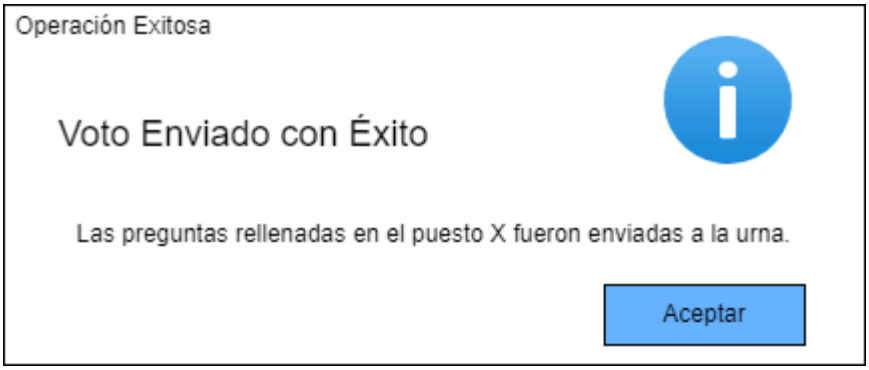

Ilustración 55. Voto enviado con éxito

5.6.1.2 Aplicación web

5.6.1.2.1 Login

Pantalla de inicio de sesión de la aplicación web:

Ilustración 56. App web. Login

5.6.1.2.2 Registro

Pantalla de registro de la aplicación web:

Ilustración 57. App web. Registro

5.6.1.2.3 Votación

Pantalla de votación de la aplicación web:

Ilustración 58. App web. Votación

5.6.2 Diagrama de navegabilidad

Se muestran los diagramas de navegabilidad para cada uno de los paquetes.

5.6.2.1 Aplicación de escritorio

5.6.2.1.1 Administrador del Proceso electoral

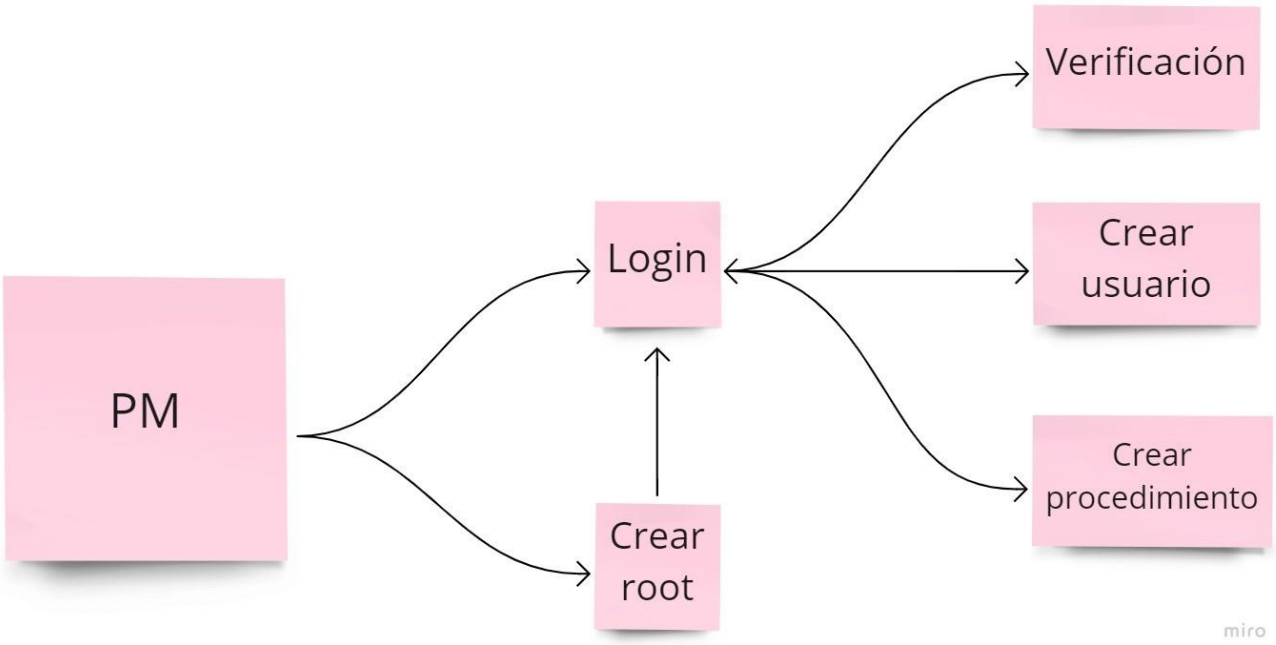

Ilustración 59. Navegabilidad, Administrador del proceso electoral

5.6.2.1.2 Escrutinio

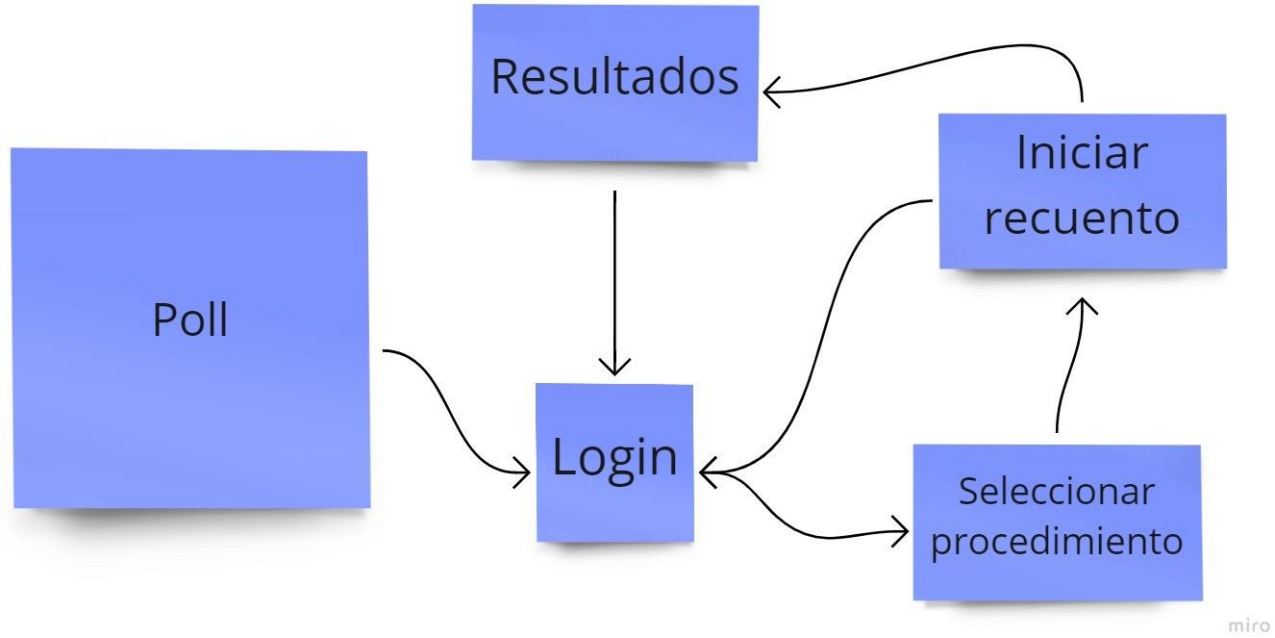

Ilustración 60. Navegabilidad. Escrutinio

5.6.2.1.3 Urna

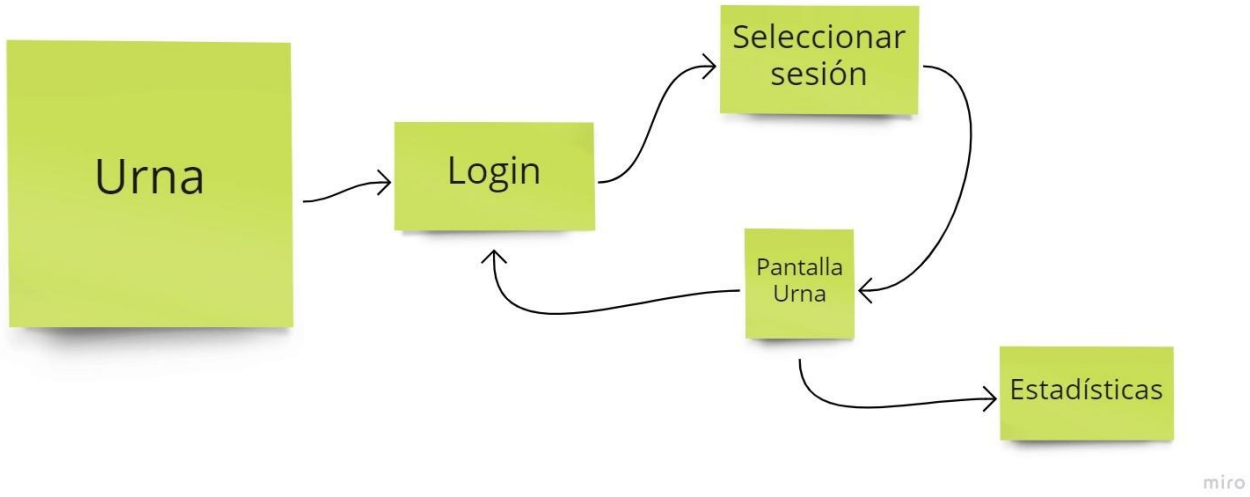

Ilustración 61. Navegabilidad. Urna

5.6.2.1.4 Mesa electoral

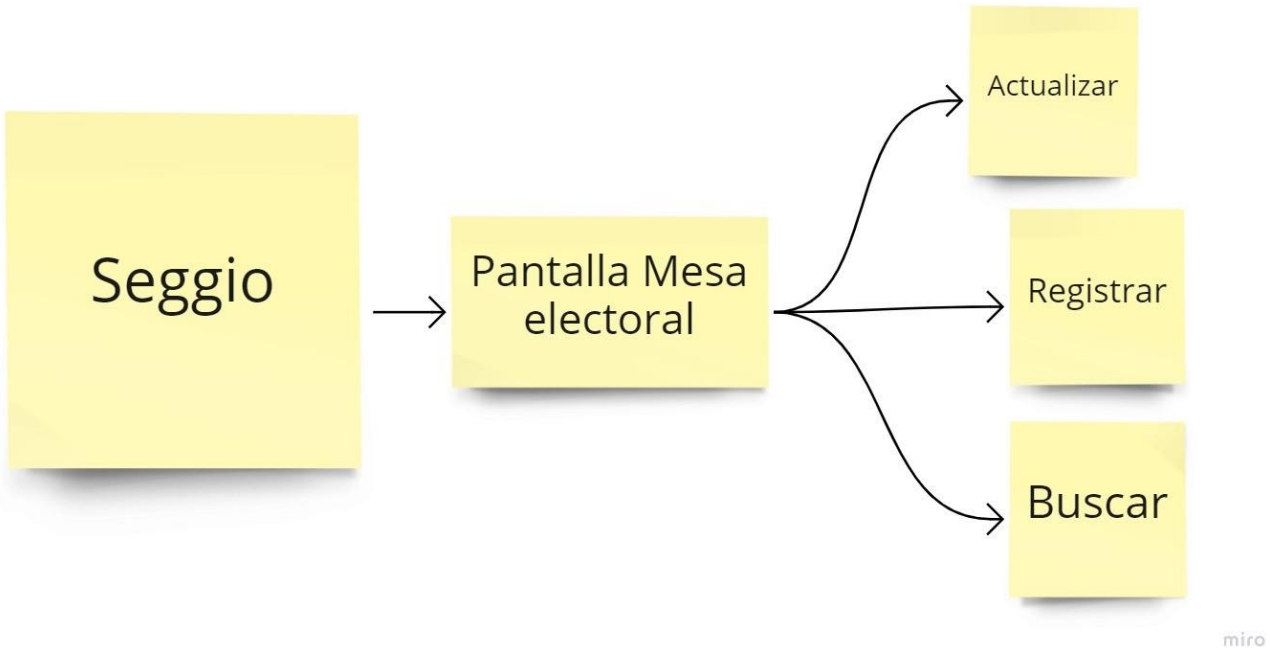

Ilustración 62. Navegabilidad. Mesa electoral.

5.6.2.1.5 Puesto de votación

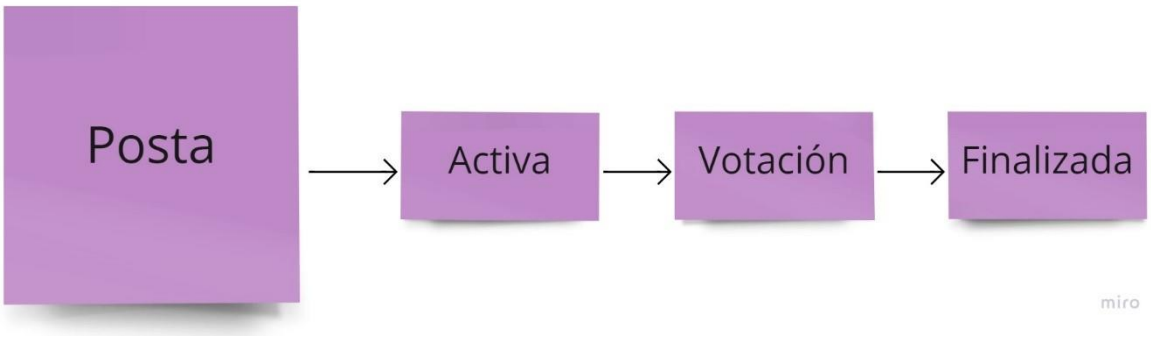

Ilustración 63. Navegabilidad. Puesto de votación

5.6.2.2 Aplicación web

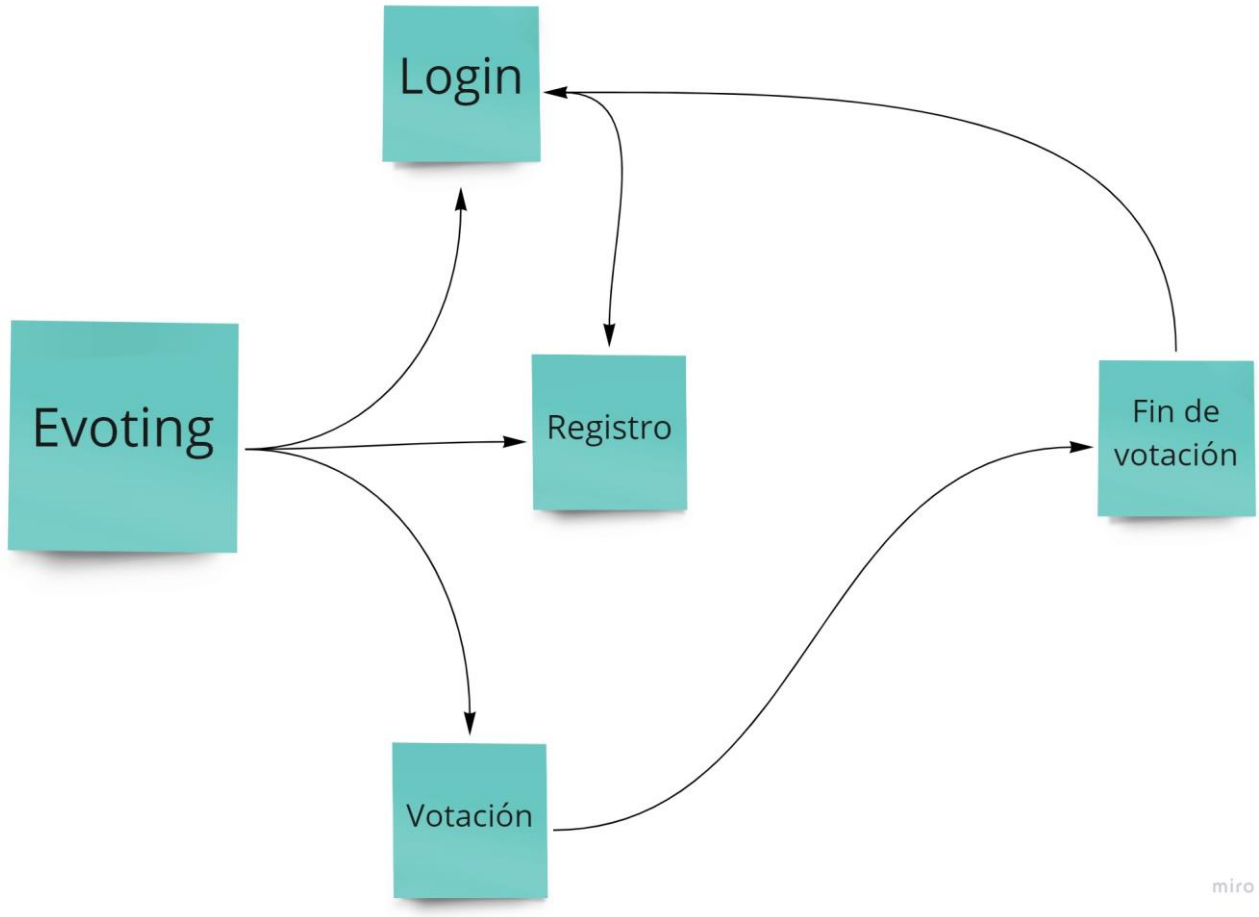

Ilustración 64. Navegabilidad. App web

5.7 ESPECIFICACIÓN DEL PLAN DE PRUEBAS

5.7.1 Aplicación de escritorio

5.7.1.1 Pruebas unitarias

Prueba 01 – Votación sin sesión	
Prueba	**Resultado esperado**
Votación sin sesión	No existe una sesión asignada para el proceso electoral.

Tabla 72. Votación sin sesión

Prueba 02 – Votación sin votante	
Prueba	**Resultado esperado**
Votación con votante con ID falso	No existe votante con el ID proporcionado.

Tabla 73. Votación sin votante

Prueba 03 – Votación sin terminal (mesa electoral)	
Prueba	**Resultado esperado**
Votación con terminal no existente	No existe el terminal (mesa electoral) proporcionado.

Tabla 74. Votación sin mesa electoral

Prueba 04 – Terminales no coinciden	
Prueba	**Resultado esperado**
Se comparan terminales con distinta IP	No son el mismo terminal

Tabla 75. Terminales no coinciden

Prueba 05 – Votación sin terminal (puesto)	
Prueba	**Resultado esperado**
Votación con terminal no existente	No existe el terminal (puesto) proporcionado.

Tabla 76. Votación sin puesto

Prueba 06 – Puesto de votación no válido para mesa electoral	
Prueba	**Resultado esperado**
El puesto de votación no pertenece a la mesa electoral	La combinación Mesa electoral – Puesto falla

Tabla 77. Puesto de votación no válido

Prueba 07 – Incoherencia pregunta asignada al votante	
Prueba	**Resultado esperado**
Se le asigna una pregunta al usuario cuando tiene otra asignada	Fallo. El votante tenía asignado otra pregunta.

Tabla 78. Incoherencia pregunta asignada

Prueba 08 – Votante ya ha votado	
Prueba	**Resultado esperado**
Se intenta votar con un votante dos veces	Fallo. El votante ya ha votado.

Tabla 79. Votante ya ha votado

5.7.1.2 Pruebas de integración

La aplicación tiene mucha parte que implica la interacción con el usuario.

Prueba 09 – Se conecta la urna con los terminales (mesa electoral y puesto)	
Prueba	**Resultado esperado**
Se arranca la urna y los terminales, se espera su conexión.	1. Se debe arrancar la urna. 2. Se debe arrancar la mesa electoral con una clave de sesión válida. 3. Se debe arrancar el puesto de votación con una clave de sesión válida.

Tabla 80. Se conecta la urna con terminales

Prueba 10 – Se realiza una votación	
Prueba	**Resultado esperado**
Se realiza una votación	1. Deben estar activas la urna, la mesa electoral y el puesto de votación. 2. Se debe buscar al votante con los criterios establecidos. 3. Seleccionar al votante y confirmar la selección. 4. Generar el código. 5. Realizar la votación. 6. El supervisor debe devolver el token para confirmar la votación.

Tabla 81. Se realiza la votación

5.7.2 Aplicación web

5.7.2.1 Pruebas unitarias

Prueba 11 – Buscar una pregunta por ID	
Prueba	**Resultado esperado**
Buscar una pregunta por ID	Se encuentra la pregunta

Tabla 82. Buscar una pregunta por ID

Prueba 12 – Comprobar el número de preguntas	
Prueba	**Resultado esperado**
Comprobar el número de preguntas	El número de preguntas es el adecuado.

Tabla 83. Comprobar número de preguntas

Prueba 13 – Buscar una pregunta por ID inválido	
Prueba	**Resultado esperado**
Buscar una pregunta por ID inválido	No se encuentra la pregunta

Tabla 84. Buscar una pregunta por ID inválidp

Prueba 14 – Encontrar procesos activos	
Prueba	**Resultado esperado**
Encontrar procesos activos	Se encuentran los procesos activos.

Tabla 85. Encontrar procesos activos

Prueba 15 – Encontrar proceso con código inválido	
Prueba	**Resultado esperado**
Encontrar proceso con código inválido	No se encuentra el proceso.

Tabla 86. Encontrar proceso con código inválido

Prueba 16 – Votante que ya ha votado	
Prueba	**Resultado esperado**
Votante que ya ha votado	Da error. Ya ha votado.

Tabla 87. Votante que ya ha votado

Prueba 17 – Validación de votante sin errores	
Prueba	**Resultado esperado**
Validación de votante sin errores	Sin errores

Tabla 88. Validación de votante sin errores

Prueba 18 – Proceso ya cerrado	
Prueba	**Resultado esperado**
Proceso ya cerrado	Da error.

Tabla 89. Proceso ya cerrado

Prueba 19 – Validación proceso abierto	
Prueba	**Resultado esperado**
Validación proceso abierto	Sin errores.

Tabla 90. Validación proceso abierto

Prueba 20 – Validación máxima de preferencias (0 escogidas)	
Prueba	**Resultado esperado**
Validación máxima de preferencias (0 escogidas)	Sin errores

Tabla 91. Validación max prefs (0)

Prueba 21 – Validación máxima de preferencias (Menor o igual)	
Prueba	**Resultado esperado**
Validación máxima de preferencias (Menor o igual)	Sin errores

Tabla 92. Validación max prefs (menor o igual)

Prueba 22 – Validación máxima de preferencias (Mayor)	
Prueba	**Resultado esperado**
Validación máxima de preferencias (mayor)	Da error.

Tabla 93. Validación max prefs (mayor)

Prueba 24 – Encontrar votante por nombre	
Prueba	**Resultado esperado**
Encontrar votante por nombre	Sin error

Tabla 94. Encontrar votante por nombre

Prueba 25 – Encontrar votante por nombre inválido	
Prueba	**Resultado esperado**
Encontrar votante por nombre inválido.	Da error

Tabla 95. Encontrar votante por nombre inválido

Prueba 26 – Encontrar votante por email	
Prueba	**Resultado esperado**
Encontrar votante por email	Sin error

Tabla 96. Encontrar votante por email

Prueba 27 – Encontrar votante por email inválido	
Prueba	**Resultado esperado**
Encontrar votante por email inválido	Da error

Tabla 97. Encontrar votante por email inválido

Prueba 28 – Realizar un registro de votante completo	
Prueba	**Resultado esperado**
Realizar un registro de usuario completo	Sin error

Tabla 98. Realizar un registro de votante completo

Prueba 29 – Cargar usuario	
Prueba	**Resultado esperado**
Cargar usuario	Sin error

Tabla 99. Cargar usuario

Capítulo 6 DISEÑO DEL SISTEMA DE INFORMACIÓN

6.1 DISEÑO DE CASOS DE USO REALES

En esta sección, se comentarán los casos de uso más importante de la aplicación con su correspondiente diagrama de secuencia.

6.1.1 Aplicación de escritorio

6.1.1.1 *Crear usuario*

El usuario raíz (root) tiene que empezar la creación de un usuario especificando el tipo de usuario (técnico o supervisor), el nombre de usuario, la contraseña y la contraseña repetida.

El controlador del proceso electoral (PM_Controller) solicita a la clase del proceso electoral (PM) que le devuelva el estado del usuario pues solo los usuarios con estado root pueden crear usuarios. Una vez devuelto, el controlador crea el nuevo usuario.

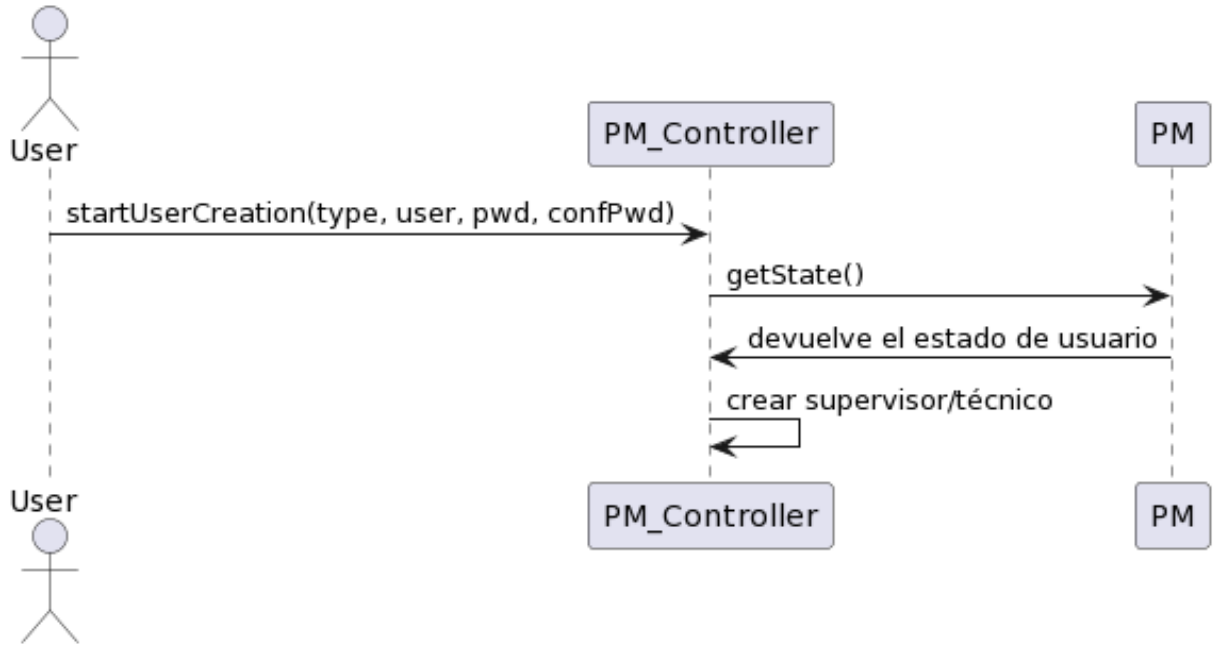

Ilustración 65. Creación de usuario

6.1.1.2 Crear proceso electoral

El usuario raíz o el técnico empiezan la creación del proceso electoral. La clase Technic invoca el método uploadProcedure(..) de PM_Controller donde se cargan los ficheros necesarios para crear el proceso electoral.

El PM_Controller solicita a la clase ProcedurePM las preguntas del proceso electoral (procedureBallots).

Con toda la información, PM_Controller invoca el método de PM_DB que inserta el proceso en la base de datos.

En caso de que todo vaya bien, se verá por pantalla un mensaje de éxito.

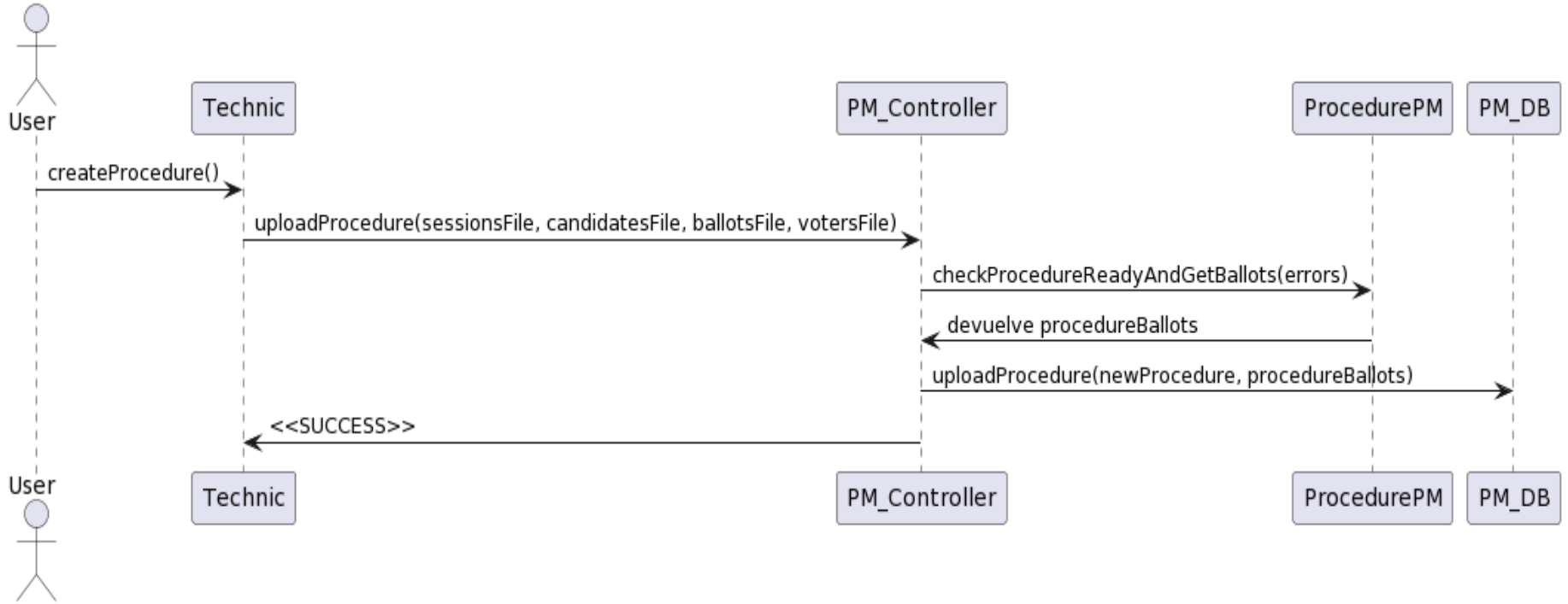

Ilustración 66. Creación de proceso electoral

6.1.1.3 Encuesta

Una vez se muestren en la pantalla los procesos electorales, el supervisor confirma el proceso y si es posible (solo se puede para procesos electorales finalizados) hacer el recuento sobre ese proceso.

Se devuelven los resultados y se muestran en la pantalla principal.

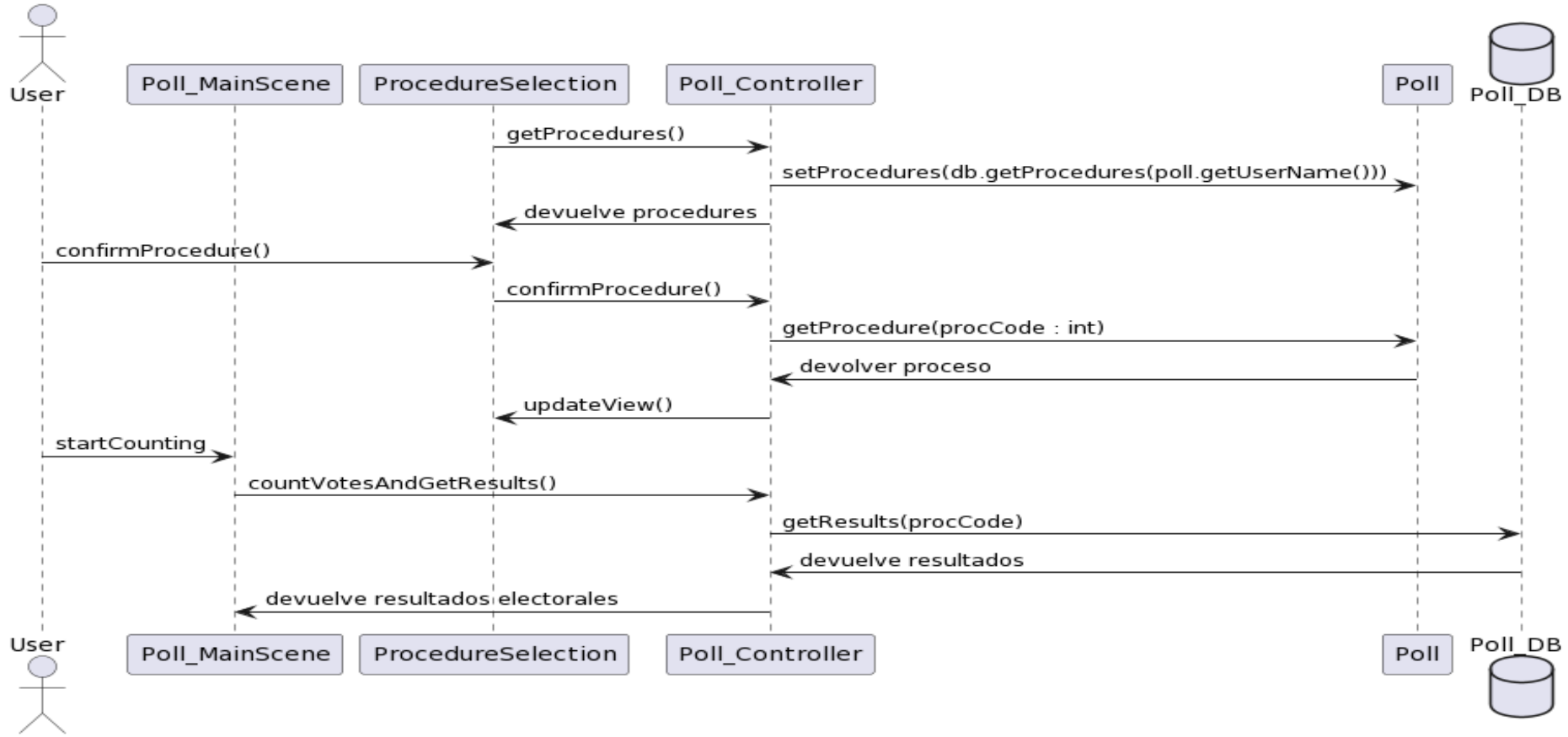

Ilustración 67. Diagrama de Secuencia,Encuesta

Estos son los estados en los que se puede encontrar la urna.
En primer lugar, la urna se encontrará no activa.
Una vez se inicie sesión (login), pasará a estar activa y cuando se seleccione el proceso pasará a estado de conteo.

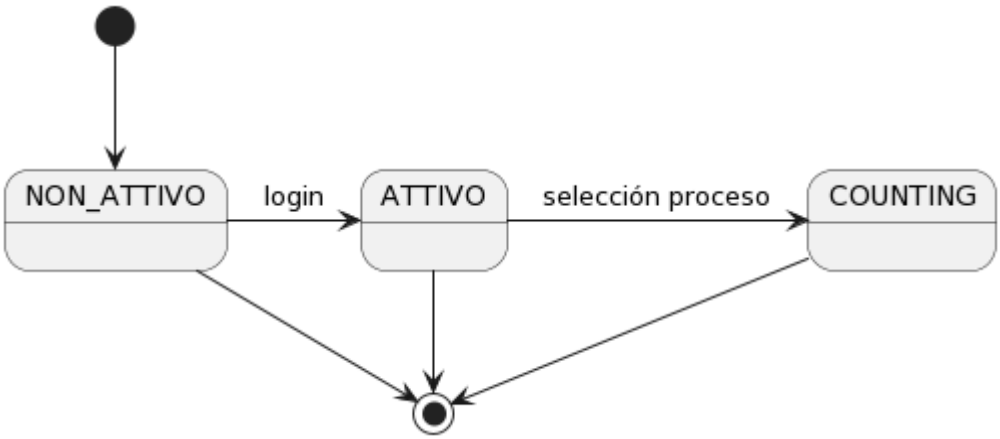

Ilustración 68. Diagramas de estado. Urna

6.1.1.4 Activar Urna

El usuario tiene que confirmar la sesión deseada. Una vez realizado ese paso, se carga la escena principal donde se muestran los mensajes de log que muestran la comunicación entre la urna y los terminales (mesa electoral y puesto de votación).

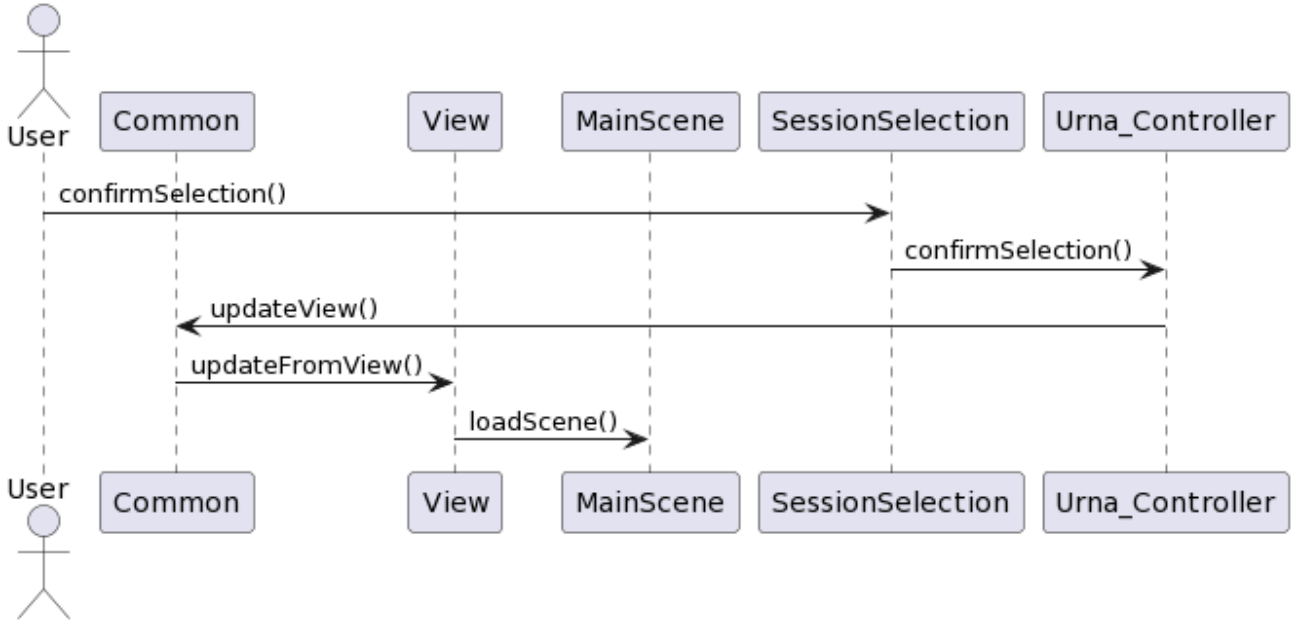

Ilustración 69. Diagrama de estados. Activar urna

6.1.1.5 Votación

El votante tiene que empezar la votación.
Una vez iniciada, la pantalla principal del puesto enseñara uno de los ballots. En cada pantalla habrá un ballot distinto donde el votante podrá mostrar sus preferencias. En cada pantalla hay un botón para avanzar a la siguiente pregunta o para retroceder.
Cuando no queden más preguntas, el votante alcanzará la pantalla de resumen de la votación.
El usuario procederá a enviar la votación.

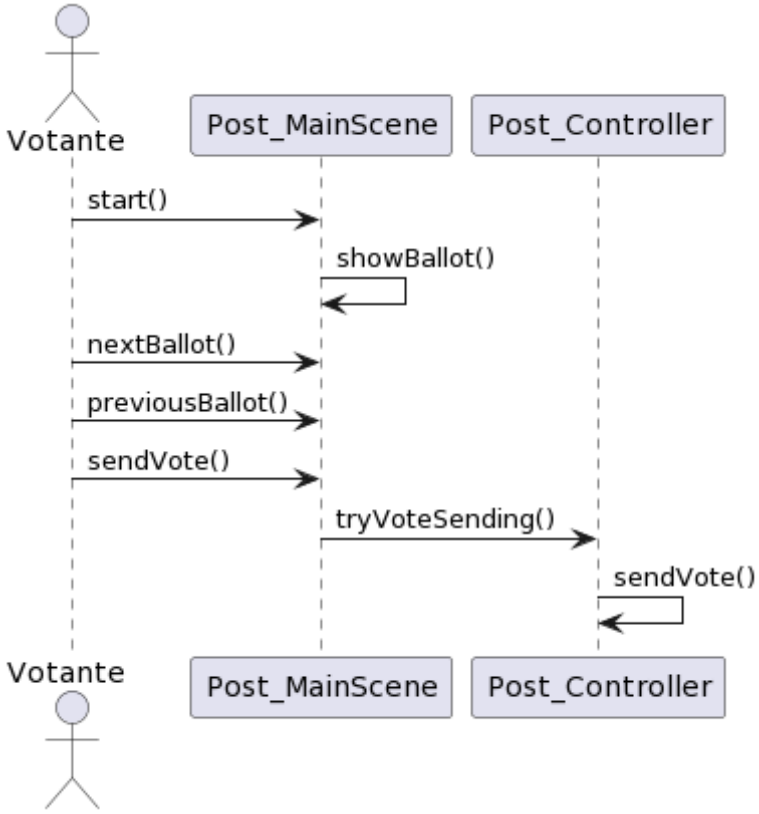

Ilustración 70. Diagrama de secuencia. Votación

6.1.2 Aplicación web

6.1.2.1 Registrar usuario

El usuario se dirige a la pantalla de registro y se carga un formulario de registro donde aparecen los procesos electorales activos.

Rellena el formulario y pulsa el botón de registrar. El sistema realiza las siguientes comprobaciones:

- El proceso electoral no sea nulo.
- El usuario no exista en la base de datos.

Si hay errores no se puede completar el registro, sino se registra el usuario y se dirige a la pantalla de login para que inicie sesión.

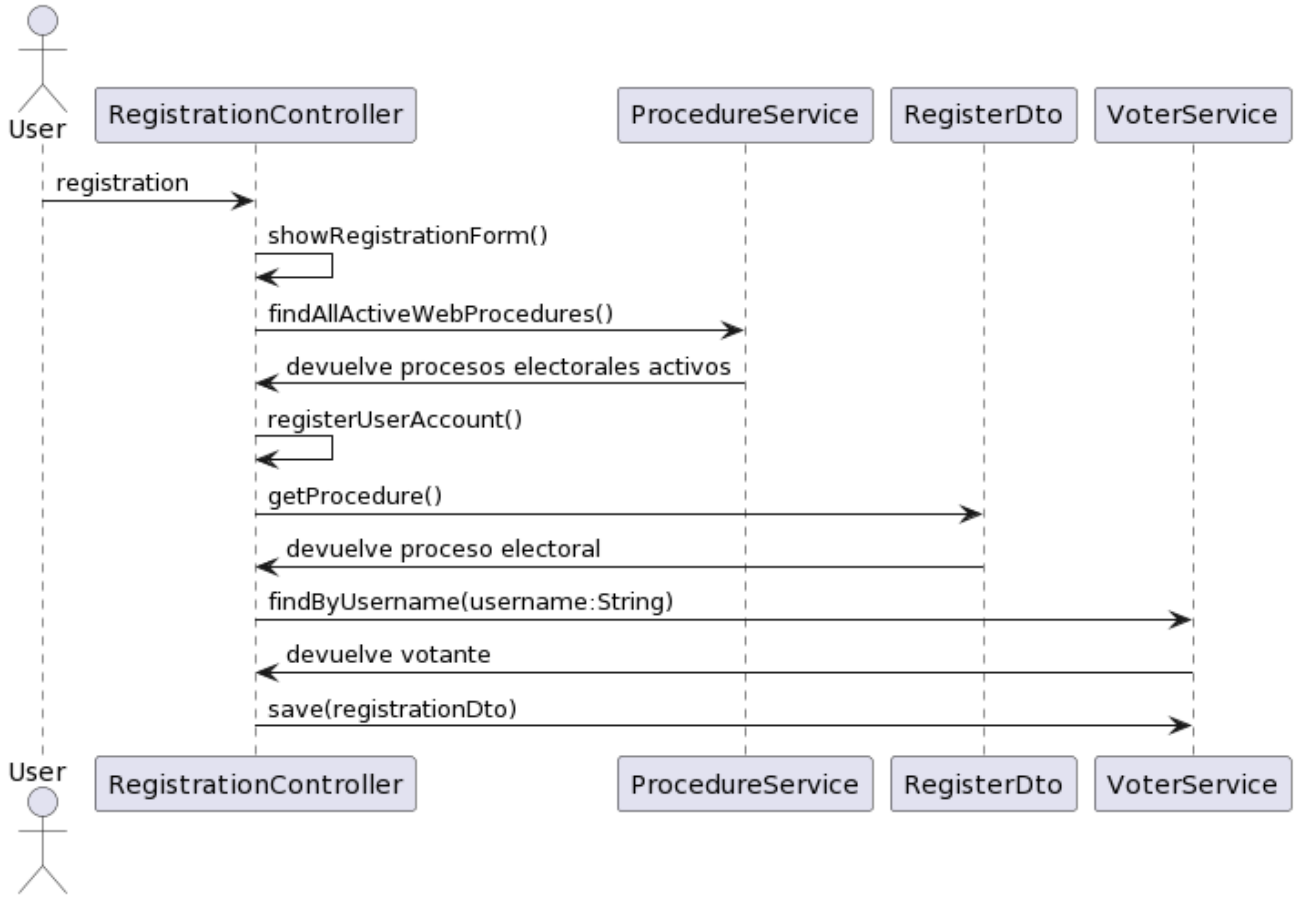

Ilustración 71. Registrar usuario web

6.1.2.2 Votación

6.1.2.2.1 Fase 1

Una vez el votante haya iniciado sesión, el sistema lo redirige a la pantalla de votación, donde se muestra el formulario de votación.

El sistema tiene que hacer una serie de validaciones para comprobar si es correcto:

- El votante no haya votado.
- El proceso no esté cerrado.

Si no se producen errores, el sistema muestra al votante todos los ballots por pantalla.

Se indica en Glosario a que hace referencia "ballot".

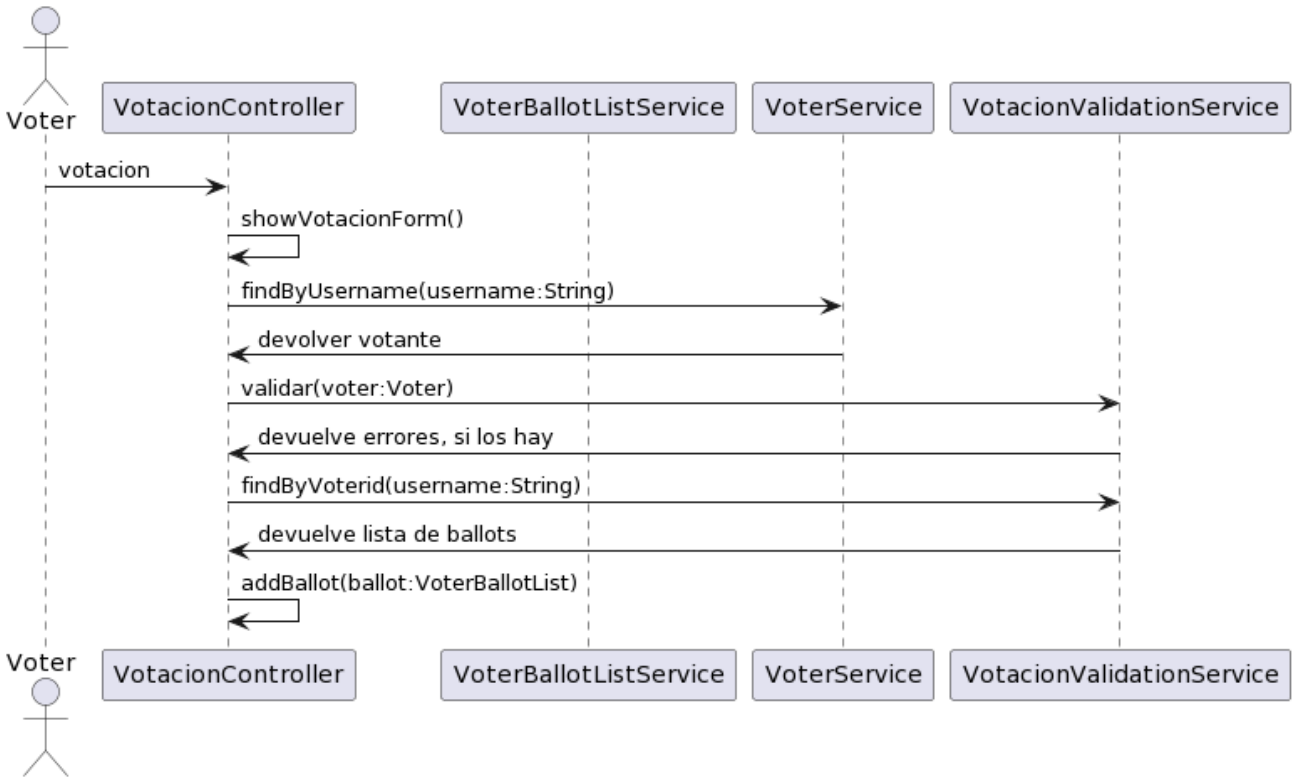

Ilustración 72. Votación web. Fase 1

6.1.2.2.2 Fase 2

Una vez el votante muestre sus preferencias, pulsará el botón de enviar votación.

El sistema debe comprobar que para aquellas preguntas donde haya un número de opciones a escoger, el usuario no haya escogido más de las permitidas.

Si todo es correcto, los votos se almacenan en la base de datos.

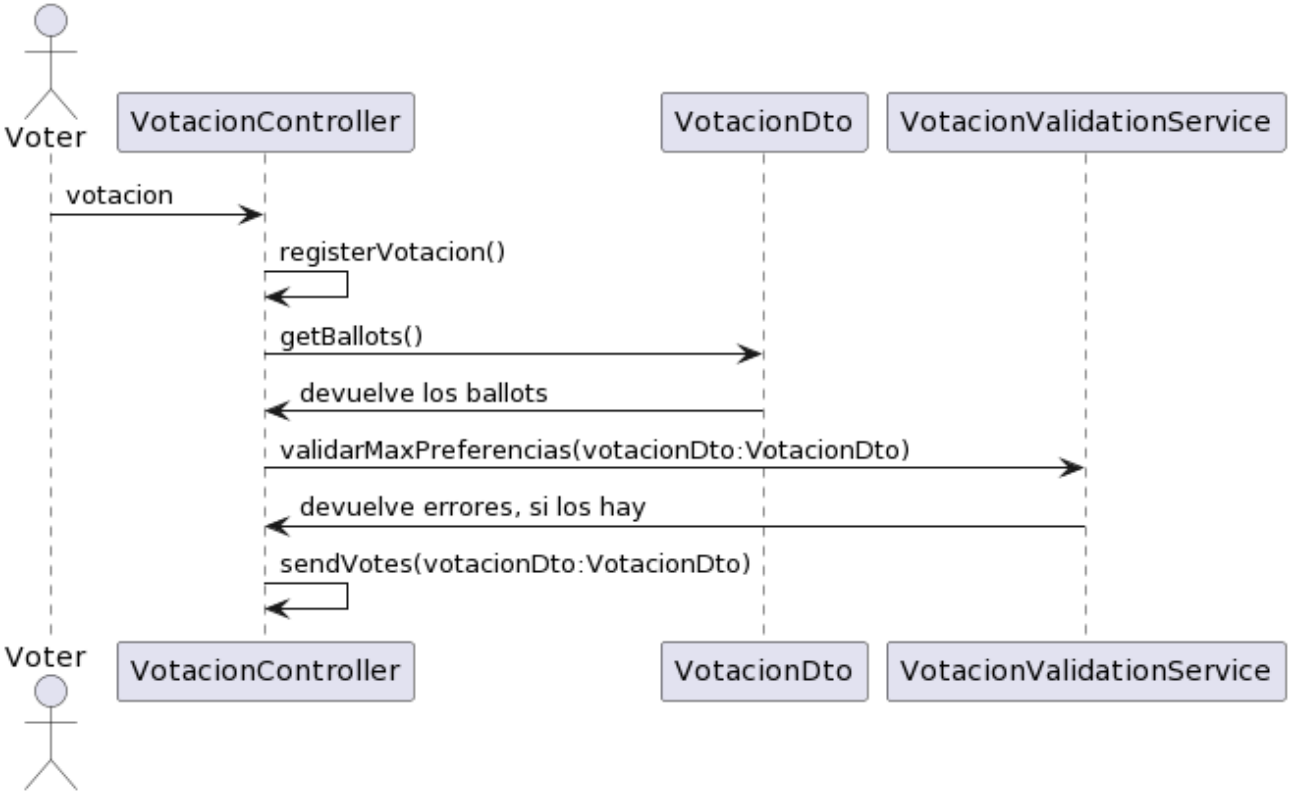

Ilustración 73. Votación web. Fase 2

6.2 Diseño de Clases

6.2.1 Aplicación de escritorio

6.2.1.1 Proceso electoral

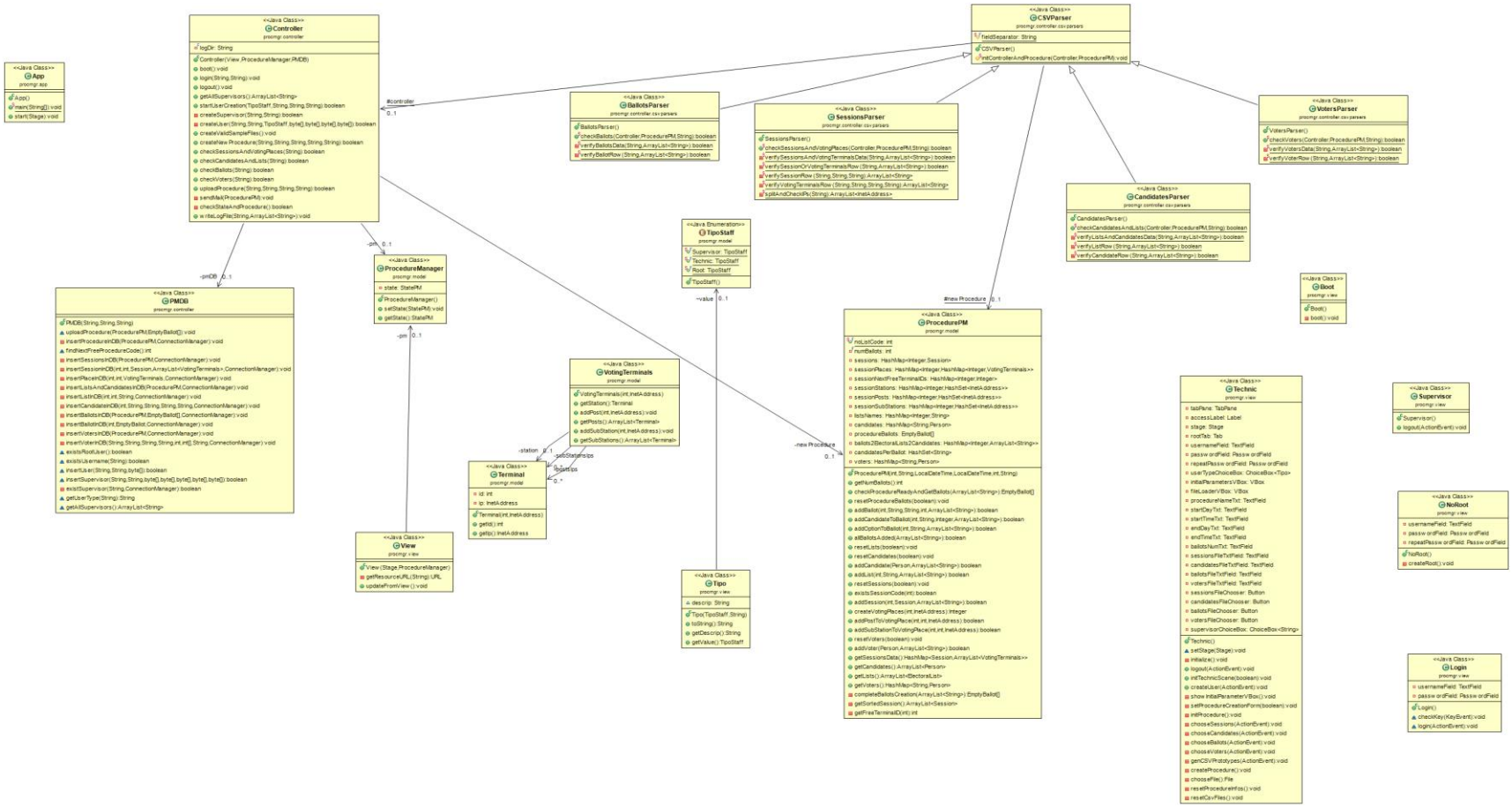

Ilustración 74. Proceso electoral

6.2.1.2 Encuesta

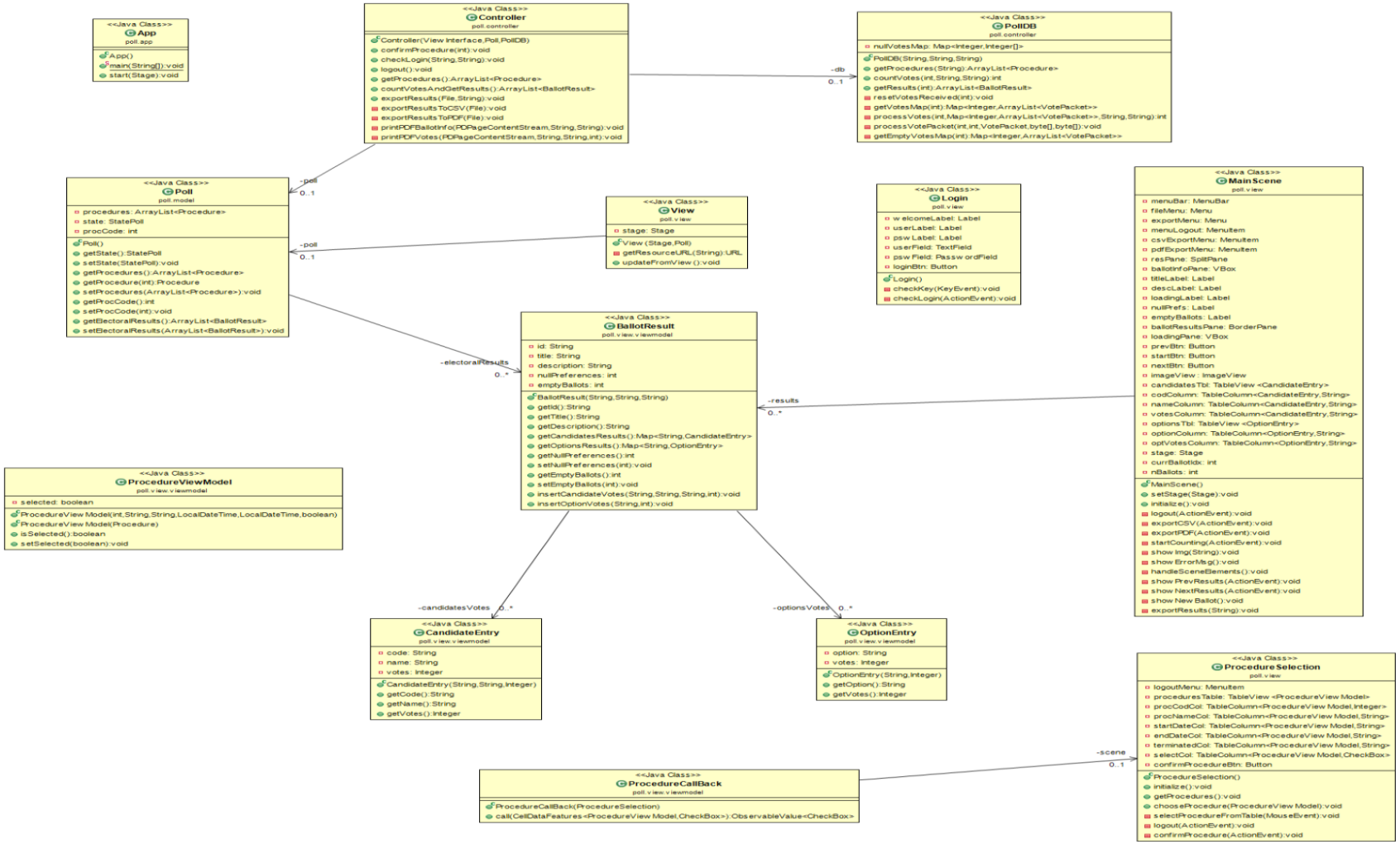

Ilustración 75. Encuesta

6.2.1.3 Urna

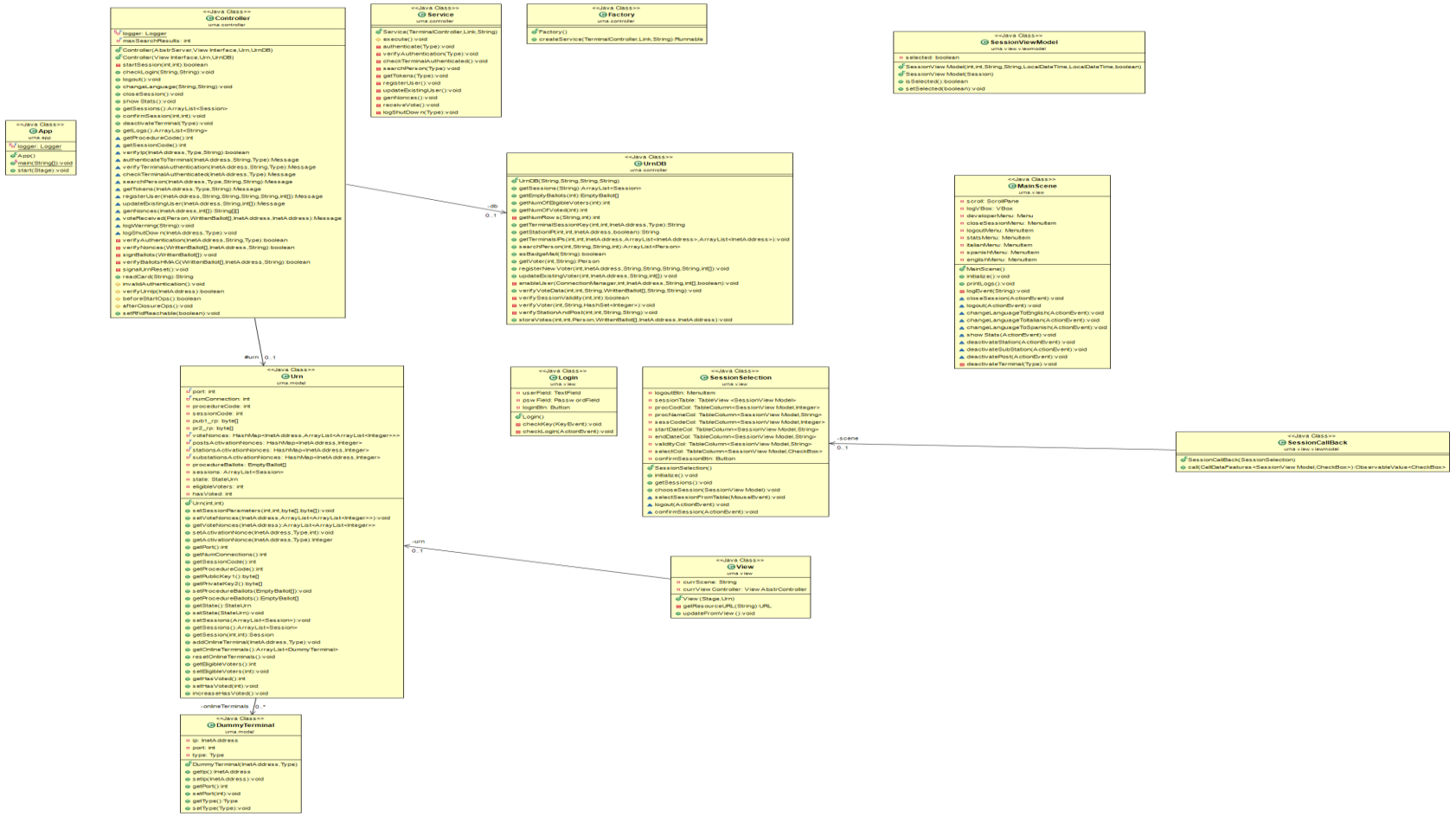

Ilustración 76. Urna

6.2.1.4 Mesa electoral

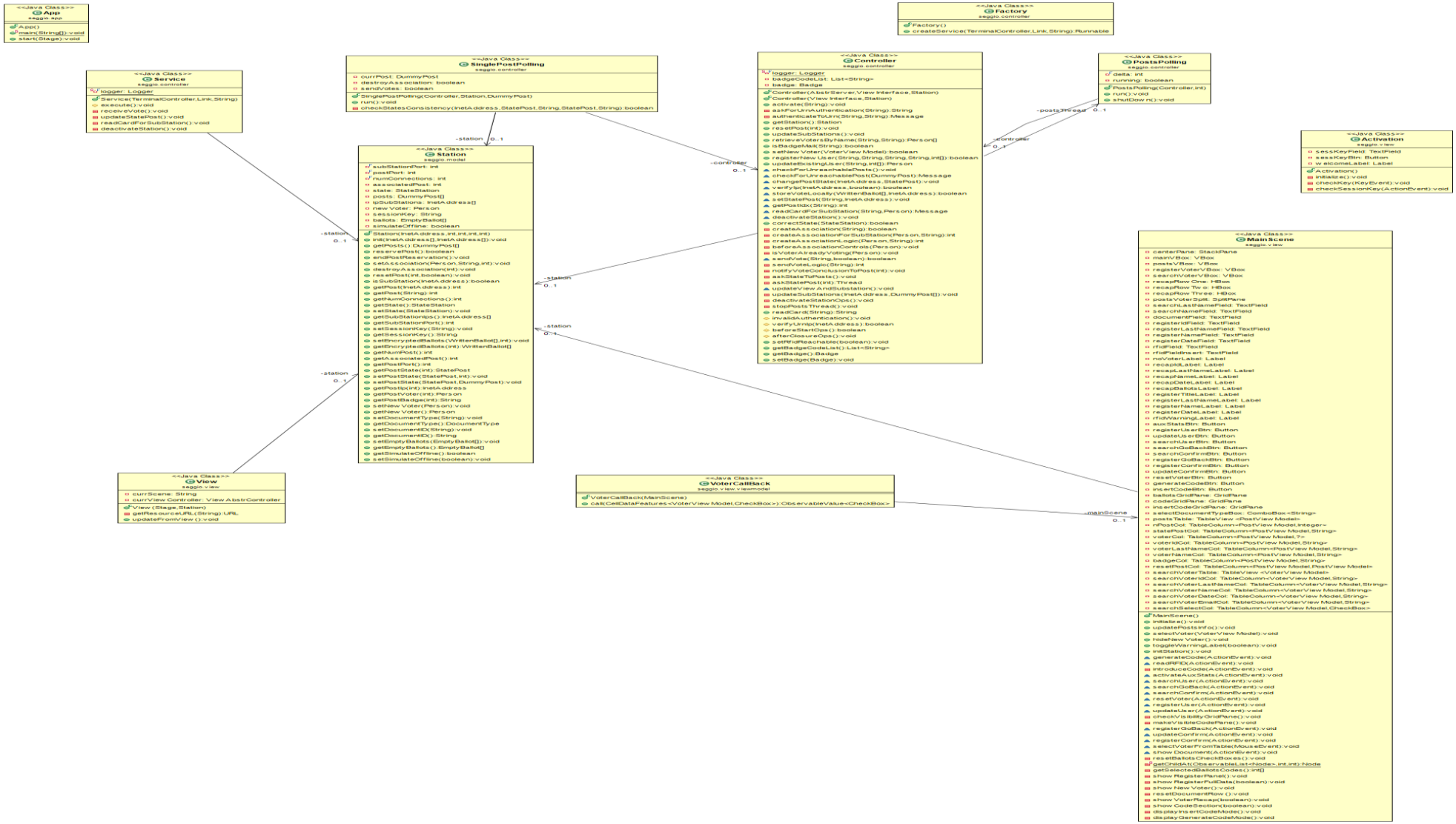

Ilustración 77. Mesa electoral

6.2.1.5 Puesto de votación

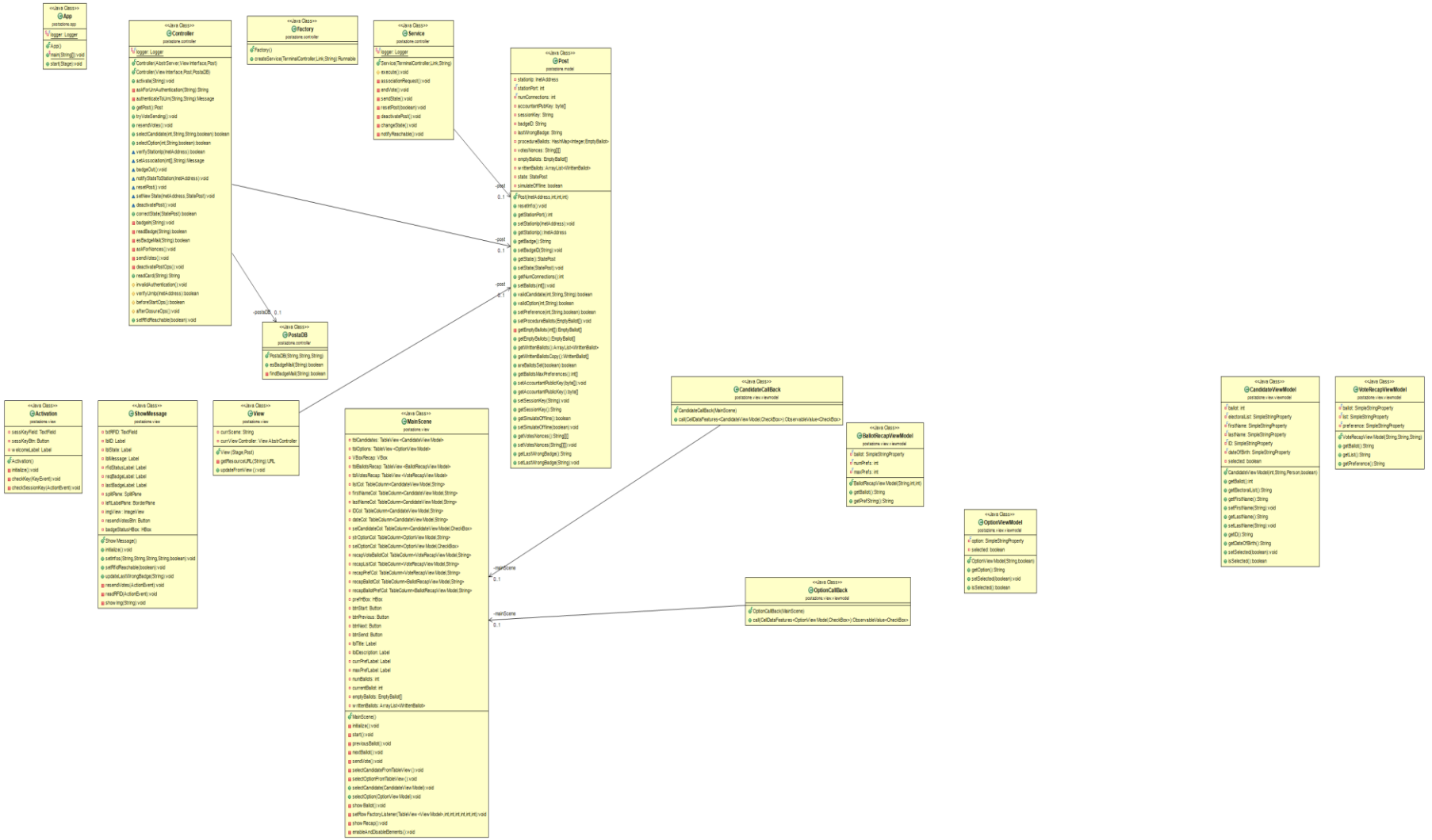

Ilustración 78. Puesto de votación

6.2.2 Aplicación web

6.2.2.1 Votación

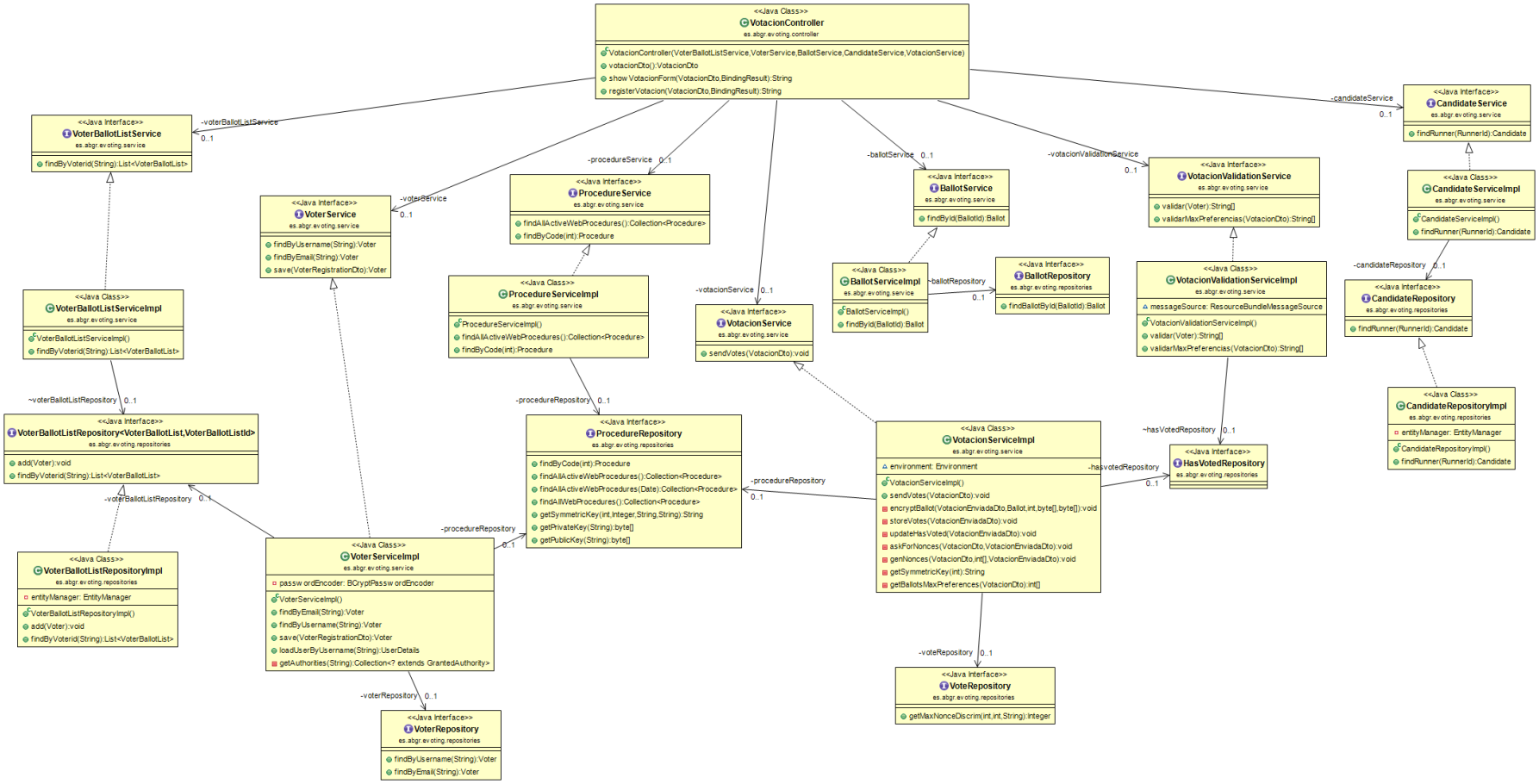

Ilustración 79. Diagrama clases. Votación web

6.2.2.2 Registro

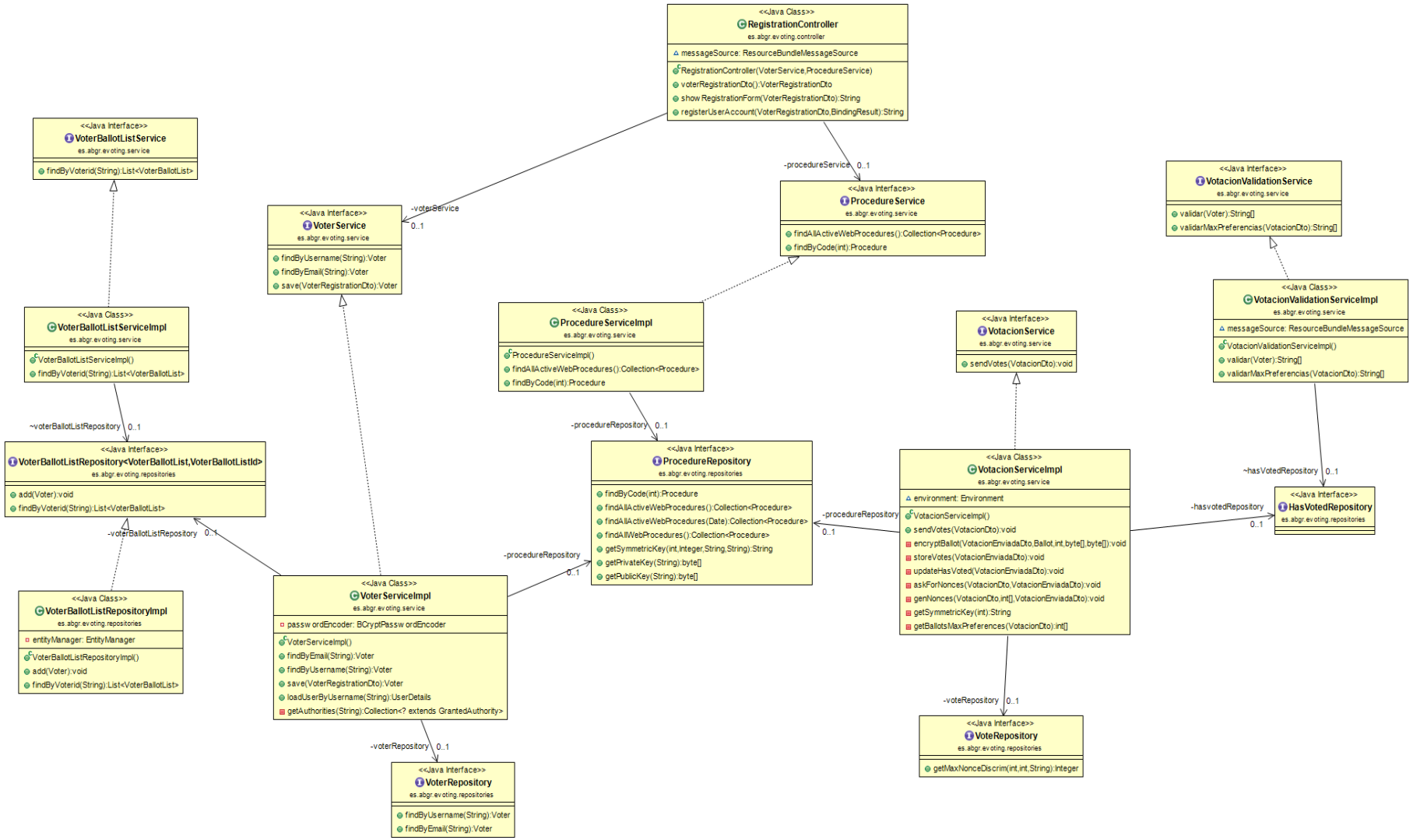

Ilustración 80. Diagrama clases. Registro web

6.3 Diseño de la Arquitectura de Módulos del Sistema

6.3.1 Diagrama de paquetes

6.3.1.1 Aplicación de escritorio

A continuación, se muestra el diagrama de paquetes de la aplicación de escritorio.

En el diagrama que se presenta, se encuentra los módulos Poll, Seggio, Urna, PM y Posta y Common.

El módulo Poll, es el encargado de realizar el recuento de la votación.

Seggio, es la mesa electoral utilizada para la gestión de la votación.

Urna, es la encargada de hacer que el Seggio y la Posta se comuniquen.

PM, es el administrador del proceso electoral.

Posta, se utiliza para que el votante realice la votación.

Common, es el módulo de utilidades común para los demás módulos.

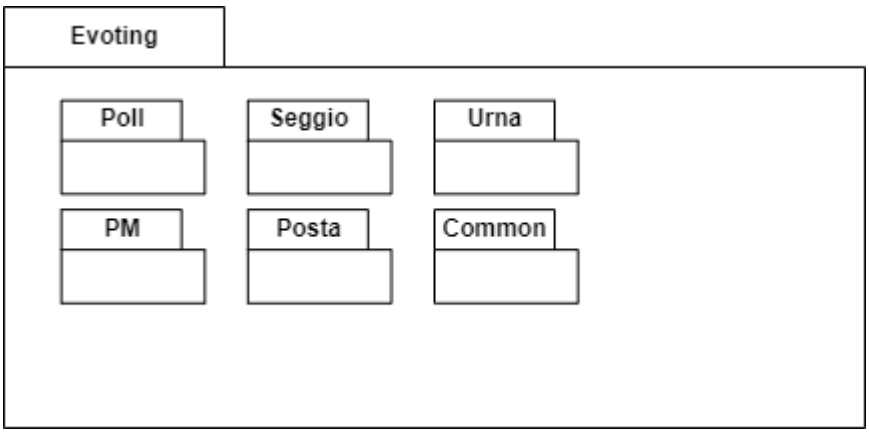

Ilustración 81. Evoting. Package diagram

Todos los módulos que hemos mencionado utilizan el patrón de arquitectura software MVC.

El modelo define la estructura de los datos, el controlador contiene la lógica de negocio y la vista donde que define la visualización.

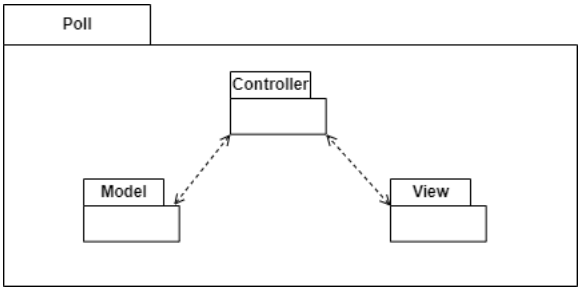

Ilustración 82. Subpackage diagram

6.3.1.2 Aplicación web

La aplicación web también hace uso del patrón de arquitectura MVC.

En primer lugar, distinguimos la capa “Model” compuesta por los paquetes repositorios y modelos.

La capa “Controller” interactúa con “Model” y a su vez con la capa “View” donde se encuentran las templates.

Por otro lado, diferenciamos el paquete “Config” para definir la configurar del sistema, como por ejemplo la seguridad.

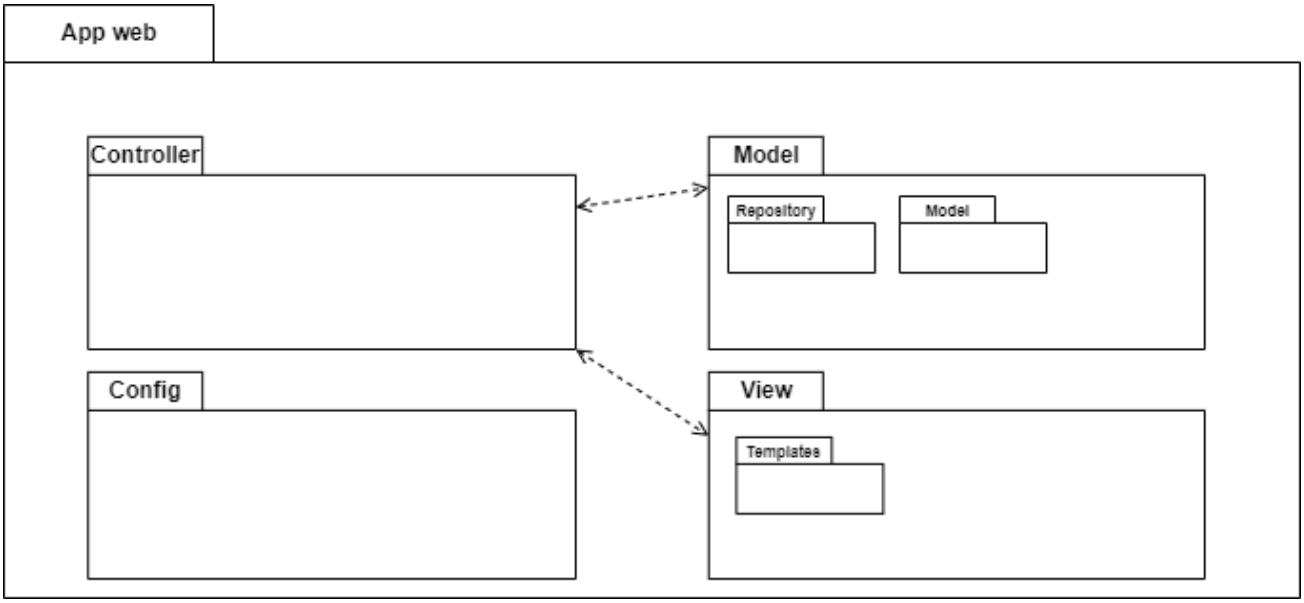

Ilustración 83. Diagrama de paquetes aplicación web

6.4 DISEÑO FÍSICO DE DATOS

6.4.1 Descripción del SGBD Usado

Para iniciar el proceso de integración de una base de datos MySQL es necesario tener disponible un servidor de base de datos apropiado con una versión funcional de este DBMS, en nuestro caso utilizamos MySQL Workbench 8.0.

Tanto la aplicación de escritorio como la web utilizan la misma base de datos y el mismo modelo E-R.

En la aplicación de escritorio, el acceso a la base de datos se hace utilizando JDBC.

En la aplicación web se han mapeado las tablas necesarias a objetos utilizando Spring Data JPA e implementando repositorios que permiten simplificar el acceso a la base de datos.

El diseño de base de datos utilizado es el de la aplicación original extraído del código de acceso a base de datos encontrado en la aplicación ya que no se disponía de un esquema de base de datos. A este diseño se añadieron relaciones entre tablas y claves primarias siendo conscientes de que puede realizarse un proceso profundo de mejora en futuras ampliaciones del prototipo.

Para el desarrollo de la aplicación web se han modificado algunas tablas añadiendo columnas que resultaban necesarias.

6.4.1.1 Diagrama E-R

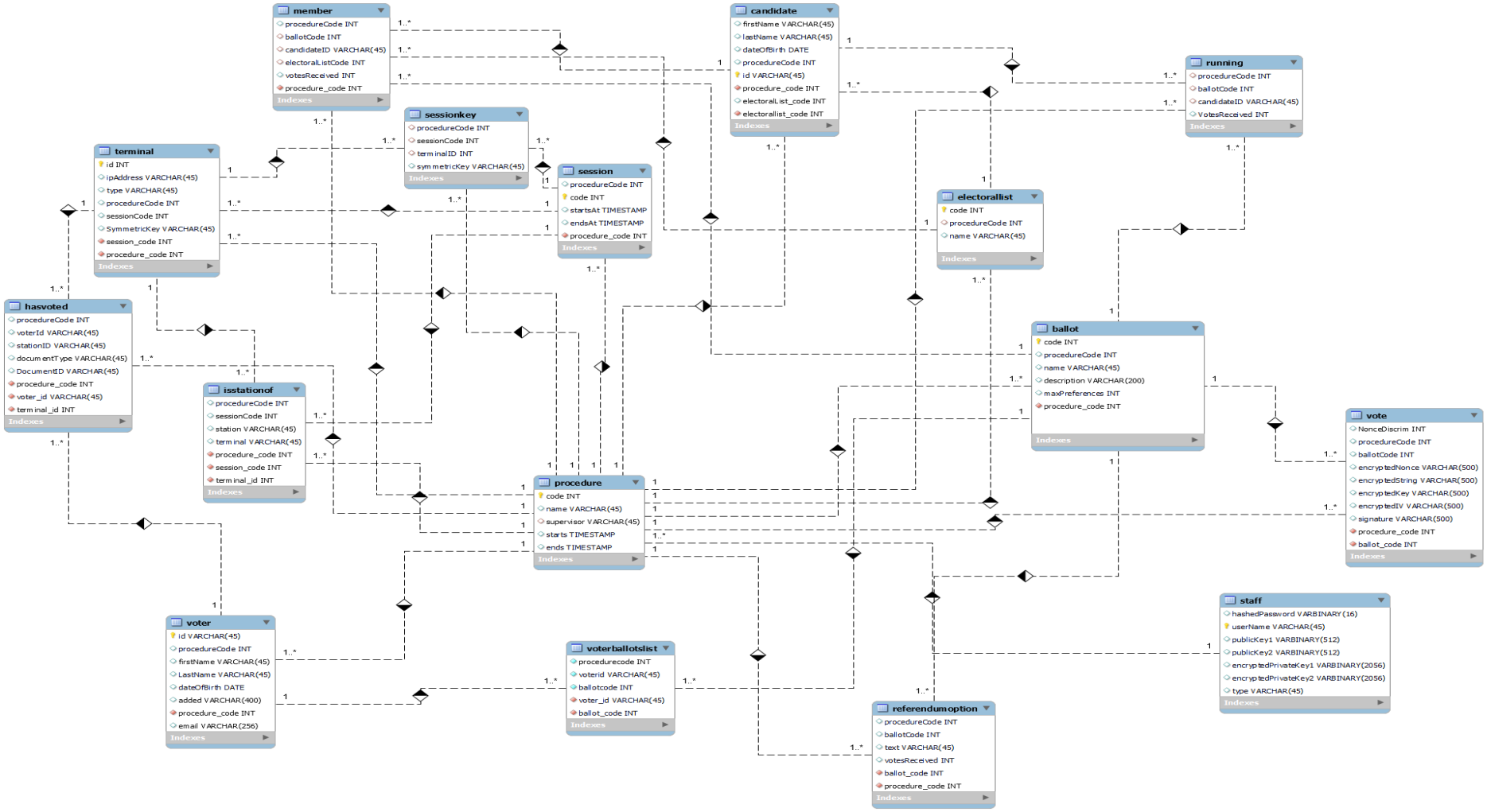

Ilustración 84. Diagrama E-R

6.4.1.2 Modelos de la aplicación web

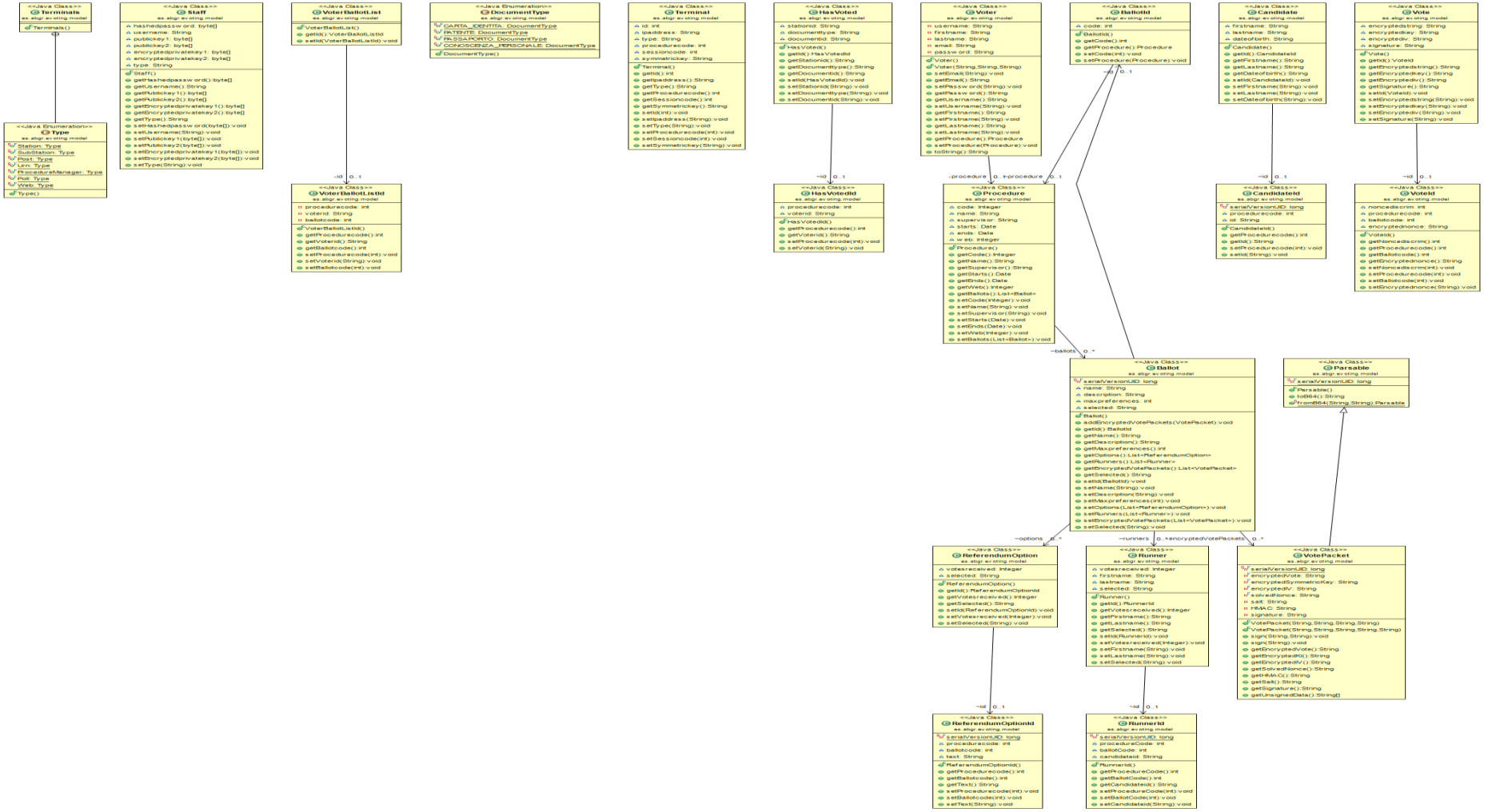

Ilustración 85. Modelos

6.5 CARGA INICIAL DE DATOS

6.5.1.1 Candidatos y listas electorales

```
#C; Código Candidato; Nombre; Apellido; Fecha de Nacimiento (Formato:
dd/mm/aaaa o NULL)
#L; Código Lista; Nombre


# EJEMPLO
#C; ABC00; Nombre1; Apellido1; 01/01/1970
#C; ABC01; Nombre2; Apellido2; 01/01/1970
#C; CF314; Pi; Greco; 14/03/1970
#L; Nombre Lista Electoral
#-----------------------------------------------------


C; A101; Javier; Bardem; 01/03/1969
C; A102; Luis; Tosar; 13/10/1971
C; A103; Javier; Cámara; 19/01/1967
C; A104; Antonio; de la Torre; 18/01/1968
C; A105; Eduard; Fernández; 25/08/1964
#-----------------------------------------------------
C; C111; Taylor; Swift; 13/12/1989
C; C112; Dua; Lipa; 22/08/1995
C; C113; Billie; Eilish; 18/12/2001
C; C114; Amy; Winehouse; 14/09/1983
C; C115; Katy; Perry; 25/10/1984
#-----------------------------------------------------
C; G121; The Beatles;;01/01/1960
C; G122; The Rolling Stones;;01/01/1962
C; G123; U2;;01/01/1976
C; G124; Queen;;01/01/1970
C; G125; Dire Straits;;01/01/1977
#-----------------------------------------------------
```

```
C; P131; Francisco; Goya; 01/10/2022
C; P132; Diego; Velazquez; 01/01/2022
C; P133; Pablo; Picasso; 01/01/2022
C; P134; Salvador; Dalí; 01/01/2022
C; P135; Joaquín; Sorolla; 01/01/2022
```

6.5.1.2 Plantilla de sesión

```
#SESIONES Y TERMINALES
#Código de sesión (temporal); Timestamp Inicio (Formato: dd/mm/aaa
hh:mm:ss); Timestamp Fin
#Código de Sesión; IP Asiento; IP Puesto 1 : ... : IP Puesto N; IP
Asiento Auxiliar 1 : ... : IP Asiento Auxiliar N


# EJEMPLO
#1; 01/01/2020 00:00:01; 31/12/2020 23:59:59
1; 192.168.1.1; 192.168.1.2 : 192.168.1.3; 192.168.1.3 : 192.168.1.4;
1; 192.168.1.25; 192.168.1.26; 192.168.1.27
#-----------------------------------------------------
1; 01/05/2022 00:00:01; 31/09/2022 23:59:59
1; 127.0.0.1; 127.0.0.1; 127.0.0.1
```

6.5.1.3 Plantilla de votantes

```
#VOTANTES
#ID Votante; Nombre; Apellido; Código Tarjeta 1, ..., Código Tarjeta N;
Fecha de Nacimiento (Formato: dd/mm/aaaa o NULL)


# EJEMPLO
#ABC00; Nombre1; Apellido1; 1,2; 01/01/1970
#ABC01; Nombre2; Apellido2; 3; NULL
#CF314; Pi; Griego; 1,3; 14/03/1970
#-----------------------------------------------------
VOT01;Albert;Espinosa; ; 1,2,3,4,5,6,7,8,9; 01/01/1970
```

```
VOT02;Sara;Mesa; ;1,2,3,4,5,6,7,8,9; 01/01/1972
VOT03;Eloy;Moreno; ; 10,11,12,13; 01/01/1974
VOT04;Dolores;Redondo; ; 10,11,12,13; 01/01/1976
```

6.5.1.4 Preguntas

```
# TARJETAS
#C; Código; Título; Descripción; Num. Preferencias; Cod. Candidato 1 [: Cod. Lista]; [...] ; Cod. Candidato N [: Cod. Lista]
#O; Código; Título; Descripción; Num. Preferencias; Opción 1; [...] ; Opción N


# EJEMPLO
#C; 1; Scheda 1; Scheda 1; 3; ABC00; ABC01 : 1; ABC02 : 2
#C; 2; Scheda 2; Descrizione; 1; CF314 : 3
#O; 3; Scheda 3; Referendum; 1; Sì; No
#-----------------------------------------------------
#Preguntas de opciones 1 maximo eligible
#-----------------------------------------------------
O; 1; ORGANIZACION 1; El curso ha estado bien organizado; 1; PESIMO; MALO; BIEN; OPTIMO
O; 2; ORGANIZACION 2; El num. de alumnos ha sido adecuado; 1; PESIMO; MALO; BIEN; OPTIMO
O; 3; Tiempo 1; Tiempo suficiente; 1; PESIMO; MALO; BIEN; OPTIMO
O; 4; Tiempo 2; Horario adecuado; 1; PESIMO; MALO; BIEN; OPTIMO
O; 5; Instalaciones 1; Aula apropiada; 1; PESIMO; MALO; BIEN; OPTIMO
O; 6; Instalaciones 2; Medios adecuados; 1; PESIMO; MALO; BIEN; OPTIMO
#-----------------------------------------------------
#Preguntas de opciones >1 maximo eligible
#-----------------------------------------------------
O; 7; Cursos 1; Marque los cursos en los que ha participado; 3; Gestion de tramites; Liderazgo; Hablar en publico; Marketing
O; 8; Cursos 2; Desde que lugar asistes al curso; 2; Oficina; Casa
```

```
O; 9; Cine 1; Elija sus 3 preferidas; 3; Forrest Gump; About Time; Little Miss Sunshine; Seven; El amor en su lugar

#----------------------------------------------------

#Candidatos, 1 maximo

#----------------------------------------------------

C; 10; Actor favorito; Elija su actor favorito; 1; A101; A102; A103; A104; A105

C; 11; Cantante preferida; Elija su cantante favorita; 1; C111; C112; C113; C114; C115

#----------------------------------------------------

#Candidatos, >1 maximo

#----------------------------------------------------

C; 12; Grupo de rock preferido; Elija los 3 grupos de rock mas representativos; 3; G121; G122; G123; G124; G125

C; 13; Pintor preferido; Seleccione sus 2 pintores favoritos; 2; P131; P132; P133; P134; P135
```

6.5.1.5 Terminales

Se deben insertar en la base de datos, lo siguientes datos para la puesta a punto de los terminales:

```
LOCK TABLES `terminal` WRITE;

INSERT INTO `terminal` VALUES (1,'127.0.0.1','Station',1,1,'QT1WNUR17FKVQW55VX1EQL2WRGG4NDJZ'),(2,'127.0.0.1','Post',1,1,'AGM549UR7JUSPUYSX2A5ERD4RZ53RL8S'),(3,'web','Web',1,1,'AGM549UR7JUSPUYSX2A5ERD4RZ53RL8S');

LOCK TABLES `isstationof` WRITE;

INSERT INTO `isstationof` VALUES (1,1,'1','2');

LOCK TABLES `sessionkey` WRITE;

INSERT INTO `sessionkey` VALUES (1,1,1,'QT1WNUR17FKVQW55VX1EQL2WRGG4NDJZ'),(1,1,2,'AGM549UR7JUSPUYSX2A5ERD4RZ53RL8S');

UNLOCK TABLES;
```

6.6 ESPECIFICACIÓN TÉCNICA DEL PLAN DE PRUEBAS

6.6.1 Aplicación de escritorio

En esta sección, se detalla el proceso de ejecución de las pruebas.

6.6.1.1 Pruebas unitarias

Para realizar las pruebas unitarias se debe realizar una configuración previa.

1. Leer los archivos psws.cfg, las claves keystore.jks y truststore.jks

```
System.setProperty("javax.net.ssl.keyStore", "ssl/keystore.jks");
System.setProperty("javax.net.ssl.keyStorePassword", CfgManager.getPassword("ks"));


System.setProperty("javax.net.ssl.trustStore", "ssl/truststore.jks");
System.setProperty("javax.net.ssl.trustStorePassword", CfgManager.getPassword("ts"));
```

2. Vaciar la base de datos actual.
3. Generar una base de datos realizando las siguientes inserciones:
    - Supervisor
    - Root
    - Proceso electoral
    - Votante
    - Preguntas

4. Se debe crear la base de datos de la urna.

```
UrnDB uDB = new UrnDB(host, port, schema, "Test");
```

Donde host es “localhost”, port “3306”, schema “SecureBallot” y “Test”, el nombre del terminal.

5. Se crean los ballots:

```
WrittenBallot wb0 = new WrittenBallot("Votable Ballot", 0, 1);
WrittenBallot wb1 = new WrittenBallot("Non Votable Ballot", 1, 1);
// WrittenBallot(título código de ballot, opcionas máximos a escoger)


WrittenBallot[] wbs0 = { wb0 }; //array de ballots
```

6. Ip Station e Ip Post

```
InetAddress ipStation = InetAddress.getByName("127.0.0.1");

InetAddress ipPost = InetAddress.getByName("127.0.0.2");
```

7. Código de proceso y de sesión.

```
int procedureCode = 0;
int sessionCode = 0;
```

A continuación, muestro el método utilizado para los tests:

```
public void verifyVoteData(int procedureCode, int sessionCode, String voterID,
        WrittenBallot[] ballots, String ipStation, String ipPost) throws PEException
{
        if (verifySessionValidity(procedureCode, sessionCode)) { //Verificar si la sesión
                es válida

                HashSet<Integer> ballotCodes = new HashSet<>();
                for (WrittenBallot ballot : ballots)
                {
                        ballotCodes.add(ballot.getCode());
                }

                verifyVoter(procedureCode, voterID, ballotCodes); //Verificar si el
                        votante es válido
        }

        verifyStationAndPost(procedureCode, sessionCode, ipStation, ipPost); //Verificar
                los terminales
}
```

Prueba 01 – Votación sin sesión

Se necesita UrnDB, WrittenBallot[], ipStation, ipPost, procedureCode, **sessionCode**, fakeID, fail.
 	
`uDB.verifyVoteData(procedureCode, sessionCode, fakeID, wbs0, ipStation.getHostAddress(), ipPost.getHostAddress());`
 	
Falla en el siguiente método:
`verifySessionValidity(procedureCode, sessionCode)`
 	
Pues no se encuentra una sesión con el código sessionCode.

Tabla 100. Especificación Técnica. Votación sin sesión

Prueba 02 – Votación sin votante

Para la siguiente prueba se inserta la sesión para el proceso electoral:
 	
`insertSessionInRealDB(procedureCode, sessionCode);`
 	
Se necesita UrnDB, WrittenBallot[], ipStation, ipPost, procedureCode, sessionCode, **fakeID**, fail.
 	
`uDB.verifyVoteData(procedureCode, sessionCode, fakeID, wbs0, ipStation.getHostAddress(),ipPost.getHostAddress());`
 	
Falla en el siguiente método:
`verifyVoter(procedureCode, voterID, ballotCodes);`
 	
Pues no se encuentra un votante con el código voterID.

Tabla 101. Especificación Técnica. Votación sin votante

Prueba 03 – Votación sin terminal (mesa electoral)

Se necesita UrnDB, WrittenBallot[], **ipStation**, ipPost, procedureCode, sessionCode, fail.
 	
`uDB.verifyVoteData(procedureCode, sessionCode, voterTest.getID(), wbs0, ipStation.getHostAddress(),ipPost.getHostAddress());`
 	
Falla en el siguiente método:
`verifyStationAndPost(procedureCode, sessionCode, ipStation, ipPost);`
 	
Pues no se encuentra la ipStation que se pasa.
 	
Una vez acabado esta prueba, se añaden los terminales en la base de datos:
`insertTerminalsInRealDB(procedureCode, sessionCode, 0, ipStation, ipPost);`

Tabla 102. Especificación Técnica. Votación sin mesa electoral

Prueba 04 – Terminales no coincide

Para esta prueba se necesitan dos nuevos terminales:
 	
`InetAddress ipSecondStation = InetAddress.getByName("127.0.0.3");`
`InetAddress ipSecondPost = InetAddress.getByName("127.0.0.4");`
 	
Se comprueba que ipStation e ipPost no son iguales que ipSecondStation e ipSecondPost respectivamente.

Tabla 103. Especificación Técnica. Terminales no coincide

Prueba 05 – Votación sin terminal (puesto)

Se necesita UrnDB, WrittenBallot[], ipStation, procedureCode, sessionCode, fail, **ipSecondPost**.
 	
`DB.verifyVoteData(procedureCode, sessionCode, voterTest.getID(), wbs0, ipStation.getHostAddress(),`**`ipSecondPost.getHostAddress()`**`);`
 	
Falla en el siguiente método:
`verifyStationAndPost(procedureCode, sessionCode, ipStation,` **`ipPost`**`);`
 	
Pues no se encuentra la ipPost que se pasa.

Tabla 104. Especificación Técnica. Votación sin puesto

Prueba 06 – Puesto de votación no válido para mesa electoral

Para la siguiente prueba, se necesitar realizar la siguiente inserción en la base de datos:
`insertTerminalsInRealDB(procedureCode, sessionCode, 2, ipSecondStation, ipSecondPost);`
 	
Se necesita UrnDB, WrittenBallot[], ipStation, procedureCode, sessionCode, fail, ipSecondPost.
 	
`DB.verifyVoteData(procedureCode, sessionCode, voterTest.getID(), wbs0, ipStation.getHostAddress(),ipSecondPost.getHostAddress());`
 	
Falla en el siguiente método:
`verifyStationAndPost(procedureCode, sessionCode, ipStation, ipPost);`
 	
Pues ipStation e ipPost no son compatibles.

Tabla 105. . Especificación Técnica. Puesto votación no válido para mesa

Prueba 07 – Incoherencia pregunta asignada al votante

Para la siguiente prueba, se necesita:
 	
`Person voterTest = new Person ("voter", "test", "VT00", null, false);`
`WrittenBallot[] wbs1 = { wb1 };`
 	
Se necesita UrnDB, ipStation, ipPost, procedureCode, sessionCode, voterTest, wbs1.
 	
`DB.verifyVoteData(procedureCode, sessionCode, voterTest.getID(), wbs1, ipStation.getHostAddress(),ipSecondPost.getHostAddress());`
 	
Falla en el siguiente método:
`verifyVoter(procedureCode, voterID, ballotCodes);`
 	
Falla porque el votante no tiene asignadas las preguntas wbs1.

Tabla 106. Especificación Técnica. Incoherencia pregunta

Prueba 08 – Votante ya ha votado

Para la siguiente prueba, se necesita:
 	
`DB.verifyVoteData(procedureCode, sessionCode, voterTest.getID(), wbs0, ipStation.getHostAddress(), ipPost.getHostAddress());`
 	
`voterTest.setDocumentType("Conoscenza Personale");`
`uDB.storeVotes(procedureCode, sessionCode, voterTest, wbs0, ipStation, ipPost);`
 	
Se necesita UrnDB, wbs0, ipStation, ipPost, procedureCode, sessionCode, fail, voterTest, res.
 	
`DB.verifyVoteData(procedureCode, sessionCode, voterTest.getID(), wbs1, ipStation.getHostAddress(),ipSecondPost.getHostAddress());`
 	
Falla en el siguiente método:
`verifyVoter(procedureCode, voterID, ballotCodes);`
 	
Falla porque el votante ya ha votado.

Tabla 107. . Especificación Técnica. Votante ya ha votado

6.6.1.2 Pruebas de integración

Prueba 09 – Se conecta la urna con los terminales (mesa electoral y puesto)
Mensajes intercambiados: Seggio: Protocol.StationAuthenticationPhase1 • Protocol.PostAuthenticationPhase1 • Protocol.validAuthentication Protocol.StationAuthenticationPhase2 • Protocol.validAuthentication Post: Protocol.PostAuthenticationPhase1 • Protocol.PostAuthenticationPhase1 • Protocol.validAuthentication Protocol.PostAuthenticationPhase2

Tabla 108. Especificación Técnica. Se conecta la urna

Prueba 10 – Se realiza votación
Mensajes intercambiados: Protocol.searchPersonReq Protocol.searchPersonAck Protocol.getTokensReq Protocol.tokensAck Protocol.nonceReq Protocol.nonceAck Protocol.sendVoteToUrn Protocol.votesReceivedAck

Tabla 109. Especificación Técnica. Se realiza votación

6.6.2 Aplicación web

Prueba 11 – Buscar una pregunta por ID
Esta prueba consiste en: • Crear un identificador de ballot. • Asignarle un código • Asignarle un proceso electoral. • Por último, se comprueba que existe un ballot con el identificador que hemos creado. Se espera que el test encuentre el ballot.

Ilustración 86. Especificación Técnica. Buscar pregunta por ID

Prueba 12 – Comprobar el número de preguntas
Esta prueba consiste en: • Buscar en el repositorio de ballots, todos ellos. Se espera que número de ballots sea el que estábamos esperando.

Tabla 110. Especificación Técnica.Comprobar número de preguntas

Prueba 13 – Buscar una pregunta por ID inválido
Esta prueba consiste en: • Crear un identificador de ballot. • Asignarle un código • Asignarle un proceso electoral. • Por último, se comprueba que existe un ballot con el identificador que hemos creado. No se espera que la prueba encuentre el ballot.

Tabla 111. Especificación Técnica.Buscar una pregunta por ID inválido

Prueba 14 – Encontrar procesos activos
Esta prueba consiste en: • Crear proceso electoral • Asignarle un código • Una fecha de inicio • Una fecha de fin • Asignarle que es web Se encuentra el proceso electoral.

Tabla 112. Especificación Técnica.Encontrar procesos activos

Prueba 15 –Encontrar proceso con fecha inválida
Esta prueba consiste en: • Buscar los procesos electorales con una fecha No se encuentra el proceso electoral.

Tabla 113. Especificación Técnica. Encontrar proceso con código inválido

Prueba 16 – Encontrar proceso con código inválido
Esta prueba consiste en: • Buscar proceso electoral con un código No se encuentra el proceso electoral.

Tabla 114. Especificación Técnica.Encontrar proceso con código inválido

Prueba 17 – Votante que ya ha votado
Esta prueba consiste en: • Se utiliza el servicio VotacionValidationService para validar un votante Se da el siguiente error ERROR_YA_VOTADO.

Tabla 115. Especificación Técnica.Votante que ya ha votado

Prueba 18 – Validación de votante sin errores
Esta prueba consiste en: • Se utiliza el servicio VotacionValidationService para validar un votante No hay errores.

Tabla 116. Especificación Técnica.Validación de votante sin errores

Prueba 19 – Proceso ya cerrado
Esta prueba consiste en: • Se utiliza el servicio VotacionValidationService para validar un votante Se da el siguiente error ERROR_PROCESO_CERRADO.

Tabla 117. Especificación Técnica.Proceso ya cerrado

Prueba 20 – Validación proceso abierto
Esta prueba consiste en: • Se utiliza el servicio VotacionValidationService para validar un votante No hay errores.

Tabla 118. Especificación Técnica.Validación proceso abierto

Prueba 21 – Validación máxima de preferencias (0 escogidas)
Esta prueba consiste en: • Se utiliza el servicio VotacionValidationService para validar el número máximo de preferencias No hay errores, pues se han escogido 0 preferencias.

Tabla 119. Especificación Técnica.Validación max prefs (0)

Prueba 22 – Validación máxima de preferencias (menor o igual)
Esta prueba consiste en: • Se utiliza el servicio VotacionValidationService para validar el número máximo de preferencias. No hay errores, se han escogido un número menor o igual que las posibles.

Tabla120. Especificación Técnica.Validación max prefs (menor o igual)

Prueba 23 – Validación máximo de preferencias (Mayor)
Esta prueba consiste en: • Se utiliza el servicio VotacionValidationService para validar el número máximo de preferencias. Hay errores, se ha escogido un número mayor que las posibles.

Tabla 121. Especificación Técnica.Validación max prefs (mayor)

Prueba 24 – Encontrar votante por nombre
Esta prueba consiste en: • Se utiliza el servicio VoterService para buscar un votante por nombre. Coincide que se encuentra al votante que estábamos esperando.

Tabla 122. Especificación Técnica.Encontrar votante por nombre

Prueba 25 – Encontrar votante por nombre inválido
Esta prueba consiste en: • Se utiliza el servicio VoterService para buscar un votante por nombre. Coincide que se encuentra al votante que estábamos esperando.

Tabla 123. Especificación Técnica. Encontrar votante por nombre inválido

Prueba 26 – Encontrar votante por email
Esta prueba consiste en: • Se utiliza el servicio VoterService para buscar un votante por email. Se encuentra el votante esperado.

Tabla 124. Especificación técnica. Encontrar votante por email

Prueba 27 – Encontrar votante por email inválido
Esta prueba consiste en • Se utiliza el servicio VoterService para buscar un votante por email. No se encuentra el votante esperado.

Tabla 125 Especificación técnica. Encontrar votante por email inválido

Prueba 28 – Realizar un registro de votante completo
Esta prueba consiste en: • Se utiliza el servicio VoterService para buscar un votante por nombre. • Se crea un VoterRegistrationDto. • Al dto, se le asigna un nombre, un apellido, un proceso electoral y un email. • Se guarda el votante, utilizando el servicio VoterService. Se comprueba que el registro se hace de forma correcta.

Tabla 126. Especificación Técnica. Encontrar votante por email inválido

Prueba 29 – Cargar usuario
Esta prueba consiste en: • Utilizar el servicio VoterService para probar si se carga el usuario correctamente. Efectivamente, la carga del usuario se realiza sin problemas.

Tabla 127. Especificación técnica. Cargar usuario

Capítulo 7 CONSTRUCCIÓN DEL SISTEMA DE INFORMACIÓN

7.1 PREPARACIÓN DEL ENTORNO DE GENERACIÓN Y CONSTRUCCIÓN

7.1.1 Estándares y normas seguidos

A lo largo de todo el desarrollo del proyecto, uno de los principales objetivos fue seguir, en la medida de lo posible, todas las pautas de desarrollo y estilo que nos han impartido durante todos los cursos del grado. Se ha tenido especial cuidado en hacer que el código sea lo más claro posible.

7.1.2 Lenguajes de programación

Java, es un lenguaje de programación orientado a objetos rápido, seguro y fiable. Es, a partir de 2012, uno de los lenguajes de programación más populares en uso, particularmente para aplicaciones de cliente-servidor de web.

Su sintaxis deriva en gran medida de C y C++, pero tiene menos utilidades de bajo nivel que cualquiera de ellos. Las aplicaciones de Java son compiladas a bytecode (clase Java), que puede ejecutarse en cualquier máquina virtual Java (JVM) sin importar la arquitectura de la computadora subyacente.

La aplicación de escritorio estaba desarrollada en Java y he realizado las extensiones también con Java.

La versión usada ha sido Java 14, perteneciente a la distribución Java SE.

La aplicación web también ha sido desarrollada con Java.

7.1.3 Herramientas y programas usados para el desarrollo

7.1.3.1 JUnit

Es un conjunto de bibliotecas utilizadas en programación para hacer pruebas unitarias de aplicaciones Java. Es un framework que permite realizar la ejecución de clases Java de manera controlada, para poder evaluar si el funcionamiento de cada uno de los métodos de la clase se comporta como se espera.

Utilizado para la realización de las pruebas unitarias.

7.1.3.2 JavaFX

Es una tecnología de software que, combinada con Java, permite crear y desplegar aplicaciones con un aspecto vanguardista y contenidos avanzados, audio y vídeo. Amplía la tecnología Java permitiendo el uso de cualquier biblioteca de Java en una aplicación JavaFX.

Permite mantener un eficaz flujo de trabajo entre diseñador y desarrollador en el que los diseñadores pueden trabajar en las herramientas que deseen mientras colaboran con los desarrolladores.

Utilizado para las distintas pantallas de la aplicación Java.

7.1.3.3 Maven

Es una herramienta de software para la gestión y construcción de proyectos Java. Tiene un modelo de configuración de construcción basado en un formato XML.

Maven utiliza un Project Object Model (POM) para describir el proyecto de software a construir, sus dependencias de otros módulos y componentes externos, y el orden de construcción de los elementos.

Viene con objetivos predefinidos para realizar ciertas tareas claramente definidas, como la compilación del código y su empaquetado.

Una característica clave de Maven es que está listo para usar en red. El motor incluido en su núcleo puede dinámicamente descargar plugins de un repositorio.

La estructura de este proyecto está construido a base de dependencias Maven.

7.1.3.4 GitHub

Es una plataforma de desarrollo colaborativo para alojar proyectos utilizando el sistema de control de versiones Git. Se utiliza principalmente para la creación de código fuente de programas de ordenador.

Lo he utilizado de forma rutinaria para tener distintas versiones de los proyectos.

7.1.3.5 MySQL Workbench

MySQL Workbench es una herramienta de diseño de bases de datos que integra el desarrollo, la administración, el diseño, la creación y el mantenimiento de bases de datos SQL en un único entorno de desarrollo integrado para el sistema de bases de datos MySQL.

Se ha usado tanto para la aplicación de escritorio como aplicación web.

7.1.3.6 Eclipse

Eclipse es un entorno de desarrollo integrado (IDE) utilizado en la programación informática. Contiene un espacio de trabajo base y un sistema de plug-in extensible para personalizar el entorno. Está escrito principalmente en Java y su uso principal es para desarrollar aplicaciones Java.

Se ha usado para la aplicación de escritorio.

7.1.3.7 Spring boot

Java Spring Framework (Spring Framework) es un marco popular, de código abierto y de nivel empresarial para crear aplicaciones standalone de nivel de producción que se ejecutan en la máquina virtual Java (JVM).

Java Spring Boot (Spring Boot) es una herramienta que hace que el desarrollo de aplicaciones web y microservicios con Spring Framework sea más rápido y fácil a través de tres capacidades principales:

- Configuración automática.
- Un enfoque obstinado de la configuración.
- La capacidad de crear aplicaciones independientes.

Se ha usado para la aplicación web.

7.1.3.8 Spring Data JPA

Spring Data JPA, parte de la familia spring data más grande, facilita la implementación de repositorios basados en JPA. Simplifica la creación de aplicaciones impulsadas por Spring que utilizan tecnologías de acceso a datos.

Implementar una capa de acceso a datos de una aplicación fue complicado durante bastante tiempo. Se tenía que escribir demasiado código repetitivo para ejecutar consultas simples. Spring Data JPA tiene como objetivo mejorar significativamente la implementación de capas de acceso a datos al reducir el esfuerzo de la cantidad que realmente se necesita.

Se ha usado para la aplicación web.

7.1.3.9 Thymeleaf

Thymeleaf es un motor de plantillas Java XML/XHTML/HTML5 que puede funcionar tanto en entornos web (basados en servlets) como no web.

Es más adecuado para servir XHTML / HTML5 en la capa de vista de aplicaciones web basadas en MVC, pero puede procesar cualquier archivo XML incluso en entornos sin conexión. Proporciona una integración completa de Spring Framework.

En las aplicaciones web, Thymeleaf pretende ser un sustituto completo de JavaServer Pages (JSP).

Thymeleaf es un software de código abierto, licenciado bajo la Licencia Apache 2.0.

Se ha utilzado para las vistas de la aplicación web.

7.1.3.10 Lombok

Project Lombok es una herramienta de biblioteca java que se utiliza para minimizar/eliminar el código repetitivo y ahorrar el valioso tiempo de los desarrolladores durante el desarrollo con solo usar algunas anotaciones. Además, también aumenta la legibilidad del código fuente y ahorra espacio.

7.1.3.10.1 Anotaciones Lombok

- @Getter y @Setter: Estas anotaciones proporcionan los métodos getter y setter para un campo.
- @NoArgsConstructor: Esta anotación se utiliza para generar un constructor sin argumentos.
- @AllArgsConstructor: Esta anotación se utiliza para generar un constructor parametrizado que acepta un solo parámetro para cada campo y los inicializa usándolo.
- @ToString: Esta anotación se utiliza para invalidar el método toString() y generar una implementación predeterminada para él.
- @EqualsAndHashCode: Esta anotación se utiliza para anular los métodos equals() y hashCode() y proporciona una implementación predeterminada para esto.
- @Data: Esta anotación es una anotación de acceso directo y agrupa @ToString, @Getter, @Setter, @EqualsAndHashCode y @RequiredArgsConstructor anotaciones en una sola anotación.
- @Builder: Esta anotación se puede utilizar para eliminar el código repetitivo involucrado en la configuración de las propiedades de un objeto.

Se ha utilizado para la aplicación web.

7.2 ELABORACIÓN DE LOS MANUALES DE USUARIO

7.2.1 Manual de Instalación y de Ejecución

La instalación del sistema Evoting consta de las siguientes partes diferenciadas:

- Terminales de escritorio
- Aplicación web
- BBDD MySQL Server

Los diferentes terminales utilizan SSL tanto para las comunicaciones entre terminales como en la comunicación entre terminal y BBDD.

Este proyecto se ha desarrollado y probado sobre el sistema operativo Windows 10.

7.2.1.1 MySQL Server

El primer paso es la instalación de un servidor MySQL.

Se ha realizado la instalación para Microsoft Windows y se debe escoger un paquete de instalación.

Para consultar más información, se debe revisar la guía de instalación. Ver [24]

7.2.1.2 MySQL Server, habilitando SSL

Una vez que se ha instalado MySQL server deben habilitarse las comunicaciones SSL, para lo cual se pueden seguir los siguientes pasos:

1. Entrar en MySQL:

```
> mysql -uroot -p
```

2. Le pedirá la contraseña correspondiente al usuario “root”. Una vez introducida la password, se debe ejecutar:

```
> mysql_ssl_rsa_setup --uid mysql
```

3. Se debe comprobar que existen los siguientes ficheros en el directorio */var/lib/mysql* :
   - *ca.pem*
   - *client-key.pem*
   - *client-cert.pem*

- *server-key.pem*
- *server-cert.pem*

4. Se debe editar */etc/mysql/mysql.conf.d/mysqld.cnf* , añadiendo al final:

```
ssl-ca = /var/lib/mysql/ca.pem
ssl-cert = /var/lib/mysql/server-cert.pem
ssl-key = /var/lib/mysql/server-key.pem
```

5. Se debe reiniciar MySQL Server comprobando que SSL está habilitado:

```
>service mysql restart
>mysql -u {db_user} -p
 mysql> SHOW VARIABLES LIKE "%ssl%";
```

Si todo ha ido correctamente las variables *have_openssl* y *have_ssl* deberían tener el valor YES.
Se pueden consultar las instrucciones para habilitar SSL en [25].
Para comprobar la conexión SSL a través de MySQL WorkBench se debe editar la conexión estableciendo:

- private key SSL key: *client-key.pem*
- public key SSL CERT: *client-cert.pem*
- Certificate Authority SSL CA: *ca.pem*

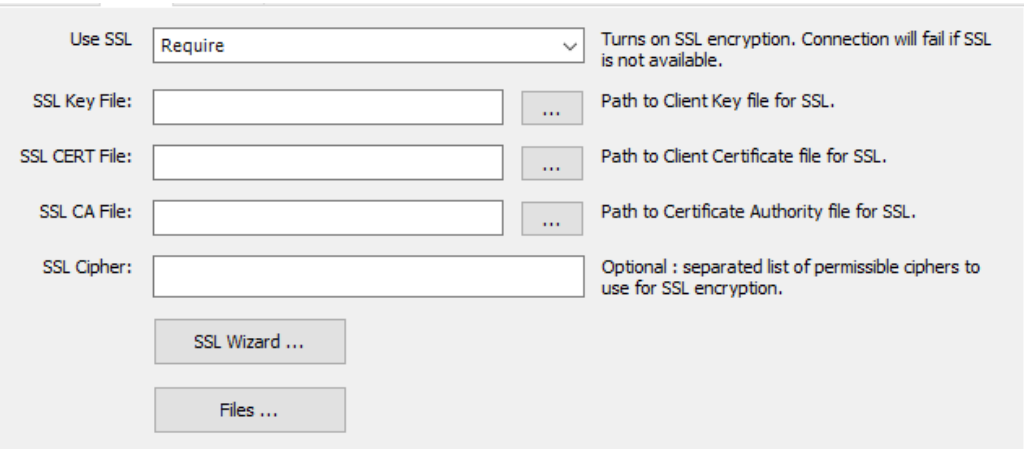

Ilustración 87. Comprobar conexión SSL MySQL WorkBench

7.2.1.3 Java KeyStore (JKS)

1. Crear un directorio nuevo y copiar los ficheros *ca.pem*, *client-cert.pem* y *client-key.pem* .
2. Ejecutar el script *jks_configuration.sh* y seguir paso a paso el proceso para la creación de ficheros de configuración con los *TrustStores*, *KeyStores* necesarios para el funcionamiento del proyecto. Este script necesita dos parámetros:
    - El path al directorio donde se encuentra el proyecto "Evoting".
    - El path al directorio creado anteriormente y en el que se han copiado los ficheros *.pem* necesarios para la conexión SSL.
3. Si todo transcurre correctamente en los módulos especificados, aparecerán un directorio *ssl/* y un *src/main/resources/cfg*.

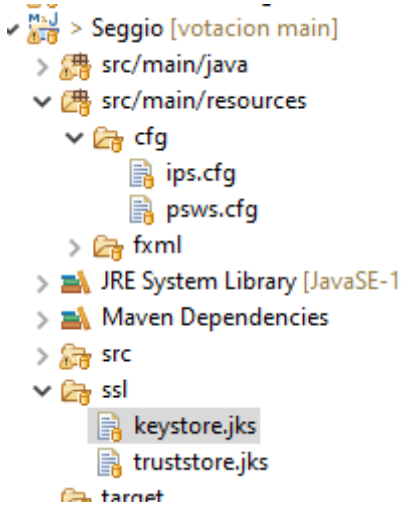

Ilustración 88. Directorios ssl y resources/cfg

Además, los módulos *Poll*, *ProcedureManager*, *Test* y *Urna* necesitan especificar las credenciales para la conexión con la base de datos en el fichero *src/main/resources/cfg/psws.cfg* estableciendo los valores para *dbu* (username) y *dbp* (password).

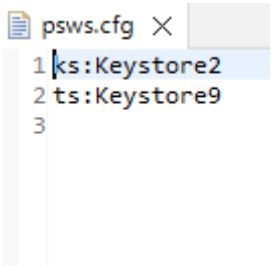

Ilustración 89. psws.cfg

7.2.1.4 Estructura de la base de datos

La estructura de base de datos se ha exportado al directorio *structure.sql* del proyecto *Evoting*.

7.2.1.5 Evoting escritorio

El sistema Evoting está formado por distintos módulos que pueden ser ejecutados en la misma máquina o en máquinas diferentes, algunos módulos se comunican entre sí a través de sockets con lo que tienen que estar en una red y algunos acceden a la base de datos MySQL con lo que tendrán que poder conectarse con el servidor de base de datos.

En la tabla Terminals se establecen las IP's de los distintos equipos que albergan los módulos. Pueden lanzarse más de una instancia de Postazione para agilizar el proceso de votación.

Conexiones entre los módulos:

	Urna	**Seggio**	**Postaziones**	**BBDD**
P. Manager				X
Urna		X	X	X
Seggio	X		X	
Postazione	X	X		
Poll				X

Tabla 128. Conexiones entre módulos

Todos los módulos son proyectos *Maven* que se empaquetan en un *jar*, ejecutable en una *JVM*, mediante un *JRE* (Java Runtime Environment).
Se construyen desde el proyecto padre "Evoting".

```
>mvn package
```

Se muestre el resultado si todo es correcto:

```
[INFO]
[INFO] Evoting ..................................... SUCCESS [  0.004 s]
[INFO] Common ...................................... SUCCESS [  0.890 s]
[INFO] Poll ........................................ SUCCESS [  0.082 s]
[INFO] Postazione .................................. SUCCESS [  0.052 s]
[INFO] ProcedureManager ............................ SUCCESS [  6.760 s]
[INFO] Seggio ...................................... SUCCESS [  0.047 s]
[INFO] SeggioAusiliario ............................ SUCCESS [  0.043 s]
[INFO] Urna ........................................ SUCCESS [  0.040 s]
[INFO] Test ........................................ SUCCESS [  0.046 s]
[INFO]
[INFO] BUILD SUCCESS
[INFO]
[INFO] Total time:  8.103 s
[INFO] Finished at: 2022-07-02T22:28:27+02:00
[INFO]
```

Ilustración 90. Resultado mvn package

7.2.1.5.1 Procedure Manager

La carga de datos se hace a través de ficheros .cvs y requiere la existencia de un usuario “root” con permisos para la creación de nuevos usuarios (técnicos y supervisores).

El comando para lanzar el “Procedure Manager” :

```
path_to_jdk>\bin\javaw.exe -Dfile.encoding=UTF-8 -p
"<path_to_project>\ProcedureManager\target\classes;<path_to_project>\Common\target\clas
ses;<path_to_maven_repository>\org\bouncycastle\bcprov-jdk15on\1.64\bcprov-jdk15on-
1.64.jar;<path_to_maven_repository>\org\apache\commons\commons-lang3\3.5\commons-
lang3-3.5.jar;<path_to_maven_repository>\org\openjfx\javafx-controls\14\javafx-controls-14-
win.jar;<path_to_maven_repository>\org\openjfx\javafx-graphics\14\javafx-graphics-14-
win.jar;<path_to_maven_repository>\org\openjfx\javafx-base\14\javafx-base-14-
win.jar;<path_to_maven_repository>\org\openjfx\javafx-fxml\14\javafx-fxml-14-
win.jar;<path_to_maven_repository>\gnu\io\rxtx\2.2.2\rxtx-
2.2.2.jar;<path_to_maven_repository>\org\apache\logging\log4j\log4j-api\2.17.2\log4j-api-
2.17.2.jar;<path_to_maven_repository>\com\sun\mail\javax.mail\1.6.2\javax.mail-1.6.2.jar" -
classpath "<path_to_maven_repository>\mysql\mysql-connector-java\8.0.20\mysql-connector-
java-8.0.20.jar;<path_to_maven_repository>\com\google\protobuf\protobuf-
java\3.6.1\protobuf-java-3.6.1.jar;<path_to_maven_repository>\org\openjfx\javafx-
controls\14\javafx-controls-14.jar;<path_to_maven_repository>\org\openjfx\javafx-
graphics\14\javafx-graphics-14.jar;<path_to_maven_repository>\org\openjfx\javafx-
base\14\javafx-base-14.jar;<path_to_maven_repository>\org\openjfx\javafx-fxml\14\javafx-
fxml-14.jar;<path_to_maven_repository>\org\apache\logging\log4j\log4j-core\2.17.2\log4j-
core-2.17.2.jar;<path_to_maven_repository>\javax\activation\activation\1.1\activation-1.1.jar"
-m ProcedureManager/procmgr.app.App
```

7.2.1.5.2 Poll

El comando para lanzar el “Poll”:

```
<path_to_jdk>\bin\javaw.exe -Dfile.encoding=UTF-8 -p
"<path_to_project>\Poll\target\classes;<path_to_project>\Common\target\classes;<path_to_m
aven_repository>\org\bouncycastle\bcprov-jdk15on\1.64\bcprov-jdk15on-
1.64.jar;<path_to_maven_repository>\org\apache\commons\commons-lang3\3.5\commons-
lang3-3.5.jar;<path_to_maven_repository>\org\openjfx\javafx-controls\14\javafx-controls-14-
win.jar;<path_to_maven_repository>\org\openjfx\javafx-graphics\14\javafx-graphics-14-
win.jar;<path_to_maven_repository>\org\openjfx\javafx-base\14\javafx-base-14-
win.jar;<path_to_maven_repository>\org\openjfx\javafx-fxml\14\javafx-fxml-14-
win.jar;<path_to_maven_repository>\gnu\io\rxtx\2.2.2\rxtx-
2.2.2.jar;<path_to_maven_repository>\org\apache\logging\log4j\log4j-api\2.17.2\log4j-api-
2.17.2.jar;<path_to_maven_repository>\org\apache\pdfbox\pdfbox\2.0.19\pdfbox-2.0.19.jar" -
classpath "<path_to_maven_repository>\mysql\mysql-connector-java\8.0.20\mysql-connector-
java-8.0.20.jar;<path_to_maven_repository>\com\google\protobuf\protobuf-
java\3.6.1\protobuf-java-3.6.1.jar;<path_to_maven_repository>\org\openjfx\javafx-
controls\14\javafx-controls-14.jar;<path_to_maven_repository>\org\openjfx\javafx-
graphics\14\javafx-graphics-14.jar;<path_to_maven_repository>\org\openjfx\javafx-
base\14\javafx-base-14.jar;<path_to_maven_repository>\org\openjfx\javafx-fxml\14\javafx-
fxml-14.jar;<path_to_maven_repository>\org\apache\logging\log4j\log4j-core\2.17.2\log4j-
core-2.17.2.jar;<path_to_maven_repository>\org\apache\pdfbox\fontbox\2.0.19\fontbox-
2.0.19.jar;<path_to_maven_repository>\commons-logging\commons-logging\1.2\commons-
logging-1.2.jar" -XX:+ShowCodeDetailsInExceptionMessages -m Poll/poll.app.App
```

7.2.1.5.3 Urna

El comando para lanzar la Urna es:

```
<path_to_jdk>\bin\javaw.exe -Dfile.encoding=UTF-8 -p
"<path_to_project>\Urna\target\classes;<path_to_project>\Common\target\classes;<path_to
_maven_repository>\org\bouncycastle\bcprov-jdk15on\1.64\bcprov-jdk15on-
1.64.jar;<path_to_maven_repository>\org\apache\commons\commons-lang3\3.5\commons-
lang3-3.5.jar;<path_to_maven_repository>\org\openjfx\javafx-controls\14\javafx-controls-14-
win.jar;<path_to_maven_repository>\org\openjfx\javafx-graphics\14\javafx-graphics-14-
win.jar;<path_to_maven_repository>\org\openjfx\javafx-base\14\javafx-base-14-
win.jar;<path_to_maven_repository>\org\openjfx\javafx-fxml\14\javafx-fxml-14-
win.jar;<path_to_maven_repository>\gnu\io\rxtx\2.2.2\rxtx-
2.2.2.jar;<path_to_maven_repository>\org\apache\logging\log4j\log4j-api\2.17.2\log4j-api-
2.17.2.jar" -classpath "<path_to_maven_repository>\mysql\mysql-connector-
java\8.0.20\mysql-connector-java-
8.0.20.jar;<path_to_maven_repository>\com\google\protobuf\protobuf-java\3.6.1\protobuf-
java-3.6.1.jar;<path_to_maven_repository>\org\openjfx\javafx-controls\14\javafx-controls-
14.jar;<path_to_maven_repository>\org\openjfx\javafx-graphics\14\javafx-graphics-
14.jar;<path_to_maven_repository>\org\openjfx\javafx-base\14\javafx-base-
14.jar;<path_to_maven_repository>\org\openjfx\javafx-fxml\14\javafx-fxml-
14.jar;<path_to_maven_repository>\org\apache\logging\log4j\log4j-core\2.17.2\log4j-core-
2.17.2.jar" -XX:+ShowCodeDetailsInExceptionMessages -m Urna/urna.app.App
```

7.2.1.5.4 Postazione

El comando para lanzar el “Puesto”:

```
<path_to_jdk>\bin\javaw.exe -Dfile.encoding=UTF-8 -p
"<path_to_project>\Postazione\target\classes;<path_to_project>\Common\target\classes;<pat
h_to_maven_repository>\org\bouncycastle\bcprov-jdk15on\1.64\bcprov-jdk15on-
1.64.jar;<path_to_maven_repository>\org\apache\commons\commons-lang3\3.5\commons-
lang3-3.5.jar;<path_to_maven_repository>\org\openjfx\javafx-controls\14\javafx-controls-14-
win.jar;<path_to_maven_repository>\org\openjfx\javafx-graphics\14\javafx-graphics-14-
win.jar;<path_to_maven_repository>\org\openjfx\javafx-base\14\javafx-base-14-
win.jar;<path_to_maven_repository>\org\openjfx\javafx-fxml\14\javafx-fxml-14-
win.jar;<path_to_maven_repository>\gnu\io\rxtx\2.2.2\rxtx-
2.2.2.jar;<path_to_maven_repository>\org\apache\logging\log4j\log4j-api\2.17.2\log4j-api-
2.17.2.jar" -classpath "<path_to_maven_repository>\mysql\mysql-connector-
java\8.0.20\mysql-connector-java-
8.0.20.jar;<path_to_maven_repository>\com\google\protobuf\protobuf-java\3.6.1\protobuf-
java-3.6.1.jar;<path_to_maven_repository>\org\openjfx\javafx-controls\14\javafx-controls-
14.jar;<path_to_maven_repository>\org\openjfx\javafx-graphics\14\javafx-graphics-
14.jar;<path_to_maven_repository>\org\openjfx\javafx-base\14\javafx-base-
14.jar;<path_to_maven_repository>\org\openjfx\javafx-fxml\14\javafx-fxml-
14.jar;<path_to_maven_repository>\org\apache\logging\log4j\log4j-core\2.17.2\log4j-core-
2.17.2.jar" -XX:+ShowCodeDetailsInExceptionMessages -m Postazione/postazione.app.App
```

7.2.1.5.5 Seggio

Comando para ejecución de la “Mesa electoral principal”:

```
<path_to_jdk>\bin\javaw.exe -Dfile.encoding=UTF-8 -p
"<path_to_project>\Seggio\target\classes;<path_to_project>\Common\target\classes;<path_t
o_maven_repository>\org\bouncycastle\bcprov-jdk15on\1.64\bcprov-jdk15on-
1.64.jar;<path_to_maven_repository>\org\apache\commons\commons-lang3\3.5\commons-
lang3-3.5.jar;<path_to_maven_repository>\org\openjfx\javafx-controls\14\javafx-controls-14-
win.jar;<path_to_maven_repository>\org\openjfx\javafx-graphics\14\javafx-graphics-14-
win.jar;<path_to_maven_repository>\org\openjfx\javafx-base\14\javafx-base-14-
win.jar;<path_to_maven_repository>\org\openjfx\javafx-fxml\14\javafx-fxml-14-
win.jar;<path_to_maven_repository>\gnu\io\rxtx\2.2.2\rxtx-
2.2.2.jar;<path_to_maven_repository>\org\apache\logging\log4j\log4j-api\2.17.2\log4j-api-
2.17.2.jar" -classpath "<path_to_maven_repository>\mysql\mysql-connector-
java\8.0.20\mysql-connector-java-
8.0.20.jar;<path_to_maven_repository>\com\google\protobuf\protobuf-java\3.6.1\protobuf-
java-3.6.1.jar;<path_to_maven_repository>\org\openjfx\javafx-controls\14\javafx-controls-
14.jar;<path_to_maven_repository>\org\openjfx\javafx-graphics\14\javafx-graphics-
14.jar;<path_to_maven_repository>\org\openjfx\javafx-base\14\javafx-base-
14.jar;<path_to_maven_repository>\org\openjfx\javafx-fxml\14\javafx-fxml-
14.jar;<path_to_maven_repository>\org\apache\logging\log4j\log4j-core\2.17.2\log4j-core-
2.17.2.jar" -XX:+ShowCodeDetailsInExceptionMessages -m Seggio/seggio.app.App
```

7.2.1.6 Evoting web

La aplicación web "Evoting" es una aplicación spring-boot con lo que tiene embebido un tomcat. En el fichero de configuración:

application.properties

```
server.port=8090
server.error.whitelabel.enabled=false
server.error.include-message=always
#spring.thymeleaf.mode=HTML
#spring.main.allow-circular-references=true
# =============================================================
# = Data Source
# =============================================================
spring.datasource.url = jdbc:mysql://localhost:3306/secureBallot?useSSL=true
spring.datasource.username = root
spring.datasource.password = @ROOT80a

# =============================================================
# = Show or not log for each sql query
# =============================================================
spring.jpa.show-sql = true

# =============================================================
# = Keep the connection alive if idle for a long time (needed in production)
# =============================================================
spring.datasource.testWhileIdle = true
spring.datasource.validationQuery = SELECT 1

# =============================================================
# = The SQL dialect makes Hibernate generate better SQL for the chosen database
# =============================================================
#spring.jpa.properties.hibernate.dialect = org.hibernate.dialect.MySQL5Dialect
# ==========================
post.ip=web
post.session=0

```

Ilustración 91. Application properties

Se debe configurar el acceso a la base de datos.

Y los parámetros del puesto de votación.

El comando de ejecución es:

```
$ java -jar evoting.jar
```

7.2.2 Manual de Usuario

7.2.2.1 Aplicación de escritorio

7.2.2.1.1 Inicio de sesión

La pantalla de inicio de sesión es similar para Procedure Manager, Poll y Urna.

Se muestra la pantalla de Procedure Manager:

Ilustración 92. Pantalla inicio de sesión

7.2.2.1.2 Proceso electoral

7.2.2.1.2.1 Crear usuario

Solo, el usuario raíz podrá crear nuevos usuarios (técnicos y supervisores).

Ilustración 93. Pantalla Crear nuevo usuario

7.2.2.1.2.2 Crear nuevo procedimiento

Tanto el usuario raíz como el técnico podrán crear nuevos procesos.

Ilustración 94. Pantalla Crear nuevo procedimiento

7.2.2.1.2.3 Archivos de sesión

Tanto el usuario raíz como el técnico podrán cargar archivos se sesión. Forma parte de la creación de nuevos procesos.

Ilustración 95. Pantalla Archivos de sesión

7.2.2.1.3 Escrutinio

7.2.2.1.3.1 Seleccionar proceso

El supervisor tendrá que escoger los procesos sobre los que se quiere hacer el escrutinio. Los procesos deben estar terminados.

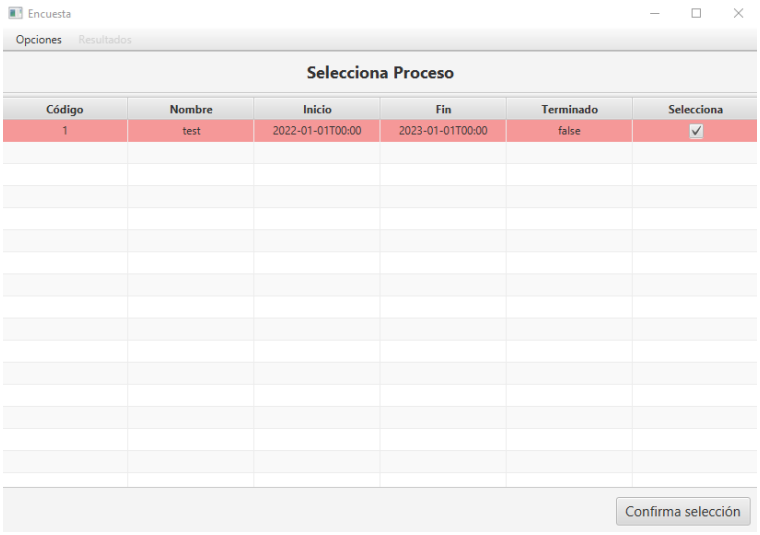

Ilustración 96. Pantalla Seleccionar Proceso

7.2.2.1.3.2 Resultados

7.2.2.1.4 Clave de sesión

Se muestra la pantalla de clave de sesión. Se utiliza tanto para Seggio como para Postazione. Se muestra la pantalla de Postazione (Puesto de votación):

Ilustración 97. Pantalla Clave de sesión

7.2.2.1.5 Urna

7.2.2.1.6 Seleccionar sesión

La sesión escogida debe ser válida.

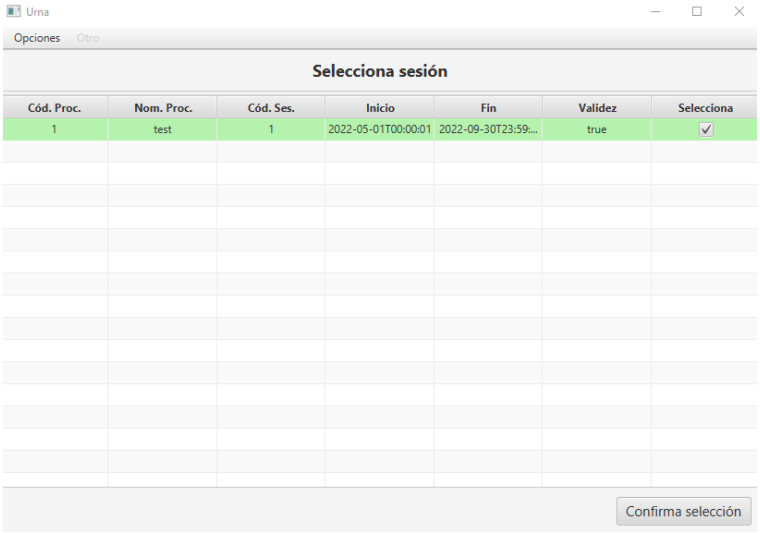

Ilustración 98. Pantalla Seleccionar sesión

7.2.2.1.7 Mensaje urna

Se muestra la pantalla de mensajes de la urna:

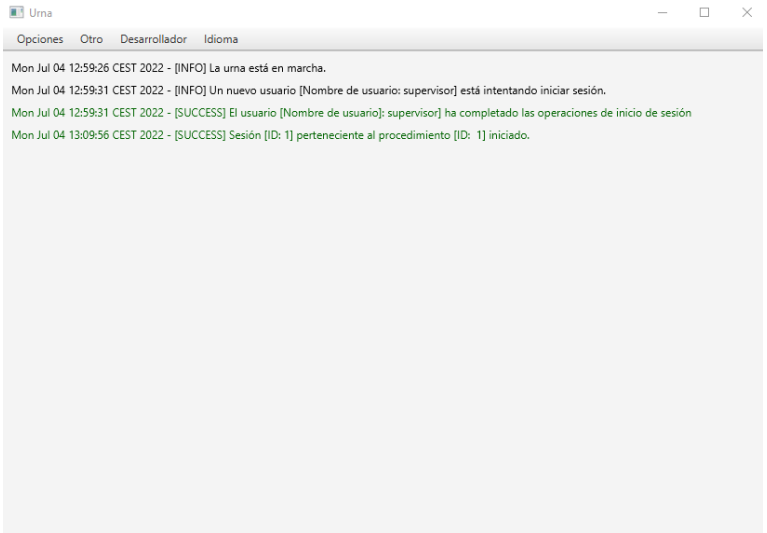

Ilustración 99. Pantalla Mensajes Urna

7.2.2.2 Mesa electoral

7.2.2.2.1 Lista de puestos

Se muestra la pantalla y la lista de puestos. El puesto que aparece está OFFLINE.

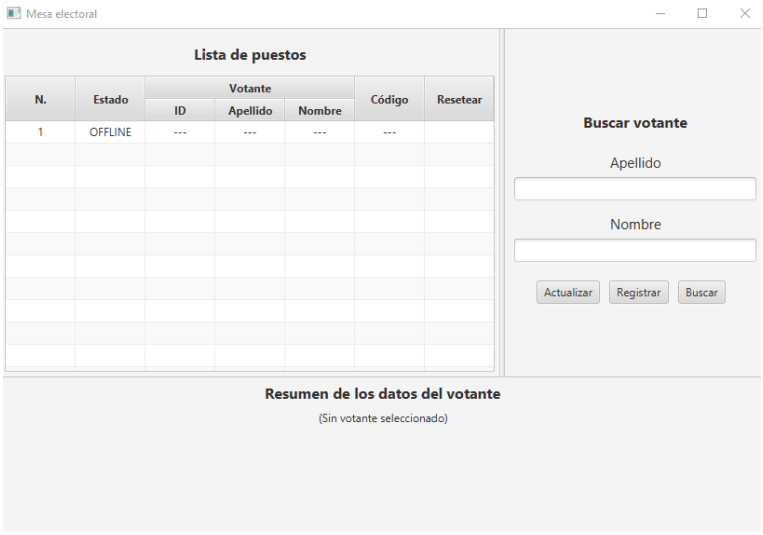

Ilustración 100. Pantalla Lista de Puestos

Desde la pantalla de lista de puestos, se puede acceder a actualizar, registrar y buscar votante.

7.2.2.2.2 Buscar votante

Debe poder escogerse el votante.

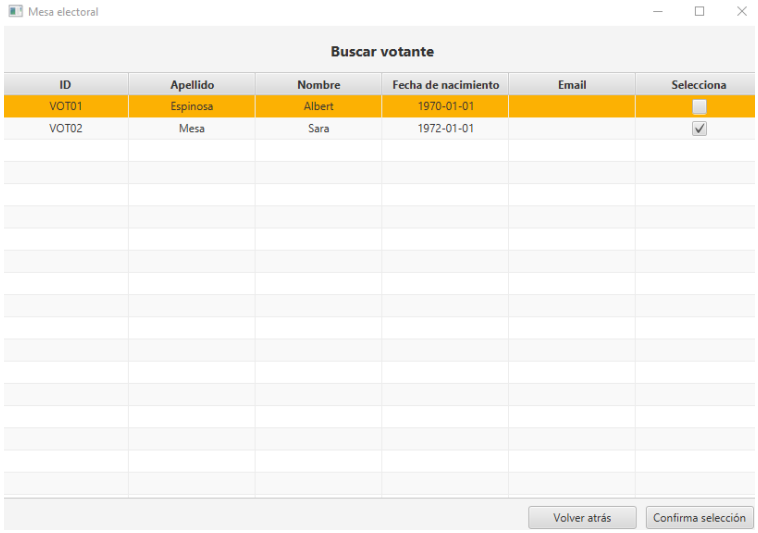

Ilustración 101. Buscar votante

7.2.2.2.3 Generar código del votante

Se debe pulsar el botón “Generar el código”

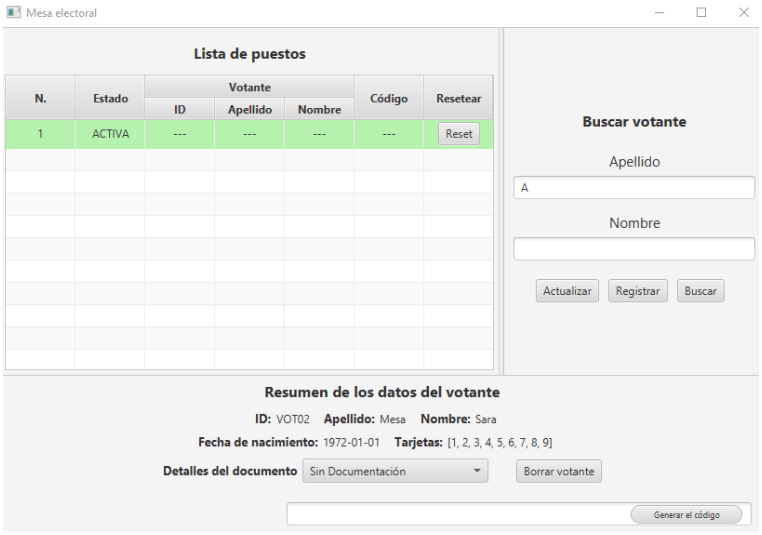

Ilustración 102. Pantalla Generar código

7.2.2.2.4 Puesto activado

Se muestra el puesto activado.

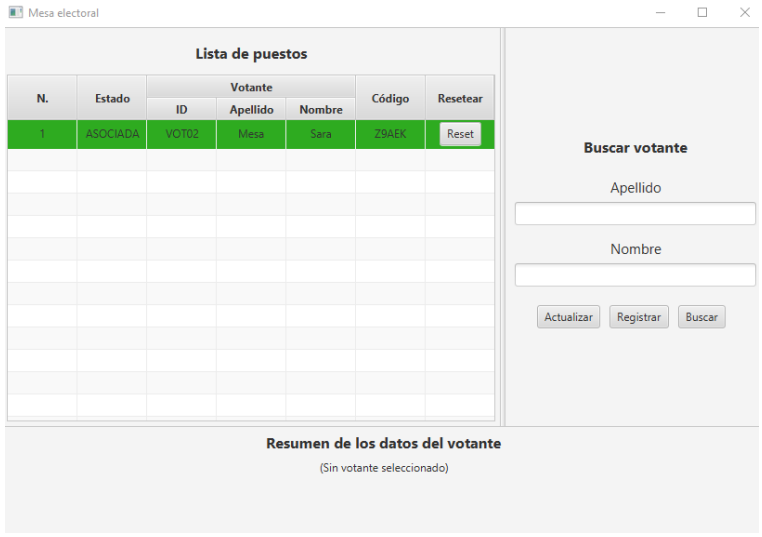

Ilustración 103. Pantalla Puesto Activado

7.2.2.2.5 Devolver código

Una vez se haya realizado la votación en el puesto de votación, se debe devolver el código en la mesa electoral:

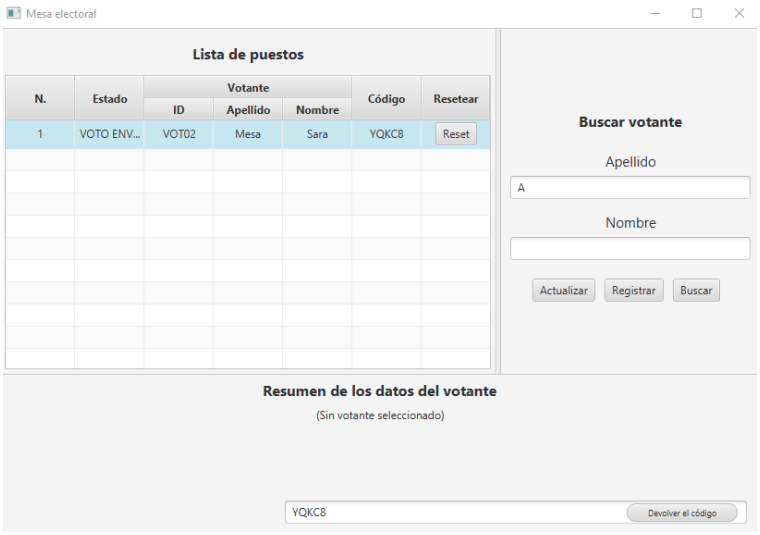

Ilustración 104. Devolver código

7.2.2.3 Puesto de votación

7.2.2.3.1 Puesto activado

Se muestra el puesto activado:

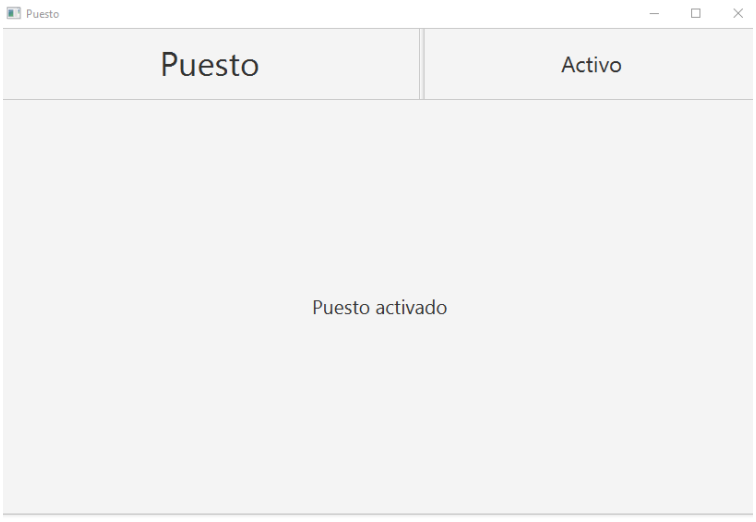

Ilustración 105. Puesto activado

7.2.2.3.2 Introduce el código

Una vez el puesto esté asociado, se debe introducir el código que aparezca en la lista de puestos.

Ilustración 106. Puesto asociado

7.2.2.3.3 Iniciar votación

Se debe iniciar la votación:

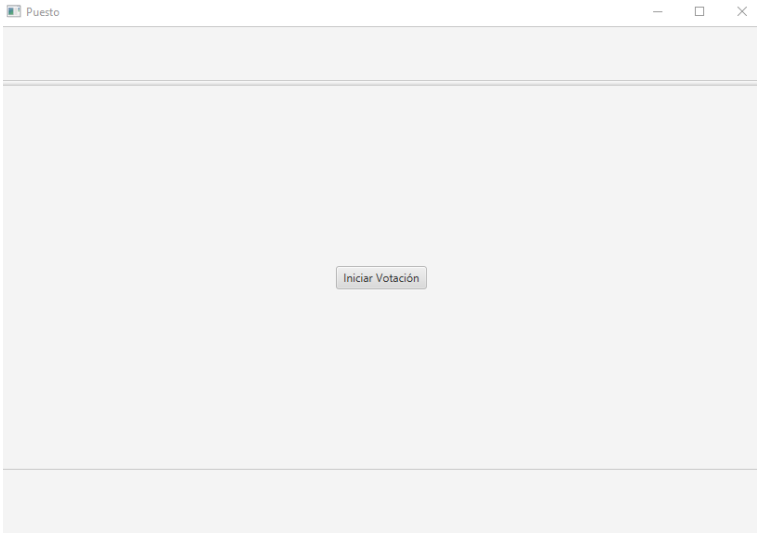

Ilustración 107. Iniciar votación

7.2.2.3.4 Escoger preferencias

El votante debe mostrar sus preferencias para cada ballot:

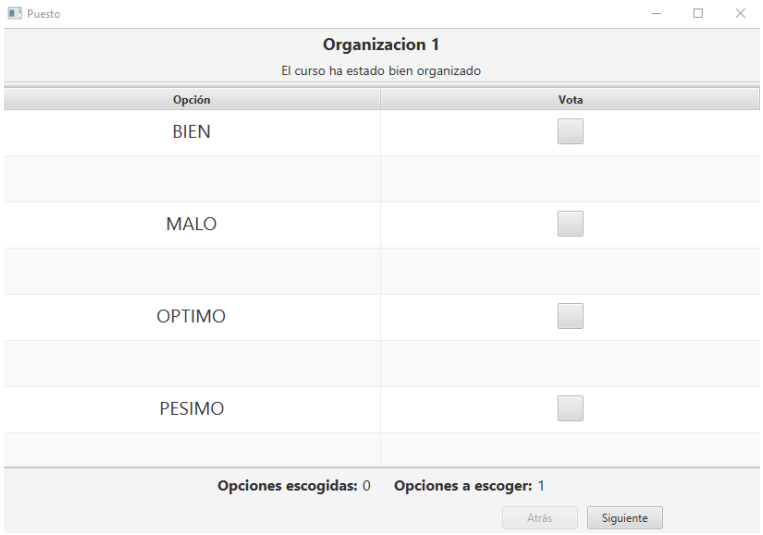

Ilustración 108. Escoger preferencias

7.2.2.3.5 Resumen de votación

Se muestra el resumen de la votación:

Ilustración 109. Resumen de votación

7.2.2.3.6 Puesto entregar token

Se debe entregar el token al supervisor para que lo devuelva en la mesa electoral:

Ilustración 110. Puesto entregar token

7.2.3 Aplicación web

7.2.3.1 Inicio de sesión

Se muestra la pantalla de inicio de sesión:

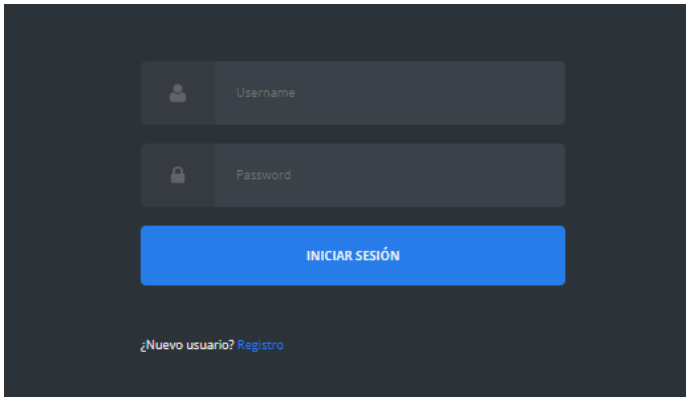

Ilustración 111. Pantalla Inicio sesión web

7.2.3.2 Registro de usuario

Se muestra el registro de usuario:

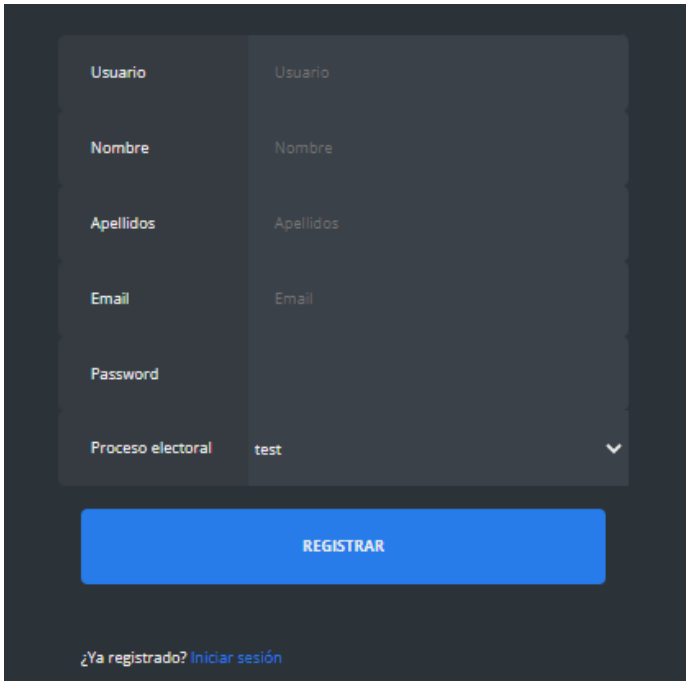

Ilustración 112. Pantalla Registro de usuario web

7.2.3.3 Votación

Se muestra la votación:

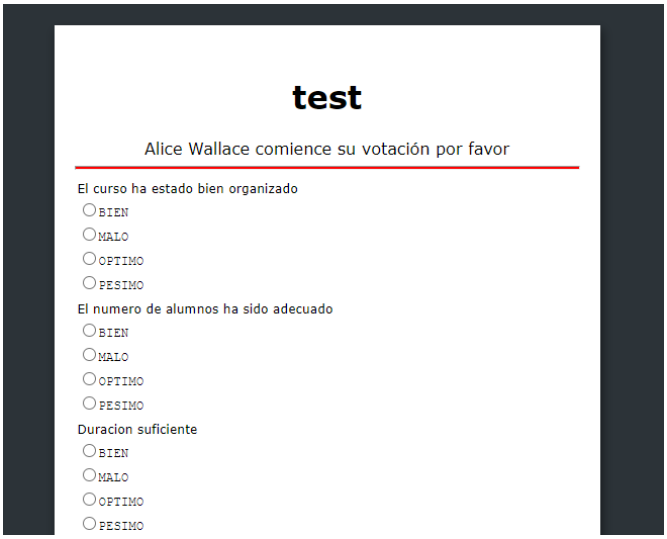

Ilustración 113. Pantalla votación

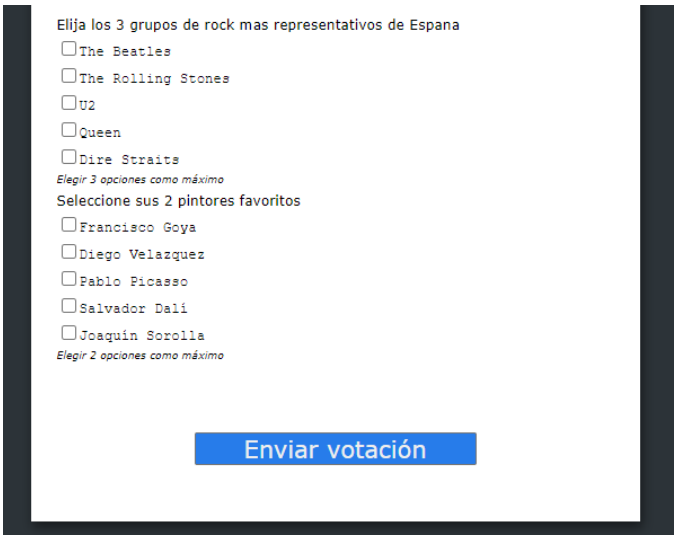

Ilustración 114. Pantalla votación II

Capítulo 8 CONCLUSIONES Y AMPLIACIONES

8.1 CONCLUSIONES

Los procesos de votación pueden mejorar la vida de la gente y ese ha sido mi propósito a la hora de escoger este proyecto. Debido a la incertidumbre del anonimato de las votaciones, este proceso sigue realizándose de modo manual, siendo un proceso muy costoso tanto en tiempo como en recursos.

Pienso que he podido aportar mi granito de arena a la hora de estudiar posibles soluciones a la automatización de los procesos electorales y hacer que pueda llegar a más gente.

Por otra parte, he tenido que implantar un sistema software y hacer un proceso de reingeniería, lo que ha supuesto un esfuerzo considerable para mí. Además, tuve que hacer una puesta a punto del entorno como he comentado en Manual de Instalación y de Ejecución.

También este proyecto me ha servido para mejorar mis conocimientos de tecnologías y frameworks de programación como Springboot y he investigado y utilizado nuevas tecnologías como por ejemplo Spring Data JPA y JavaFX.

Por último, creo que sucesivas ampliaciones al proyecto pueden sumar para conseguir el objetivo, consiguiendo un sistema de votación consistente, anónimo y ágil.

8.2 AMPLIACIONES

Se han pensado diversas ampliaciones que se podrían llevar a cabo para seguir mejorando el sistema.

8.2.1 Cambiar sistema creación procesos electorales

Actualmente los procesos electorales se crean a través de .csv que pueden llegar a ser un poco complicados de manejar.

Lo ideal sería agilizar el proceso de creación a través de pantallas que fueran más intuitivas.

8.2.2 Dar permiso a los votantes usando un lector RFID

A la hora de mejorar la interacción con el votante, sería necesario el uso de un lector RFID.

A continuación, dejo los pasos de configuración que se deberían realizar (aparte de adquirir un lector válido):

Se deben instalar algunos drivers:

1. Añadir el usuario al grupo propietario de los ficheros */dev/tty**, el fichero *default,* normalmente. A continuación, cierra la sesión e inicie sesión para actualizar los permisos:

```
user@pc: sudo usermod -a -G dialout user
user@pc: reboot
```

2. Copiar *rfid/librxtxSerial.so* en */usr/lib:*

```
user@pc: sudo cp rfid/librxtxSerial.so /usr/lib
```

3. Instalar Maven y añadir el fichero *rfid/RXTXcomn.jar* al repositorio local:

```
user@pc: sudo apt-get install maven
user@pc: mvn install:install-file -DgroupId=gnu.io -
DartifactId=rxtx -Dversion=2.2pre2 -Dpackaging=jar -
Dfile='rfid/RXTXcomm.jar' -DgeneratePom=true
```

Se debe repetir el proceso para cada ordenador donde se use el proyecto.

8.2.3 Censo electoral

Los votantes deben comprobarse contra un censo electoral, este proceso podría ser automatizado, bien comprobando contra servicios existentes en administraciones de comprobación de censo o también en los casos que estos servicios no estuviesen disponibles, podrían incorporase al modelo de datos una tabla de censo, en la que los votantes tuvieran que estar registrados para poder emitir

su voto. El censo tendría que poder ser modificado, y por tanto requeriría de un añadido, posiblemente en la aplicación web, que permitiera consultar los individuos censados, modificar los datos incorrectos, añadir y eliminar individuos.

8.2.4 Mejoras interfaces

Los interfaces son susceptibles de una mejora substantiva en cuanto usabilidad, objetivo que excedía la planificación del actual proyecto.

Los resultados podrían presentarse con métodos más atractivos, incluyendo gráficas.

8.2.5 Mejora en repositorio de datos

Es posible realizar un rediseño del modelo de datos, una vez que se tienen claras las tablas y datos que se requieren para el proceso.

APÉNDICES

A. PLAN DE GESTIÓN DE RIESGOS

A continuación, se presentan los riesgos de los proyectos detectados por el equipo de desarrollo.

A.1 Descripción

A.1.1 Pérdida de un compañero

- Identificador: Rsk-1
- Categoría: Gestión de proyecto
- Subcategoría: Comunicación

Un compañero del equipo decide irse del proyecto o pide la baja.

A.1.2 Requisitos adicionales

- Identificador: Rsk-2
- Categoría: Negocio

Por culpa de un cambio a lo largo del proyecto se tenga que llevar a cabo la adición de uno o varios requisitos más.

A.1.3 Uso de tecnología nueva

- Identificador: Rsk-3
- Categoría: Técnico
- Subcategoría: Tecnológica

Se puede dar el caso de que se utilice una tecnología nueva al inicio o durante el desarrollo del proyecto.

A.1.4 Mala formación de los usuarios finales

- Identificador: Rsk-4
- Categoría: Organizacional
- Subcategoría: Recursos

Los usuarios finales han recibido mala formación y no son capaces de sacar el máximo provecho a la aplicación por lo que recurren al personal de soporte para resolver sus dudas.

A.2 Análisis de los riesgos

Riesgo	**Probabilidad**	**Impacto**				**Impacto**
		Presupuesto	Planificación	Alcance	Calidad	
Pérdida de un compañero	Alta	Bajo	Crítico	Bajo	Alto	0,63
Requisitos adicionales	Alta	Medio	Alto	Medio	Alto	0,39
Uso de tecnología nueva	Alta	Alto	Alto	Medio	Alto	0,39
Mala formación de los usuarios finales	Alta	Bajo	Bajo	Inapreciable	Inapreciable	0,11

Tabla 129. Análisis de Riesgos

A.3 Respuesta a los riesgos

- Rsk-1. Estrategia: Asumir el riesgo. Contratar a un nuevo trabajador para sustituir al compañero ya sea que está de baja temporal o definitiva. El tiempo que se tarde en contratar al otro compañero, se tendría que redistribuir entre el resto de los compañeros, siempre intentando que fuera el mínimo posible.
- Rsk-2. Estrategia: Mitigar el riesgo. Invitar al cliente a desarrollar el proyecto periódicamente.

- Rsk-3. Estrategia: Asumir el riesgo. Realizar la formación del equipo de proyecto al inicio o durante el proyecto. Contratar a un experto de la tecnología para ayudar al equipo.
- Rsk-4. Estrategia: Asumir el riesgo. Revisar los manuales de formación para comprobar si están bien explicados. Volver a realizar tareas de formación a los usuarios de manera más detallada.

B. PRESUPUESTO DE COSTES

B.1 Estudio de viabilidad

I1	I2	I3	Descripción	Horas	Precio	Subtotal (1)	Subtotal (2)	Total
1			***Estudio de viabilidad***					**11.550,00 €**
	1		Estudio del arte				630,00 €	
		1	Administrador de sistemas	3	32,00 €	96,00 €		
		1	Analista	3	43,00 €	129,00 €		
		1	Arquitecto de software	3	45,00 €	135,00 €		
		1	Desarrollador de software	3	34,00 €	102,00 €		
		1	Jefe de proyecto	3	56,00 €	168,00 €		
	2		Contacto con responsables				420,00 €	
		1	Administrador de sistemas	2	32,00 €	64,00 €		
		1	Analista	2	43,00 €	86,00 €		
		1	Arquitecto de software	2	45,00 €	90,00 €		
		1	Desarrollador de software	2	34,00 €	68,00 €		
		1	Jefe de proyecto	2	56,00 €	112,00 €		
	3		Plan de viabilidad				1.260,00 €	
		1	Administrador de sistemas	6	32,00 €	192,00 €		
		1	Analista	6	43,00 €	258,00 €		
		1	Arquitecto de software	6	45,00 €	270,00 €		
		1	Desarrollador de software	6	34,00 €	204,00 €		
		1	Jefe de proyecto	6	56,00 €	336,00 €		
	4		Estudio de alternativas				3.360,00 €	
		1	Administrador de sistemas	16	32,00 €	512,00 €		
		1	Analista	16	43,00 €	688,00 €		
		1	Arquitecto de software	16	45,00 €	720,00 €		
		1	Desarrollador de software	16	34,00 €	544,00 €		
		1	Jefe de proyecto	16	56,00 €	896,00 €		
	5		Planificación inicial				1.680,00 €	

		1	Administrador de sistemas	8	32,00 €	256,00 €		
		1	Analista	8	43,00 €	344,00 €		
		1	Arquitecto de software	8	45,00 €	360,00 €		
		1	Desarrollador de software	8	34,00 €	272,00 €		
		1	Jefe de proyecto	8	56,00 €	448,00 €		
	6		Elaboración presupuesto inicial				3.360,00 €	
		1	Administrador de sistemas	16	32,00 €	512,00 €		
		1	Analista	16	43,00 €	688,00 €		
		1	Arquitecto de software	16	45,00 €	720,00 €		
		1	Desarrollador de software	16	34,00 €	544,00 €		
		1	Jefe de proyecto	16	56,00 €	896,00 €		
	7		Requisitos iniciales				840,00 €	
		1	Administrador de sistemas	4	32,00 €	128,00 €		
		1	Analista	4	43,00 €	172,00 €		
		1	Arquitecto de software	4	45,00 €	180,00 €		
		1	Desarrollador de software	4	34,00 €	136,00 €		
		1	Jefe de proyecto	4	56,00 €	224,00 €		

Tabla 130. Presupuesto. Estudio de viabilidad

B.2 Arranque del proyecto

I1	I2	I3	Descripción	Horas	Precio	Subtotal (1)	Subtotal (2)	Total
1			***Arranque del proyecto***					**1.979,00 €**
	1		Revisión de objetivos				792,00 €	
		1	Analista	8	43,00 €	344,00 €		
		1	Jefe de proyecto	8	56,00 €	448,00 €		
	2		Revisión de requisitos				21,50 €	
		1	Analista	0,5	43,00 €	21,50 €		
	3		Preparación del entorno de desarrollo y pruebas				544,00 €	
		1	Desarrollador de software	16	34,00 €	544,00 €		
	4		Configuración del entorno de desarrollo				544,00 €	

		1	Desarrollador de software	16	34,00 €	544,00 €		
	5		Revisión de la planificación				49,50 €	
		1	Analista	0,5	43,00 €	21,50 €		
		1	Jefe de proyecto	0,5	56,00 €	28,00 €		
	6		Cierre presupuesto inicial				28,00 €	
		1	Jefe de proyecto	0,5	56,00 €	28,00 €		

Tabla 131. Presupuesto. Arranque del proyecto

B.3 Análisis

I1	I2	I3	Descripción	Horas	Precio	Subtotal	Total
1			***Análisis***				**2.272,00 €**
	1		Definir requisitos con detalle			344,00 €	
		1	Analista	8	43,00 €		
	2		Especificación detallada de requisitos			1.032,00 €	
		1	Analista	24	43,00 €		
	3		Elaboración del presupuesto de cliente inicial			896,00 €	
		1	Jefe de proyecto	16	56,00 €		

Tabla 132. Presupuesto. Análisis

B.4 Diseño

I1	I2	I3	Descripción	Horas	Precio	Subtotal (1)	Subtotal (2)	Total
1			***Diseño***					**4.050,00 €**
	1		Definición de la arquitectura				360,00 €	
		1	Arquitecto de software	8	45,00 €	360,00 €		
	2		Diseño de clases				1.080,00 €	
		1	Arquitecto de software	24	45,00 €	1.080,00 €		
	3		Especificación del modelo de datos				720,00 €	
		1	Arquitecto de software	16	45,00 €	720,00 €		
	4		Especificación de las interfaces de comunicación				90,00 €	
		1	Arquitecto de software	2	45,00 €	90,00 €		
	5		Diseño de interfaces de usuario				1.800,00 €	
		1	Arquitecto de software	40	45,00 €	1.800,00 €		

Tabla 133. Presupuesto. Diseño

B.5 Implementación

I1	I2	I3	Descripción	Horas	Precio	Subtotal (1)	Subtotal (2)	Total
1			***Implementación***					**7.344,00 €**
	1		Nuevas mejoras del sistema				7.344,00 €	
		1	Desarrollador de software	216	34,00 €	7.344,00 €		

Tabla 134. Presupuesto. Implementación

B.6 Pruebas

I1	I2	I3	I4	Descripción	Horas	Precio	Subtotal (1)	Subtotal (2)	Total
1				**Pruebas**					**2.088,00 €**
	1			Implementación de pruebas unitarias				696,00 €	
		1		Tester	24	29,00 €	696,00 €		
	1			**Pruebas de integración**				1.392,00 €	
		1		Diseño					
			1	Tester	24	29,00 €	696,00 €		
		1		Implementación					
			1	Tester	8	29,00 €	232,00 €		
		1		Ejecución					
			1	Tester	8	29,00 €	232,00 €		
		1		Documentación					
			1	Tester	8	29,00 €	232,00 €		

Tabla 135. Presupuesto. Pruebas

B.7 Documentación

I1	I2	I3	Descripción	Horas	Precio	Subtotal (1)	Subtotal (2)	Total
1			***Documentación***					**7.392,00 €**
	1		Realizar la documentación y manuales de instalación				2.112,00 €	
		1	Administrador de sistemas	32	32,00 €	1.024,00 €		
		1	Desarrollador de software	32	34,00 €	1.088,00 €		
	1		Realizar la documentación y manuales de configuración del sistema				2.640,00 €	

		1	Administrador de sistemas	40	32,00 €	1.280,00 €		
		1	Desarrollador de software	40	34,00 €	1.360,00 €		
	1		Realizar la documentación y manuales de ejecución del sistema				2.640,00 €	
		1	Administrador de sistemas	40	32,00 €	1.280,00 €		
		1	Desarrollador de software	40	34,00 €	1.360,00 €		

Tabla 136. Presupuesto. Documentación

B.8 Despliegue

I1	I2	I3	Descripción	Horas	Precio	Subtotal (1)	Subtotal (2)	Total
1			**Despliegue**					1.208,00 €
	1		Instalar el sistema en los servidores de prueba y producción de la empresa contratante				488,00 €	
		1	Administrador de sistemas	8	32,00 €	256,00 €		
		2	Tester	8	29,00 €	232,00 €		
	1		Desplegar el sistema en los servidores de prueba y producción de la empresa contratante				488,00 €	
		1	Administrador de sistemas	8	32,00 €	256,00 €		
		2	Tester	8	29,00 €	232,00 €		
	1		Ejecución de pruebas de integración en los servidores de prueba y producción de la empresa contratante				232,00 €	
		1	Tester	8	29,00 €	232,00 €		

Tabla 137. Presupuesto. Despliegue

B.9 Cierre de proyecto

I1	I2	I3	Descripción	Horas	Cantidad	Subtotal (1)	Subtotal (2)	Total
1			***Cierre de proyecto***					**1.227,20 €**
	1		Cierre del prespuesto de cliente				28,00 €	
		1	Jefe de proyecto	0,5	56,00 €	28,00 €		
	2		Definición de ampliaciones futuras				720,00 €	
		1	Desarrollador de software	8	34,00 €	272,00 €		
		2	Jefe de proyecto	8	56,00 €	448,00 €		
	3		Cambios en la documentación				272,00 €	
		1	Desarrollador de software	8	34,00 €	272,00 €		
	4		Guardar copia de código y documentación para consultas futuras				11,20 €	
		1	Jefe de proyecto	0,2	56,00 €	11,20 €		
	5		Cierre memoria				168,00 €	
		1	Jefe de proyecto	3	56,00 €	168,00 €		
	6		Defensa TFG				28,00 €	
		1	Jefe de proyecto	0,5	56,00 €	28,00 €		

Tabla 138. Presupuesto. Cierre de proyecto

B.10 Reuniones

I1	I2	I3	Descripción	Horas	Cantidad	Subtotal	Total
1			**Reuniones con el cliente**				**196,00 €**
	1		Reunión - Toma de contacto				
		1	Jefe de proyecto	0,5	56,00 €	28,00 €	
	2		Reunión - Estudio de viabilidad				
		1	Jefe de proyecto	0,5	56,00 €	28,00 €	
	3		Reunión - Arranque de proyecto				
		1	Jefe de proyecto	0,5	56,00 €	28,00 €	
	4		Reunión - Principio de Análisis				
		1	Jefe de proyecto	0,5	56,00 €	28,00 €	
	5		Reunión - Fin de Análisis				

		1	Jefe de proyecto	0,5	56,00 €	28,00 €	
	6		Reunión - Fin de Diseño				
		1	Jefe de proyecto	0,5	56,00 €	28,00 €	
	7		Reunión - Fin implementación				
		1	Jefe de proyecto	0,5	56,00 €	28,00 €	

Tabla 139. Presupuesto. Reuniones

B.11 Hardware

El proyecto tiene una duración de 1046,7 horas.

	Cantidad	Precio/unidad	Subtotal	Total
Hardware				**2.353,00 €**
Portátil	4	449,00 €	1.796,00 €	
Tablet	2	209,00 €	418,00 €	
Dispositivo móvil	1	139,00 €	139,00 €	

Tabla 140. Presupuesto. Hardware

B.12 Costes indirectos

El proyecto tiene una duración de 1046,7 horas.

Servicio	Coste hora	Coste proyecto
Consumo de electricidad	0,25 €	261,68 €
Cuota de Internet	0,20 €	209,34 €
Total		**471,02 €**

Tabla 141. Presupuesto. Costes indirectos

C. ENCRIPTACIÓN DE LOS VOTOS

En este apartado se explicará cómo funciona la encriptación de los votos.

La tarea de encriptación de los ballots (preguntas) comienza en el puesto de votación en la siguiente función:

`Postazione/src/main/java/postazione/controller/Controller.askForNonces`

Esa función, solicita a la urna virtual los nonces (números aleatorios) que se necesitan para encriptar los votos de los usuarios. Recupera y rellena un vector de enteros con el máximo de preferencias para cada ballot.

En caso de que haya 3 ballots con 3, 4, 1 máximo de preferencias, se devolverá un vector {3, 4, 1}.

Una vez, la urna reciba la solicitud, llama a la siguiente función:

`Urna/src/main/java/urna/controller/Controller.genNonces`

```
String [][] genNonces(InetAddress ipPost, int[] structure) throws PEException {


String sessionKey = db.getTerminalSessionKey(urn.getProcedureCode(),
urn.getSessionCode(), ipPost, Terminals.Type.Post);


ArrayList<ArrayList<Integer>> voteNonces =
      NonceManager.genMultipleNonces(structure);


String [][] encryptedNonces =   NonceManager.encryptMultipleNonces(voteNonces,
sessionKey);


urn.setVoteNonces(ipPost, voteNonces);



return encryptedNonces;
```

Ilustración 115. Urna.Controller.genNonces

Esta función

- Devuelve la clave de sesión del puesto de votación.

- Crea un vector de nonces, de acuerdo con el número de preferencias de los ballots enviados por el post (puesto de votación).
    - La estructura de nuestro ejemplo era {3, 4, 1}
    - Los nonces generados se organizarán de la siguiente manera: {{n00, n01, n02}, {n10, n11, n12, n13}, {n20}}.
- Encripta los nonces utilizando la clave de sesión del puesto de votación.
- Guarda los nonces en un mapa. Asociándolos con la IP del post.
- Devuelve los nonces encriptados para que puedan ser enviados al post.

El post recibe los nonces encriptados {{En00, En01, En02}, {En10, En11, En12, En13}, {En20}} y finalmente puede continuar con la encriptación de las preferencias.

En la siguiente función

`Postazione/src/main/java/postazione/controller/Controller.sendVote`

en

```
…

int i = 0;
for (WrittenBallot ballot : encryptedBallots) {
	ballot.encryptBallot(pubKey, encryptedNonces[i], sessionKey);
	i++;
}
…
```

Ilustración 116. Postazione.Controller.sendVote

Cada ballot continua con la creación del paquete de votación, usando el vector de nonces encriptado, llamando a la función

`Common/src/main/java/model/WrittenBallot.encryptBallot`

Y en particular:

```
int index = 0;
for (String preference: preferencesSet) {
	VotePacket packet = VoteEncryption.encrypt(preference, Kpu_rp,
	encryptedNonces[index], sessionKey);
	index++;

	encryptedVotePackets.add(packet);
}
for (int i = maxPref - index; i > 0; i--) {
	VotePacket emptyPacket =
	VoteEncryption.encrypt(Protocol.emptyPreference,
	Kpu_rp, encryptedNonces[index], sessionKey);
	index++;

	encryptedVotePackets.add(emptyPacket);
}
```

Ilustración 117. Common.WrittenBallot.encryptBallot

La encriptación de cada paquete de votación se realiza en la siguiente función:

`Common/src/main/java/encryption/VoteEncryption.encrypt`

```
	private static VotePacket encrypt (String vote, Key Kpu_rp, String
encryptedNonce, String sessionKey) throws PEException {
		byte [] ki = AES.genKey(RandStrGenerator.gen (64, 128));
		byte [] iv = AES.genIV(RandStrGenerator.gen (16, 32));

		String encryptedVote = AES.encryptVote(vote, ki, iv);
		String encryptedKi = RSA_OAEP.encrypt(ki, Kpu_rp, false);
		String encryptedIv = RSA_OAEP.encrypt(iv, Kpu_rp, false);
		String solvedNonce =
	NonceManager.solveChallenge(encryptedNonce,
	sessionKey, 3);

		VotePacket packet = new VotePacket(encryptedVote,
	encryptedKi, encryptedIv, solvedNonce);
		HMAC.sign(packet, sessionKey);

		return packet;
	}
```

Ilustración 118. Common.VoteEncrypt.encrypt

Primero, se crean el string aleatorio ki (clave simétrica) e iv (valor inicial), utilizando AES, y más concretamente el modo CBC.

Se usan para encriptar encryptedVote (preferencia de voto) y encriptarse a sí mismos utilizando la clave pública del supervisor Kpu_rp.

Para que el post pruebe su identidad ante la urna virtual, debe superar el reto propuesto por el nonce (el reto que se encarga del envío de votos es el tercero, por lo tanto, se pasa como parámetro un "3").

Se crea el paquete de votación que contiene todos los datos e inmediatamente se firma usando la clave de sesión simétrica del post.

Los ballots rellenados con los paquetes de votación se envían a la urna virtual.

La urna recibe y analiza los ballots en

`Urna/src/main/java/urna/controller/Controller.voteReceived`

Y en particular en:

```
…
db.verifyVoteData(procedureCode, sessionCode, voterID, encryptedBallots,
      ipStation.getHostAddress(), ipPost.getHostAddress());


String sessionKey = db.getTerminalSessionKey(procedureCode, sessionCode,     ipPost,
Terminals.Type.Post);


if (!verifyNonces(encryptedBallots, ipPost, sessionKey)) {
…
      return response;
}


if (verifyBallotsHMAC(encryptedBallots, ipPost, sessionKey)) {
      signBallots(encryptedBallots);
      db.storeVotes(procedureCode, sessionCode, voter, encryptedBallots,
      ipStation, ipPost);


      …
}
```

Ilustración 119. Urna.Controller.voteReceived

La función anterior realiza lo siguiente:

- Los datos sobre la sesión, station (mesa electoral), el post y el votante, se comprueban (db.verifyVoteData).
- Los nonces se comprueban (verifyNonces).
- La firma digital se comprueba (verifyBallotsHMAC).

Si todos los controles se superan el voto se guarda en la base de datos (db.storeVotes).

D. INTERNACIONALIZACIÓN DEL SISTEMA

Para llevar a cabo la internacionalización utilizo ResourceBundle que utiliza el idioma que tenga por defecto el sistema. En mi caso, el idioma por defecto es el castellano.

Se muestra el método de traducción:

```
public static String getResourceBundle(String string) {
	return ResourceBundle.getBundle("etiquetas").getString(string);
}
```

Se debe crear un fichero etiquetas_*language*.properties para cada idioma deseado. Por ejemplo, para inglés debería existir un fichero etiquetas_*en*.properties.

Muestro a continuación los ficheros que he creado para español, inglés e italiano:

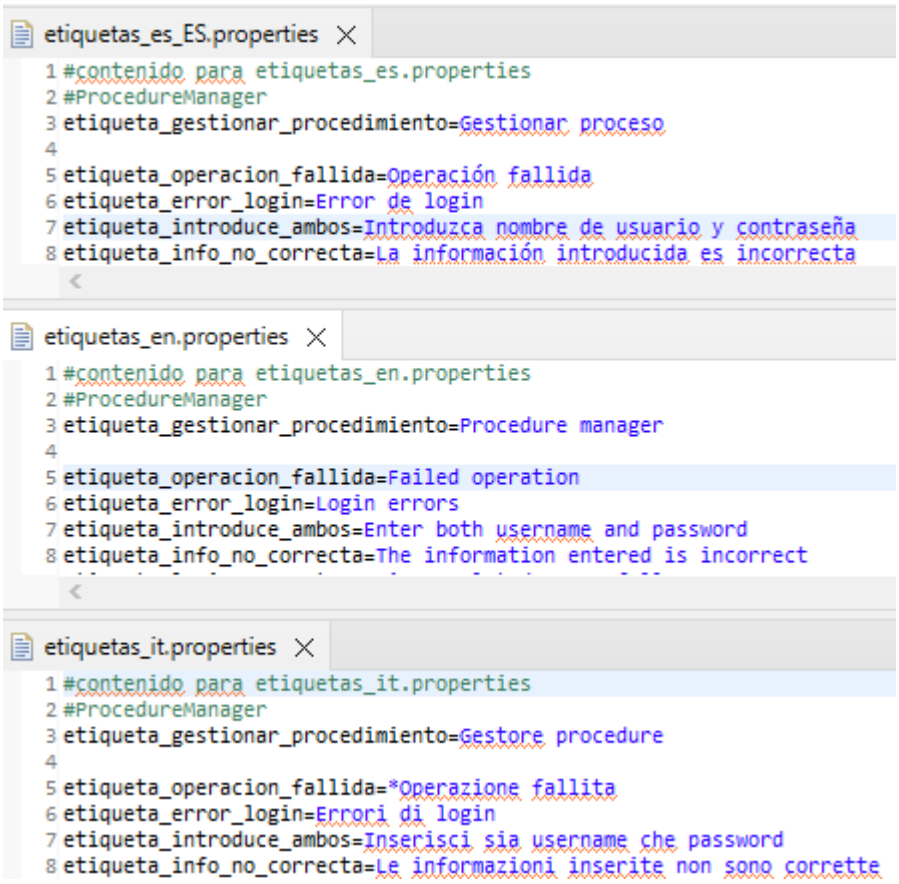

Ilustración 120. Ficheros etiquetas

Si se desea cambiar el idioma a inglés, se debe añadir la línea marcada en amarillo al método de internacionalización:

```
public static String getResourceBundle(String string) {
	Locale.setDefault(new Locale("en", "EN"));
	return ResourceBundle.getBundle("etiquetas").getString(string);
}
```

Por otra parte, he añadido en la Urna un botón para que el usuario pueda cambiar el idioma desde la interfaz:

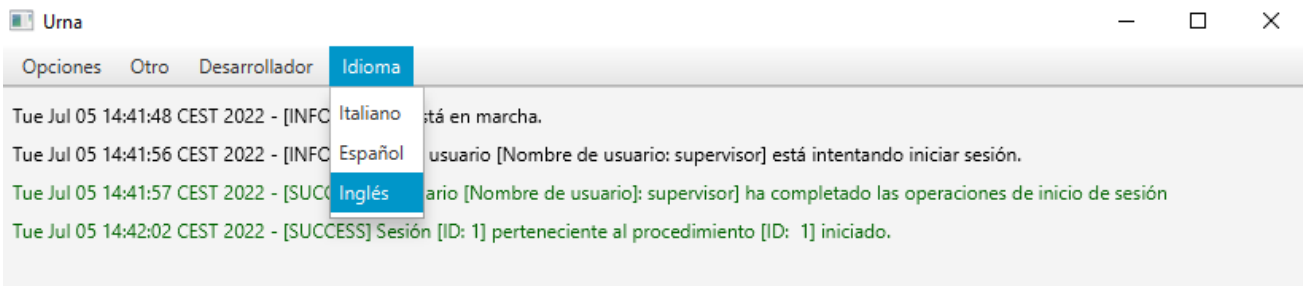

Ilustración 121. Cambiar idioma

Se cambia el idioma del terminal:

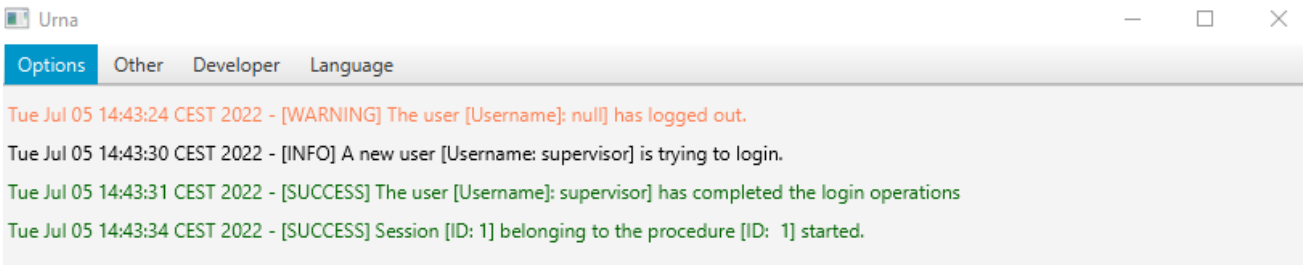

Ilustración 122. Idioma cambiado

E. GLOSARIO

- **Procedure Manager**: Administrador de procesos electorales.
- **Poll**: Escrutinio.
- **Seggio**: Mesa electoral.
- **Postazione**: Puesto de votación.
- **Ballot**: Preguntas de una votación.
- **Nonce**: Número aleatorio, utilizado en tareas criptográficas.

F. REPOSITORIOS

Los repositorios del proyecto son los siguientes:

- **Aplicación de escritorio**: https://github.com/UO264254/evoting
- **Aplicación web:** https://github.com/UO264254/evoting_web

G. REFERENCIAS BIBLIOGRÁFICAS

[1] J. M. Redondo, «Documentos-modelo para Trabajos de Fin de Grado/Master de la Escuela de Informática de Oviedo,» 17 6 2019. [En línea]. Available: https://www.researchgate.net/publication/327882831_Plantilla_de_Proyectos_de_Fin_de_Carrera_de_la_Escuela_de_Informatica_de_Oviedo.

[2] J. Redondo, «Creación y evaluación de plantillas para trabajos de fin de grado como buena práctica docente.,» *Revista de Innovación y Buenas Prácticas Docentes,* p. pp, 2020.

[3] Voto presencial (Elecciones Parlamento Andalucía) - Junta de Andalucía (n.d). Retrieved June 28, 2022, from https://www.eleccionesparlamentoandalucia2018.es/el-proceso-electoral/el-voto-y-sus-modalidades/voto-presencial/

[4] AES vs. RSA Encryption: What Are the Differences? - Precisely (n.d). Retrived June 28, 2022, from https://www.precisely.com/blog/data-security/aes-vs-rsa-encryption-differences

[5] Helios Voting - Helios, Trust the vote (n.d). Retrieved June 28, 2022, from https://vote.heliosvoting.org/

[6] Voto y encuestas telemáticos - Universitat Jaume I (n.d). Retrieved June 28, 2022, from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi4nLa0t7H0AhU0mVwKHe4jCu4QFnoECAQQAQ&url=https%3A%2F%2Fadministracionelectronica.gob.es%2Fpae_Home%2Fdam%2Fjcr%3A8bee806c-bcc9-4be6-aa66-8ca991f8d23b%2F108inciativas-legales.pdf&usg=AOvVaw1DiDcXAydrvjd7hP6Q2bGC

[7] Kuorum (n.d). Retrieved June 28, 2022 from https://kuorum.org/es/

[8] Vicenzo Agate, Alessandra De Paola, Pierluca Ferraro, Giuseppe Lo Re, Marco Morana, «SecureBallot: A secure open source e-Voting system», 2021. Available: https://www.sciencedirect.com/science/article/abs/pii/S1084804521001776?via%3Dihub#!

[9] Formato de direcciones email - RFC5322 (n.d), from https://datatracker.ietf.org/doc/html/rfc5322 and RFC6854(n.d) from https://datatracker.ietf.org/doc/html/rfc5322

[10] Java - Wikipedia (n.d). Retrieved July 02, 2022 from https://en.wikipedia.org/wiki/Java_(programming_language).

[11] JUnit - Wikipedia (n.d). Retrieved July 02, 2022 from https://es.wikipedia.org/wiki/JUnit

[12] Maven - Wikipedia (n.d). Retrieved July 02, 2022 from https://es.wikipedia.org/wiki/Maven

[13] Github - Wikipedia (n.d). Retrieved July 02, 2022 from https://es.wikipedia.org/wiki/GitHub

[14] Eclipse - Wikipedia (n.d). Retrieved July 02, 2022 from https://es.wikipedia.org/wiki/Eclipse_(software)

[15] Java Spring Boot - IBM (n.d). Retrieved July 02, 2022 from https://www.ibm.com/cloud/learn/java-spring-boot

[16] Spring Data JPA - Spring (n.d). Retrieved July 02, 2022 from https://spring.io/projects/spring-data-jpa#:~:text=Spring%20Data%20JPA%20aims%20to,will%20provide%20the%20implementation%20automatically.

[17] Thymeleaf - Wikipedia (n.d). Retrieved July 02, 2022 from https://en.wikipedia.org/wiki/Thymeleaf

[18] Introduction to project lombok - GeeksforGeeks (n.d). Retrieved July 02, 2022 from https://www.geeksforgeeks.org/introduction-to-project-lombok-in-java-and-how-to-get-started/#:~:text=Project%20Lombok%20is%20a%20java,source%20code%20and%20saves%20space.

[19] Guides - Spring (n.d). Retrieved July 03, 2022 from https://spring.io/guides/gs/spring-boot/

[20] Running a Sprint Boot App - Baeldung (n.d). Retrieved July 03, 2022 from https://www.baeldung.com/spring-boot-run-maven-vs-executable-jar.

[21] Run a Java Application from the Command Line - Baeldung (n.d). Retrieved July 03, 2022 from https://www.baeldung.com/java-run-jar-with-arguments.

[22] A Guide to the ResourceBundle - Baeldung (n.d). Retrieved July 03, 2022 from https://www.baeldung.com/java-resourcebundle.

[23] Aquilino A. Juan Fuente, Benjamín López Pérez, «Dirección y Planificación de Próyectós Infórmaticós, Guía de Aprendizaje de la asignatura de Dirección y Planificación de Proyectos Informáticos» Versión 0.087, 2021. Available: https://unioviedo.sharepoint.com/sites/TFG12/Documentos%20compartidos/Forms/AllItems.aspx?id=%2Fsites%2FTFG12%2FDocumentos%20compartidos%2FGeneral%2FMemoria%2FDPPI%2E2019%2E087%2Epdf&parent=%2Fsites%2FTFG12%2FDocumentos%20compartidos%2FGeneral%2FMemoria&p=true&wdLOR=cA8058645%2DF757%2D4F85%2DBD04%2DE51A9AB6C912&ga=1

[24] Installing MySQL on Microsoft Windows - MySQL (n.d). Retrieved July 08, 2022 from https://dev.mysql.com/doc/mysql-installation-excerpt/5.7/en/windows-installation.html

[25] Configuring MySQL to Use Encrypted Connections - Retrieved July 09, 2022 from https://dev.mysql.com/doc/refman/5.7/en/using-encrypted-connections.html

GNU FREE DOCUMENTATION LICENSE

Version 1.3, 3 November 2008

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that

overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "publisher" means any person or entity that distributes copies of the Document to the public.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications",

"Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the

last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. *Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.*
B. *List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.*
C. *State on the Title page the name of the publisher of the Modified Version, as the publisher.*
D. *Preserve all the copyright notices of the Document.*
E. *Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.*
F. *Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.*
G. *Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.*
H. *Include an unaltered copy of this License.*
I. *Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.*
J. *Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the*

Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. *For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.*
L. *Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.*
M. *Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.*
N. *Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.*
O. *Preserve any Warranty Disclaimers.*

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See https://www.gnu.org/licenses/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option

of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING

"Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

```
Copyright (C)  YEAR  YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.3
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled "GNU
Free Documentation License".
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with … Texts." line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.