



UNIVERSIDAD
NACIONAL
DE LA PLATA

FACULTAD DE INFORMÁTICA

TALLER DE PROYECTO 2 INGENIERÍA EN COMPUTACIÓN

G3 – SmartPoll: Sistema de votación segura y transparente con blockchain

Informe de Avance

Grupo de trabajo:

- Blasco, Gonzalo Gabino - Legajo N° 03282/6
- Cabral, Ramiro Nicolás - Legajo N° 03226/6
- Polanis, Iván Valentín - Legajo N° 03266/5

Docente responsable: Gastón Maron

FACULTAD DE INFORMÁTICA

1. Descripción General del Proyecto

El proyecto **SmartPoll** propone el desarrollo de un sistema de votación electrónica basado en blockchain, con el objetivo de superar las limitaciones de los métodos tradicionales y de otras tecnologías previas de voto electrónico. El enfoque principal es garantizar transparencia, verificabilidad y confianza en el proceso electoral, minimizando riesgos de fraude y preservando la privacidad del votante.

La propuesta se centra en implementar un flujo de votación controlado mediante pases de acceso digitales. Cada votante recibe un código QR único, aleatorio y firmado, que valida su derecho a participar. Una vez autenticado, el sistema emite un token anónimo de voto, independiente del QR inicial, que se consume al emitir el sufragio, evitando el doble voto y asegurando la separación entre identidad e intención de voto. El registro final se realiza en una blockchain permissionada, garantizando inmutabilidad, auditoría abierta y conteo verificable.

a) Propuesta original

El diseño inicial incluyó:

- Generación de códigos QR únicos asociados al DNI para autenticar votantes.
- Validación de dichos QR mediante un sistema de ingreso seguro.
- Emisión de un token de voto anónimo tras la validación.
- Registro de cada sufragio como transacción en una blockchain permissionada.
- Conteo automático, público y verificable de los resultados.
- Separación estricta entre la identidad del votante y el contenido del voto.

Se definieron como **objetivos primarios** el desarrollo de la interfaz web, el mecanismo de validación, la interfaz de sufragio y la transparencia del proceso; y como **objetivos secundarios** la posibilidad de soportar múltiples votaciones y el padrón electoral.

b) Propuestas o modificaciones a partir de evaluaciones de la cátedra

Hasta el momento, la **propuesta original se mantiene intacta**, sin cambios solicitados por la cátedra en esta primera etapa.



FACULTAD DE INFORMÁTICA

c) Decisiones propias o complementarias

Durante el desarrollo se modificó el flujo original con el fin de reforzar la seguridad y simplificar la experiencia del votante:

- Se resolvió que el votante solo pueda presentarse con un dispositivo móvil con conexión a internet. Esta decisión elimina el uso de QR impresos, reduciendo riesgos de pérdida, duplicación o falsificación, y asegura que toda la comunicación del pase se realice en forma digital.
- Se decidió que el Token Anónimo de Voto (TAV) no sea entregado al votante, sino generado directamente en la estación de votación. De esta manera, se evita que el votante transporte el TAV y se garantiza que solo se utilice dentro del entorno controlado de la mesa. En este nuevo esquema, es la estación de votación la que habilita al dispositivo de la mesa de ingreso para que se pueda escanear un QR. Una vez escaneado y validado el pase, el dispositivo de ingreso notifica a la estación de votación que se autorice una nueva votación y, en ese momento, se genera el TAV en la propia estación.
- Se decidió realizar el deploy completo de la plataforma en la nube, utilizando Amazon Web Services (AWS) como entorno de producción. Esta decisión tuvo como finalidad asegurar la disponibilidad, estabilidad y coherencia entre los distintos módulos del sistema, permitiendo que tanto el backend como el frontend funcionen de manera integrada bajo condiciones reales de operación.

FACULTAD DE INFORMÁTICA

2. Materiales y Presupuesto

En la **Tabla 1**, se presentan las listas de materiales que serán utilizados para llevar a cabo el proyecto, en ella se detallan: la cantidad, su ubicación y costo unitario.

Componente	Cantidad	Ubicación / Uso	Costo / U (USD)
Raspberry Pi 3 Model B	2	Mesa de ingreso y cuarto oscuro	\$72.00
Cámara USB Logitech C170	1	Mesa de ingreso (lectura de QR-Pase)	\$36.00
Pantalla táctil para Raspberry Pi	1	Cuarto oscuro	\$42.00

Tabla 1: Materiales utilizados en SmartPoll.

Todos los materiales que se observan en la **Tabla 1** ya se encuentran disponibles para ser utilizados en el proyecto. Si bien para el proyecto se requiere de dos Raspberry Pi, solo se dispone de una sola puesto que la interfaz de votación se realizará con una notebook. No se requerirá hardware adicional con fondos de la cátedra.

Además fue necesario contratar servicios en la nube para alojar distintas aplicaciones desarrolladas. La mayoría de servicios utilizados están cubiertos por el *Free-Tier* de Amazon Web Services (AWS), por lo que no representan un costo adicional. Solo poseemos un costo bajo demanda de los siguientes recursos:

- **IPv4 pública:** \$0.005 USD por hora.
- **Instancia t4g.micro de EC2:** \$0.0084 USD por hora.

3. Esquema Gráfico del Proyecto

En la **Figura 1** se representa gráficamente el flujo de SmartPoll.

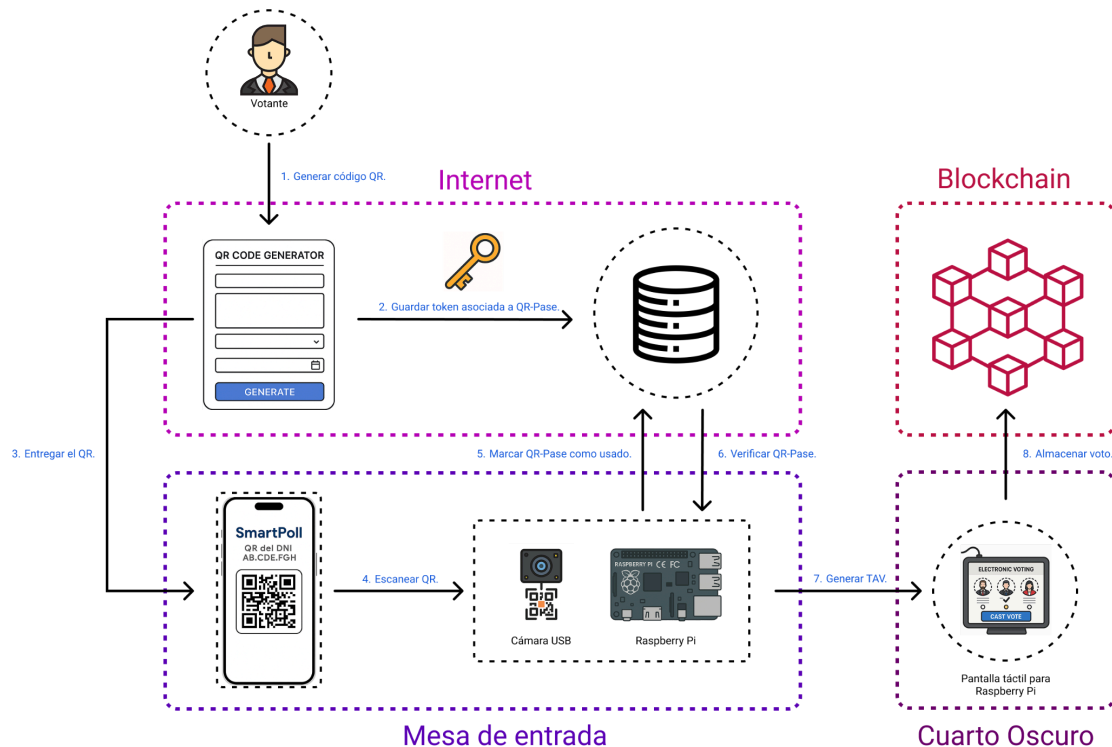


Figura 1: Flujo de funcionamiento de Smartpoll.

A continuación, se detalla cada una de las etapas del flujo representado en la **Figura 1**, describiendo las acciones que realiza el votante y el hardware involucrado en cada paso.

Antes de iniciar el proceso, el votante debe registrarse en la plataforma web, ingresando correo electrónico, DNI y contraseña.

1. **Generación del QR-Pase (Plataforma Web + Servidor en la nube):**
Una vez validado el registro, el sistema genera un token aleatorio y lo asocia a un QR-Pase único y firmado, vinculado al DNI del votante. El QR se muestra en la plataforma para que el votante pueda presentarlo en la mesa de ingreso.
2. **Almacenamiento del token asociado al QR-Pase (Base de datos en la nube):**
El token generado se guarda en la base de datos en la nube, quedando listo para



FACULTAD DE INFORMÁTICA

ser validado en el momento del sufragio.

3. **Presentación del QR-Pase (Dispositivo del votante):**

El votante presenta el QR-Pase en su dispositivo en la mesa de entrada para su verificación.

4. **Escaneo del QR-Pase (Raspberry Pi con cámara USB):**

Una Raspberry Pi equipada con cámara USB escanea el QR-Pase presentado por el votante.

5. **Marcado del QR-Pase como utilizado (Raspberry Pi + Servidor en la nube):**

La Raspberry Pi valida contra la base de datos si el QR-Pase es válido y no ha sido consumido.

- Si es válido, el sistema lo marca como utilizado.
- Si no es válido o ya fue consumido, no se permite el acceso al cuarto oscuro.

6. **Respuesta del servidor (Servidor + SSE activo):**

A través de la conexión SSE, el servidor notifica al cliente que el QR-Pase ya fue consumido. El dispositivo del votante muestra que está habilitado para ingresar al cuarto oscuro y la conexión se cierra.

7. **Generación del TAV de votación (Raspberry Pi en cuarto oscuro):**

Cuando la Raspberry de la mesa de entrada notifica el ingreso de un votante, la Raspberry del cuarto oscuro genera y firma el Token Anónimo de Votación (TAV), habilitando la interfaz de votación. El votante emite su voto, que se envía junto con el TAV firmado al servidor para su validación y registro.

8. **Almacenamiento del TAV en la blockchain permissionada (Servidor + Red blockchain):**

El TAV se registra en la blockchain permissionada, asegurando inmutabilidad, trazabilidad y conteo verificable.

El esquema de conexiones físicas del sistema SmartPoll se caracteriza por su sencillez y modularidad, dado que solo intervienen dos unidades de Raspberry Pi 3 Model B, cada una con un propósito bien definido:



UNIVERSIDAD
NACIONAL
DE LA PLATA

FACULTAD DE INFORMÁTICA

- Raspberry Pi de Mesa de Ingreso: conectada a una cámara USB Logitech C170, encargada de la lectura del QR-Pase presentado por el votante.
- Raspberry Pi del Cuarto Oscuro: conectada a una pantalla táctil, utilizada para la interfaz de votación y emisión del sufragio.

Ambas placas se alimentan mediante un adaptador de 5V y 3A, y se comunican con el servidor alojado en la nube mediante conexión Ethernet o Wi-Fi, dependiendo de la disponibilidad de red.



FACULTAD DE INFORMÁTICA

4. Grado de Avance, Problemas y Soluciones

De acuerdo con lo planificado en el Plan de Proyecto, para la fecha de entrega del Informe de Avance de Octubre se esperaba haber concluido y documentado en la bitácora los siguientes componentes:

- **Interfaz Web:** desarrollo de la plataforma base de interacción.
- **Interfaz de Registro y Escaneo de QR:** implementación de la funcionalidad destinada a validar el acceso mediante la lectura de un código QR.
- **Interfaz de Votación:** diseño y puesta en marcha de la interfaz de usuario destinada a la emisión del voto.

Al momento de la entrega del presente informe, se verificó que las tareas previstas se cumplieron en los plazos acordados, quedando cada una de ellas registradas en la bitácora y debidamente documentadas. En este sentido, el avance planificado para Octubre se corresponde con lo efectivamente alcanzado.

En cuanto al hardware, se realizaron pruebas sobre el **módulo de lectura de QR** y la **comunicación entre el dispositivo móvil de un votante con el backend, y del backend con la Raspberry Pi**.

Se verificaron los siguientes consumos en los dispositivos efectivamente probados:

- **Raspberry Pi**
 - Tensión: 5 V
 - Corriente: 3 A
 - Conector de entrada: Micro-USB
- **Cámara USB (mesa de ingreso)**
 - Tensión: 5 V
 - Corriente: 250–300 mA
 - Alimentación: USB-A

En las próximas etapas se continuará con la integración de los módulos restantes y la validación de la plataforma en condiciones de uso más cercanas a las previstas en el

FACULTAD DE INFORMÁTICA

escenario real. Estas actividades han sido organizadas de forma cronológica en el calendario presentado a continuación.

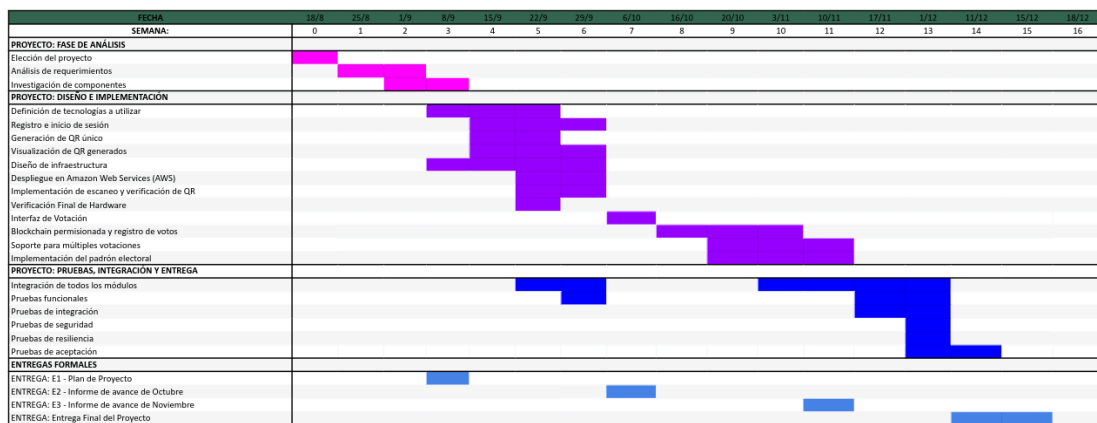


Figura 2: Calendario de avance del proyecto.

En la **Figura 2** se muestra el diagrama de Gantt semanal, donde se señalan tanto las actividades ya completadas como las que restan por realizar. Para una mejor visualización, el diagrama completo puede consultarse en formato ampliado [aquí](#).

FACULTAD DE INFORMÁTICA

Desarrollo Backend

Tecnologías utilizadas

Para el desarrollo del sistema se emplearon diversas tecnologías que permitieron garantizar la eficiencia, escalabilidad y mantenibilidad del proyecto.

- **Lenguaje y framework:** Se utilizó **Java 21.0.8** junto con **Spring Boot**, dado que Java 21 es la versión LTS más reciente, lo que asegura soporte extendido y actualizaciones de seguridad. Spring Boot, por su parte, simplifica la creación de aplicaciones robustas, permitiendo una estructura modular facilitando la gestión de dependencias y configuraciones. Además, el responsable del desarrollo del backend ya contaba con experiencia en este entorno, lo que aceleró el proceso de implementación y redujo la curva de aprendizaje.
- **Entorno de desarrollo (IDE):** El backend fue desarrollado en **IntelliJ IDEA Ultimate**, un entorno que ofrece integración nativa con proyectos Spring Boot, soporte para testing, manejo de control de versiones y herramientas avanzadas para la gestión de dependencias.
- **Dependencias adicionales:** Para mejorar la calidad del código y reducir tareas repetitivas, se incorporaron las siguientes librerías:
 - **Lombok:** utilizada para eliminar la necesidad de escribir manualmente getters, setters, constructores y otros métodos comunes, lo que mejora la legibilidad del código.
 - **MapStruct:** implementada para el mapeo automático entre entidades y Data Transfer Objects (DTOs), evitando la creación manual de clases de conversión y reduciendo posibles errores humanos.

Manejo de datos del usuario

Para la creación de cuentas, se solicitaron los datos mínimos necesarios: DNI, correo electrónico y contraseña. El DNI se representó mediante el tipo Long, en lugar de un String, con el fin de facilitar la validación numérica y evitar inconsistencias por el formato (con o sin puntos). Esta decisión garantiza una representación uniforme en toda la aplicación y simplifica las validaciones de integridad de datos.

Errores y soluciones

- **Necesidad de reiniciar la aplicación tras cada modificación del código en el backend.**

La causa es la configuración por defecto de Spring Boot e IntelliJ IDEA sin soporte para recarga automática.

FACULTAD DE INFORMÁTICA

Cómo solución se incorporó la dependencia Spring Boot DevTools en el archivo `pom.xml`, habilitando el Hot Reload. Luego, se ajustaron las opciones del IDE para permitir la compilación automática incluso con la aplicación en ejecución. Esto mejoró la experiencia de desarrollo y redujo significativamente los tiempos de prueba y ajuste.

- **Dificultad para probar la aplicación en distintos entornos de ejecución (desarrollo, pruebas locales y producción).**

Como solución se definieron perfiles de configuración en Spring Boot:

- `dev`: entorno de desarrollo habitual.
- `local`: pensado para pruebas locales independientes del resto de los servicios.
- `prod`: configurado para el despliegue en la nube (AWS).

De esta forma, cada integrante puede ejecutar el backend con el perfil deseado simplemente configurando la variable de entorno `SPRING_PROFILES_ACTIVE`.

Comunicación en tiempo real

Se desarrollaron las interfaces de usuario para validación de identidad y presentación del QR y la interfaz de votación en el cuarto oscuro.

Para la interacción en tiempo real entre el cliente y el servidor se analizaron principalmente dos alternativas de comunicación:

- **SSE**: permite que el servidor envíe datos de manera continua al cliente a través de una conexión HTTP abierta. Es ideal para aplicaciones en las que la comunicación es principalmente unidireccional, ya que el cliente solo escucha los eventos emitidos por el servidor. Además, es más simple de implementar y mantener.
- **Websockets**: establecen un canal de comunicación **bidireccional** entre cliente y servidor, permitiendo el envío de mensajes en ambos sentidos en tiempo real. Si bien ofrecen mayor flexibilidad, implican una configuración más compleja y un consumo de recursos ligeramente superior.

En base al análisis de las características de ambas comunicaciones se decidió utilizar **SSE** porque la comunicación requerida en este caso es unidireccional: el servidor es quien envía siempre la información al cliente, transmitiendo eventos como el *payload* para generar el QR o la notificación de que el código fue consumido.

FACULTAD DE INFORMÁTICA

Desarrollo frontend y webserver

Frontend

Se decidió desarrollar dos aplicaciones web separadas: una para la interfaz de QR y otra para la interfaz de votación. Para mantener coherencia y facilitar el desarrollo, se optó por utilizar el mismo stack tecnológico en ambas, unificando herramientas, librerías y flujos de trabajo.

Tecnologías utilizadas

Para el desarrollo del sistema se emplearon diversas tecnologías que permitieron garantizar eficiencia, escalabilidad y mantenibilidad.

- **Stack tecnológico:** Se utilizó **Vite**, **React**, **TypeScript** y **SWC** en ambas aplicaciones, con **Node.js** como entorno de ejecución y **Docker** para asegurar consistencia entre los entornos de desarrollo y producción. Esta elección permitió unificar el stack, facilitar la integración de componentes y simplificar la gestión de dependencias y scripts de desarrollo.
- **Gestión de dependencias y compilación:** Se utilizó **pnpm** como gestor de paquetes, por su eficiencia en espacio y velocidad.
- **UI y maquetado:** Para agilizar el desarrollo de la interfaz y garantizar consistencia visual, se emplearon librerías como **TailwindCSS**, **Radix-UI** y **ShadCn**, permitiendo construir componentes reutilizables y estilizados de manera coherente en ambas aplicaciones.
- **Consistencia del entorno:** Se definió una versión específica de **Node.js** (22.19 LTS) y se replicó en **Docker**, asegurando que los entornos de desarrollo y ejecución fueran idénticos y reproducibles.
- **Entorno de desarrollo:** Se utilizó **Visual Studio Code** como editor principal, aprovechando su ecosistema de extensiones, integración con sistemas de control de versiones y herramientas de depuración.

FACULTAD DE INFORMÁTICA

Webserver

Se decidió implementar un webserver dedicado para gestionar la comunicación entre la Raspberry de entrada, la Raspberry del cuarto oscuro y la interfaz de votación. Este servidor se encarga de generar y gestionar los **Tokens Anónimos de Votación (TAV)**, notificar al frontend cuando un votante está autorizado y recibir los votos emitidos para su validación temporal antes de subirlos a la blockchain.

Tecnologías utilizadas

Para el desarrollo del webserver se emplearon diversas tecnologías que permitieron garantizar eficiencia, escalabilidad y mantenibilidad.

- **Stack tecnológico:** Se utilizó **Node.js** y **Express** para levantar el webserver, proporcionando un entorno ligero, flexible y ampliamente conocido. Esta elección permitió definir rutas HTTP para la autorización de votantes y la recepción de votos, así como integrar fácilmente un servidor SSE (Server-Sent Events) para notificaciones en tiempo real hacia la interfaz de votación.
- **Gestión de tokens y persistencia temporal:** Para almacenar los TAVs de manera segura y temporal se utilizó **Redis**, configurado con **TTL** para que los tokens caduquen automáticamente si no son utilizados, evitando que un mismo token pueda ser reutilizado.
- **Consistencia del entorno:** Se definió la misma versión de Node.js (22.19 LTS) que en el frontend y se replicó en Docker, asegurando entornos idénticos y reproducibles, facilitando la escalabilidad y el despliegue.
- **Entorno de desarrollo:** Se utilizó Visual Studio Code como editor principal, aprovechando su ecosistema de extensiones y herramientas de depuración para Node.js.

Comunicación con la interfaz de votación

De manera similar a lo evaluado para la comunicación con la interfaz del QR, se determinó que el webserver debía conectarse con la interfaz de votación mediante SSE para enviar actualizaciones en tiempo real y garantizar un flujo eficiente de información. Por otro lado, la emisión de los votos se realiza mediante peticiones HTTP, lo que simplifica la integración y permite mantener un control claro y seguro sobre la validez de cada voto.



FACULTAD DE INFORMÁTICA

Desarrollo de Arquitectura Cloud y Despliegue

Se avanzó en la implementación de la infraestructura completa del sistema de votación, abarcando tanto el despliegue cloud como la automatización del ciclo de integración y entrega y la definición de infraestructura como código. El proyecto alcanzó un estado funcional estable y escalable, con despliegue automatizado en la nube y conexión entre todos los componentes del sistema.

Arquitectura Cloud

Se diseñó e implementó una arquitectura two-tier sobre AWS, con una subred pública destinada al balanceador de carga y una subred privada que aloja las instancias de aplicación y la base de datos. La arquitectura se replicó en dos *Availability Zones* para garantizar alta disponibilidad y tolerancia a fallos.

La infraestructura se compone de los siguientes servicios principales:

- **ECR:** Registro privado de imágenes Docker integrado con ECS y GitHub Actions.
- **ECS (con EC2):** Orquestación de contenedores con control total del entorno y bajo costo.
- **S3:** Almacenamiento de sitio web estático y archivos públicos.
- **CloudFront:** CDN global para distribución rápida y segura del contenido.
- **ALB (Application Load Balancer):** Balanceo de carga del backend y soporte HTTPS.
- **RDS (PostgreSQL):** Base de datos relacional gestionada en subnets privadas.
- **ACM:** Certificados SSL/TLS gratuitos para el dominio personalizado.
- **IAM:** Gestión de permisos y credenciales seguras para despliegue y CI/CD.

En la **Figura 3** se detalla la integración y conexión de estos servicios en la arquitectura desarrollada en AWS.

FACULTAD DE INFORMÁTICA

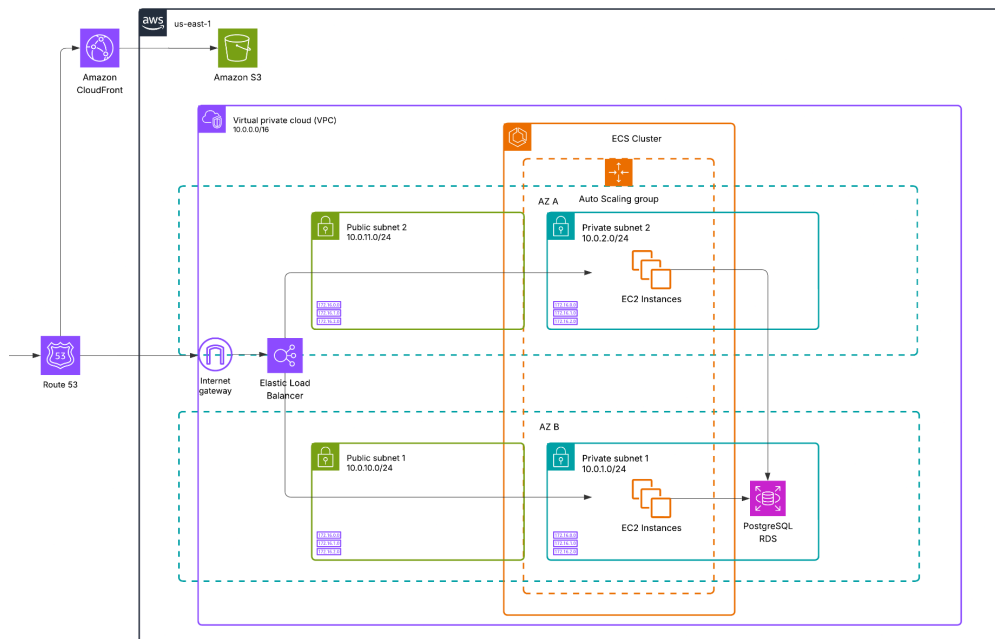


Figura 3: Arquitectura en la nube.

En la **Figura 3** se muestra la arquitectura desarrollada en AWS, compuesta por una parte de acceso público que recibe las requests de los clientes, y una parte privada en la que se alojan las instancias de EC2 y la base de datos PostgreSQL. También, se incluye el Bucket de S3 y la distribución de CloudFront para servir el contenido con mínima latencia a los usuarios.

Además, se utilizó un dominio personalizado adquirido mediante el GitHub Student Pack en get.tech. La validación del dominio se realizó con registros CNAME, y las conexiones HTTP se redirigen automáticamente a HTTPS en ambos extremos (CloudFront y ALB).

CI/CD – Integración y Despliegue Continuo

Para automatizar el proceso de despliegue, se configuraron pipelines mediante GitHub Actions, tanto para el frontend como para el backend.

Para el **Frontend**, se realiza el build del proyecto utilizando el comando `npm run build`, luego se sincronizan los archivos automáticamente con el bucket de S3 preconfigurado. Por último, se invalida la caché de Cloudfront para actualizar el contenido al instante.



FACULTAD DE INFORMÁTICA

Para el **Backend**, se buildea una nueva imagen de Docker y se la almacena en el registro privado de ECR, con un tag correspondiente al hash del commit. Luego, se redefine la tarea de ECS para usar la nueva imagen.

Se aplicó el principio de Least Privilege, utilizando un usuario de IAM dedicado, con permisos estrictamente necesarios para las acciones de despliegue. Las credenciales fueron almacenadas como secrets en GitHub, manteniendo la seguridad del flujo CI/CD.

Este sistema elimina por completo las intervenciones manuales y permite una entrega continua en cada commit a la branch Master.

Terraform – Infraestructura como Código

La totalidad del entorno cloud se gestionó con Terraform, utilizando un diseño modular para mantener la infraestructura ordenada y fácilmente escalable.

Se implementaron módulos independientes para cada componente: ECR, ECS, S3, ELB, VPC, y más adelante se añadieron RDS, CloudFront y Route 53.

Se añadió un archivo `.gitignore` para evitar el versionado de los state files de Terraform, los cuales contienen información sensible.

El flujo de trabajo de Terraform permite planificar y aplicar cambios con los comandos `terraform plan` y `terraform apply`, otorgando despliegues predecibles y reproducibles.

Desarrollo del sistema de lectura de QR-Pase

Como complemento del sistema de votación, se desarrolló un módulo físico para la validación de códigos QR.

Se configuró una Raspberry Pi conectada por Ethernet, accedida mediante SSH, y equipada con una cámara USB. Se instalaron las librerías necesarias para el procesamiento de imágenes y la comunicación con la API.

El script desarrollado en Python ejecuta un bucle continuo que detecta códigos QR mediante la cámara. Cuando se detecta un código válido, se realiza una solicitud POST al endpoint de la API (<https://api.smartpoll.tech/api/qrcode/consume/>) con el contenido del código. Este proceso permite verificar la validez del QR en tiempo real, funcionando como una terminal de registro en la mesa de entrada de la votación.

El sistema fue probado con el frontend y backend locales, validando su correcto funcionamiento y su integración con la API.

FACULTAD DE INFORMÁTICA

5. Documentación Relacionada

5.1 Hardware construido

Al ser este proyecto mayoritariamente de Software, de los físico solo se puede mostrar la Raspberry Pi 3 con cámara USB:



Figura 4: Materiales utilizados para la lectura del código QR.

La **Figura 4** muestra cómo se conecta. Este hardware estará en la mesa de entrada.

5.2 La Interfaz Web

La interfaz web es presentada en el dispositivo móvil del votante. En la **Figura 5** se pueden observar la interfaz de inicio de sesión:

FACULTAD DE INFORMÁTICA



The image shows a web interface for logging into the SmartPoll platform. At the top, there is a QR code with a blue shield icon containing a white padlock, and the text "SMARTPOLL" below it. Below the QR code, the text "Ingresa tus credenciales para acceder a la plataforma de votación" is displayed. There are two input fields: "Email o DNI" and "Contraseña". The "Email o DNI" field has a placeholder text "Ingresa tu email o DNI". The "Contraseña" field has a placeholder text "Ingresa tu contraseña". Below these fields is a dark grey button with a white shield icon and the text "Iniciar Sesión". At the bottom, there is a link that says "¿No tienes una cuenta? Regístrate".

Figura 5: Interfaz Web del inicio de sesión de SmartPoll.

Donde se puede destacar que el usuario puede hacerlo a partir de su Email o DNI, ambos únicos en el sistema, y su contraseña de más de 4 caracteres.

Una vez que el usuario inicia la sesión, se muestra en pantalla el QR-Pase, como se puede ver en la **Figura 6**.

FACULTAD DE INFORMÁTICA



Figura 6: Interfaz Web QR-Pase.

Cuando el código es presentado frente a la cámara de la Raspberry Pi, el sistema lo valida y, una vez verificado, se muestra la siguiente interfaz **Figura 7**.

FACULTAD DE INFORMÁTICA

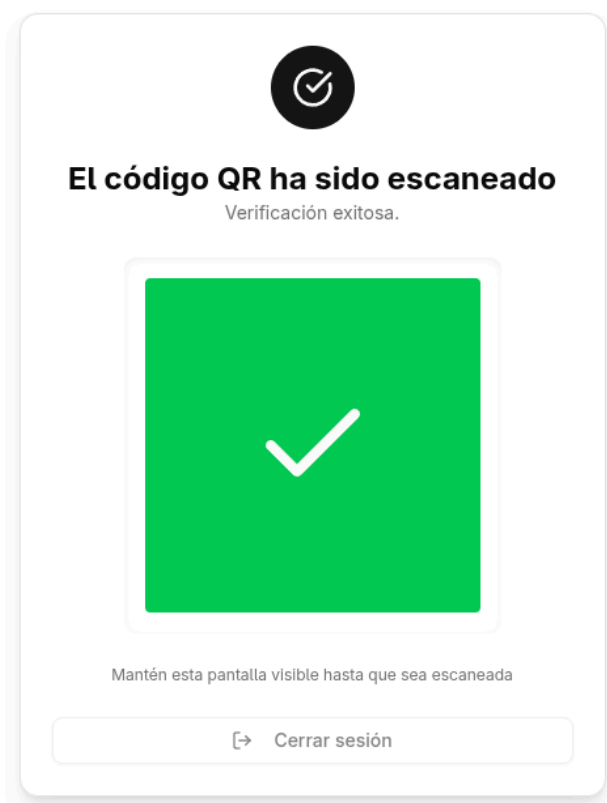


Figura 7: Interfaz Web QR-Pase escaneado con éxito

En esta se observa que se le indica al usuario que ya puede proceder a emitir su voto.

El funcionamiento completo de SmartPoll en la mesa de entrada se encuentra en el siguiente link: <https://youtu.be/DNYplzXZ5zw>

FACULTAD DE INFORMÁTICA

5.3 Interfaz de votación

En la pantalla táctil de la Raspberry Pi del cuarto oscuro, se presenta la interfaz de votación la cual muestra una pantalla de espera, que indica que todavía no hay un usuario que haya escaneado el QR-Pase para votar, como se muestra en la **Figura 8**.



Figura 8: Interfaz de votación de SmartPoll en estado de espera.

Una vez que el usuario escanea con éxito el QR-Pase, la Raspberry Pi de la mesa de entrada se comunica con la de votación, pasando a la pantalla donde el usuario podrá seleccionar al candidato y votar como se presenta en la **Figura 9**.

FACULTAD DE INFORMÁTICA

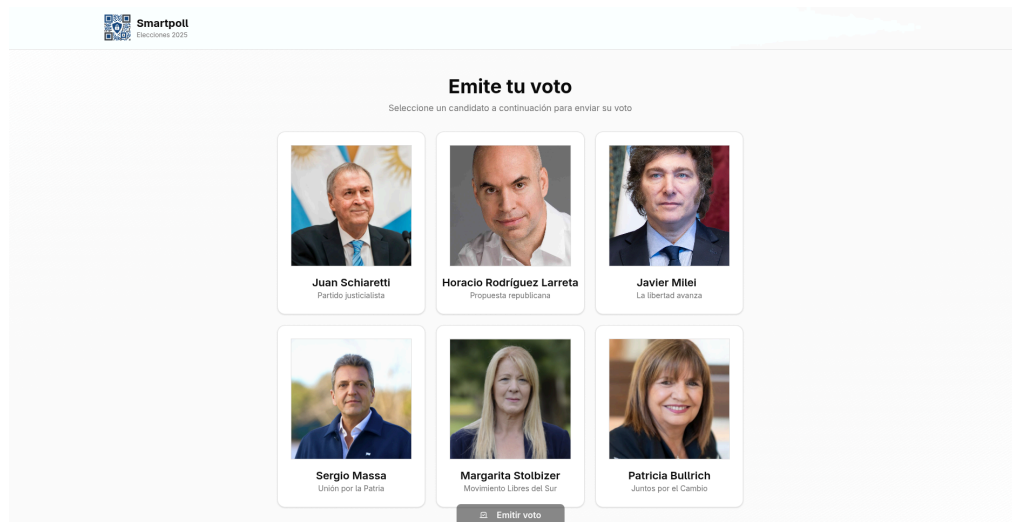


Figura 9: Interfaz de votación de SmartPoll con los candidatos.

5.4 Bibliografía

Algunos links a recursos utilizados para llevar a cabo el proyecto:

- [Hyperledger Fabric Docs](#)
- [Mapstruct Docs](#)
- [Terraform Docs](#)
- [AWS Docs](#)
- [OpenCV Docs](#)
- [Vite](#)
- [React](#)
- [Shaden Docs](#)
- [Spring Boot](#)
- [Server-Sent Events](#)
- [Postman Docs](#)
- [Raspberry Pi 3 Model B Datasheet](#)
- [Webcam C170 Guia](#)
- [Raspberry Pi Touch Display 2 Datasheet](#)

Link al código fuente: <https://github.com/tpII/2025-G3-SmartPoll>

Link al video de presentación: <https://youtu.be/ENbInc9eZks>

Link a la bitácora: <https://github.com/tpII/2025-G3-SmartPoll/wiki/Bit%C3%A1cora>