

[www.gobiernopublico.com](http://www.gobiernopublico.com)

# Gobierno Público - Documento Técnico Integral

---



**gobiernopublico**  
T U V O Z , T U V O T O

## 1. Introducción Tecnológica

Gobierno Público es un sistema distribuido de gobernanza digital que utiliza tecnologías de vanguardia para garantizar transparencia, privacidad, descentralización, trazabilidad y participación ciudadana efectiva. Este documento describe en detalle todos los componentes técnicos del proyecto, incluyendo arquitectura blockchain, privacidad criptográfica, identidad digital, interfaz de usuario, auditoría, y despliegue de infraestructura.

El objetivo de este documento es servir como manual técnico tanto para desarrolladores como para auditores, técnicos de sistemas, investigadores o cualquier parte interesada en comprender a fondo cómo funciona Gobierno Público y qué recursos se requieren para su desarrollo, mantenimiento y escalabilidad futura.

Gobierno Público es un sistema distribuido de gobernanza digital que utiliza tecnologías de vanguardia para garantizar transparencia, privacidad, descentralización, trazabilidad y participación ciudadana efectiva. Este documento describe en detalle todos los componentes técnicos del proyecto, incluyendo arquitectura blockchain, privacidad criptográfica, identidad digital, interfaz de usuario, auditoría, y despliegue de infraestructura.

El objetivo de este documento es servir como manual técnico tanto para desarrolladores como para auditores, técnicos de sistemas, investigadores o cualquier parte interesada en comprender a fondo cómo funciona Gobierno Público y qué recursos se requieren para su desarrollo, mantenimiento y escalabilidad futura.

Gobierno Público es un sistema distribuido de gobernanza digital que utiliza tecnologías de vanguardia para garantizar transparencia, privacidad, descentralización, trazabilidad y participación ciudadana efectiva. Este documento describe en detalle todos los componentes técnicos del proyecto, incluyendo arquitectura blockchain, privacidad criptográfica, identidad digital, interfaz de usuario, auditoría, y despliegue de infraestructura.

El objetivo de este documento es servir como manual técnico tanto para desarrolladores como para auditores, técnicos de sistemas, investigadores o cualquier parte interesada en comprender a fondo cómo funciona Gobierno Público y qué recursos se requieren para su desarrollo, mantenimiento y escalabilidad futura.

Gobierno Público es un sistema distribuido de gobernanza digital que utiliza tecnologías de vanguardia para garantizar transparencia, privacidad, descentralización, trazabilidad y participación ciudadana efectiva. Este documento describe en detalle todos los componentes técnicos del proyecto, incluyendo arquitectura blockchain, privacidad criptográfica, identidad digital, interfaz de usuario, auditoría, y despliegue de infraestructura.

El objetivo de este documento es servir como manual técnico tanto para desarrolladores como para auditores, técnicos de sistemas, investigadores o cualquier parte interesada en comprender a fondo cómo funciona Gobierno Público y qué recursos se requieren para su desarrollo, mantenimiento y escalabilidad futura.

Gobierno Público es un sistema distribuido de gobernanza digital que utiliza tecnologías de vanguardia para garantizar transparencia, privacidad, descentralización, trazabilidad y participación ciudadana efectiva. Este documento describe en detalle todos los componentes técnicos del proyecto, incluyendo arquitectura blockchain, privacidad criptográfica, identidad digital, interfaz de usuario, auditoría, y despliegue de infraestructura.

El objetivo de este documento es servir como manual técnico tanto para desarrolladores como para auditores, técnicos de sistemas, investigadores o cualquier parte interesada en comprender a fondo cómo funciona Gobierno Público y qué recursos se requieren para su desarrollo, mantenimiento y escalabilidad futura.

Gobierno Público es un sistema distribuido de gobernanza digital que utiliza tecnologías de vanguardia para garantizar transparencia, privacidad, descentralización, trazabilidad y participación ciudadana efectiva. Este documento describe en detalle todos los componentes técnicos del proyecto, incluyendo arquitectura blockchain, privacidad criptográfica, identidad digital, interfaz de usuario, auditoría, y despliegue de infraestructura.

El objetivo de este documento es servir como manual técnico tanto para desarrolladores como para auditores, técnicos de sistemas, investigadores o cualquier parte interesada en comprender a fondo cómo funciona Gobierno Público y qué recursos se requieren para su desarrollo, mantenimiento y escalabilidad futura.

Gobierno Público es un sistema distribuido de gobernanza digital que utiliza tecnologías de vanguardia para garantizar transparencia, privacidad, descentralización, trazabilidad y participación ciudadana efectiva. Este documento describe en detalle todos los componentes técnicos del proyecto, incluyendo arquitectura blockchain, privacidad criptográfica, identidad digital, interfaz de usuario, auditoría, y despliegue de infraestructura.

El objetivo de este documento es servir como manual técnico tanto para desarrolladores como para auditores, técnicos de sistemas, investigadores o cualquier parte interesada en comprender a fondo cómo funciona Gobierno Público y qué recursos se requieren para su desarrollo, mantenimiento y escalabilidad futura.

Gobierno Público es un sistema distribuido de gobernanza digital que utiliza tecnologías de vanguardia para garantizar transparencia, privacidad, descentralización, trazabilidad y participación ciudadana efectiva. Este documento describe en detalle todos los componentes técnicos del proyecto, incluyendo arquitectura blockchain, privacidad

criptográfica, identidad digital, interfaz de usuario, auditoría, y despliegue de infraestructura.

El objetivo de este documento es servir como manual técnico tanto para desarrolladores como para auditores, técnicos de sistemas, investigadores o cualquier parte interesada en comprender a fondo cómo funciona Gobierno Público y qué recursos se requieren para su desarrollo, mantenimiento y escalabilidad futura.

Gobierno Público es un sistema distribuido de gobernanza digital que utiliza tecnologías de vanguardia para garantizar transparencia, privacidad, descentralización, trazabilidad y participación ciudadana efectiva. Este documento describe en detalle todos los componentes técnicos del proyecto, incluyendo arquitectura blockchain, privacidad criptográfica, identidad digital, interfaz de usuario, auditoría, y despliegue de infraestructura.

El objetivo de este documento es servir como manual técnico tanto para desarrolladores como para auditores, técnicos de sistemas, investigadores o cualquier parte interesada en comprender a fondo cómo funciona Gobierno Público y qué recursos se requieren para su desarrollo, mantenimiento y escalabilidad futura.

Gobierno Público es un sistema distribuido de gobernanza digital que utiliza tecnologías de vanguardia para garantizar transparencia, privacidad, descentralización, trazabilidad y participación ciudadana efectiva. Este documento describe en detalle todos los componentes técnicos del proyecto, incluyendo arquitectura blockchain, privacidad criptográfica, identidad digital, interfaz de usuario, auditoría, y despliegue de infraestructura.

El objetivo de este documento es servir como manual técnico tanto para desarrolladores como para auditores, técnicos de sistemas, investigadores o cualquier parte interesada en comprender a fondo cómo funciona Gobierno Público y qué recursos se requieren para su desarrollo, mantenimiento y escalabilidad futura.

## 2. Arquitectura General del Sistema

Gobierno Público está compuesto por dos plataformas interconectadas: gobiernopublico.com para votaciones anónimas (en testnet Sepolia) y gobiernopublico.org para votaciones verificadas con identidad (en Polygon). Ambas funcionan como DAOs gobernadas por smart contracts en Aragon y utilizan almacenamiento distribuido y tecnologías de privacidad como zk-SNARKs.

La plataforma sigue una arquitectura modular, donde cada componente puede ser auditado, actualizado o reemplazado sin afectar al resto del sistema. Esta arquitectura garantiza la resiliencia, la posibilidad de escalar horizontalmente, y la compatibilidad con futuros estándares del ecosistema Web3.

Los módulos principales incluyen: gestión de identidades, motor de votación, creación y validación de propuestas, sistema de reputación, análisis de resultados, panel de transparencia, sistema de notificaciones, base de datos descentralizada y capa de frontend adaptativa (web/app).

Gobierno Público está compuesto por dos plataformas interconectadas: gobiernopublico.com para votaciones anónimas (en testnet Sepolia) y gobiernopublico.org para votaciones verificadas con identidad (en Polygon). Ambas funcionan como DAOs gobernadas por smart contracts en Aragon y utilizan almacenamiento distribuido y tecnologías de privacidad como zk-SNARKs.

La plataforma sigue una arquitectura modular, donde cada componente puede ser auditado, actualizado o reemplazado sin afectar al resto del sistema. Esta arquitectura garantiza la resiliencia, la posibilidad de escalar horizontalmente, y la compatibilidad con futuros estándares del ecosistema Web3.

Los módulos principales incluyen: gestión de identidades, motor de votación, creación y validación de propuestas, sistema de reputación, análisis de resultados, panel de transparencia, sistema de notificaciones, base de datos descentralizada y capa de frontend adaptativa (web/app).

Gobierno Público está compuesto por dos plataformas interconectadas: gobiernopublico.com para votaciones anónimas (en testnet Sepolia) y gobiernopublico.org para votaciones verificadas con identidad (en Polygon). Ambas funcionan como DAOs gobernadas por smart contracts en Aragon y utilizan almacenamiento distribuido y tecnologías de privacidad como zk-SNARKs.

La plataforma sigue una arquitectura modular, donde cada componente puede ser auditado, actualizado o reemplazado sin afectar al resto del sistema. Esta arquitectura garantiza la resiliencia, la posibilidad de escalar horizontalmente, y la compatibilidad con futuros estándares del ecosistema Web3.

Los módulos principales incluyen: gestión de identidades, motor de votación, creación y validación de propuestas, sistema de reputación, análisis de resultados, panel de

[www.gobiernopublico.com](http://www.gobiernopublico.com)

transparencia, sistema de notificaciones, base de datos descentralizada y capa de frontend adaptativa (web/app).

Gobierno Público está compuesto por dos plataformas interconectadas: gobiernopublico.com para votaciones anónimas (en testnet Sepolia) y gobiernopublico.org para votaciones verificadas con identidad (en Polygon). Ambas funcionan como DAOs gobernadas por smart contracts en Aragon y utilizan almacenamiento distribuido y tecnologías de privacidad como zk-SNARKs.

La plataforma sigue una arquitectura modular, donde cada componente puede ser auditado, actualizado o reemplazado sin afectar al resto del sistema. Esta arquitectura garantiza la resiliencia, la posibilidad de escalar horizontalmente, y la compatibilidad con futuros estándares del ecosistema Web3.

Los módulos principales incluyen: gestión de identidades, motor de votación, creación y validación de propuestas, sistema de reputación, análisis de resultados, panel de transparencia, sistema de notificaciones, base de datos descentralizada y capa de frontend adaptativa (web/app).

Gobierno Público está compuesto por dos plataformas interconectadas: gobiernopublico.com para votaciones anónimas (en testnet Sepolia) y gobiernopublico.org para votaciones verificadas con identidad (en Polygon). Ambas funcionan como DAOs gobernadas por smart contracts en Aragon y utilizan almacenamiento distribuido y tecnologías de privacidad como zk-SNARKs.

La plataforma sigue una arquitectura modular, donde cada componente puede ser auditado, actualizado o reemplazado sin afectar al resto del sistema. Esta arquitectura garantiza la resiliencia, la posibilidad de escalar horizontalmente, y la compatibilidad con futuros estándares del ecosistema Web3.

Los módulos principales incluyen: gestión de identidades, motor de votación, creación y validación de propuestas, sistema de reputación, análisis de resultados, panel de transparencia, sistema de notificaciones, base de datos descentralizada y capa de frontend adaptativa (web/app).

Gobierno Público está compuesto por dos plataformas interconectadas: gobiernopublico.com para votaciones anónimas (en testnet Sepolia) y gobiernopublico.org para votaciones verificadas con identidad (en Polygon). Ambas funcionan como DAOs gobernadas por smart contracts en Aragon y utilizan almacenamiento distribuido y tecnologías de privacidad como zk-SNARKs.

La plataforma sigue una arquitectura modular, donde cada componente puede ser auditado, actualizado o reemplazado sin afectar al resto del sistema. Esta arquitectura garantiza la resiliencia, la posibilidad de escalar horizontalmente, y la compatibilidad con futuros estándares del ecosistema Web3.

[www.gobiernopublico.com](http://www.gobiernopublico.com)

Los módulos principales incluyen: gestión de identidades, motor de votación, creación y validación de propuestas, sistema de reputación, análisis de resultados, panel de transparencia, sistema de notificaciones, base de datos descentralizada y capa de frontend adaptativa (web/app).

Gobierno Público está compuesto por dos plataformas interconectadas: gobiernopublico.com para votaciones anónimas (en testnet Sepolia) y gobiernopublico.org para votaciones verificadas con identidad (en Polygon). Ambas funcionan como DAOs gobernadas por smart contracts en Aragon y utilizan almacenamiento distribuido y tecnologías de privacidad como zk-SNARKs.

La plataforma sigue una arquitectura modular, donde cada componente puede ser auditado, actualizado o reemplazado sin afectar al resto del sistema. Esta arquitectura garantiza la resiliencia, la posibilidad de escalar horizontalmente, y la compatibilidad con futuros estándares del ecosistema Web3.

Los módulos principales incluyen: gestión de identidades, motor de votación, creación y validación de propuestas, sistema de reputación, análisis de resultados, panel de transparencia, sistema de notificaciones, base de datos descentralizada y capa de frontend adaptativa (web/app).

Gobierno Público está compuesto por dos plataformas interconectadas: gobiernopublico.com para votaciones anónimas (en testnet Sepolia) y gobiernopublico.org para votaciones verificadas con identidad (en Polygon). Ambas funcionan como DAOs gobernadas por smart contracts en Aragon y utilizan almacenamiento distribuido y tecnologías de privacidad como zk-SNARKs.

La plataforma sigue una arquitectura modular, donde cada componente puede ser auditado, actualizado o reemplazado sin afectar al resto del sistema. Esta arquitectura garantiza la resiliencia, la posibilidad de escalar horizontalmente, y la compatibilidad con futuros estándares del ecosistema Web3.

Los módulos principales incluyen: gestión de identidades, motor de votación, creación y validación de propuestas, sistema de reputación, análisis de resultados, panel de transparencia, sistema de notificaciones, base de datos descentralizada y capa de frontend adaptativa (web/app).

Gobierno Público está compuesto por dos plataformas interconectadas: gobiernopublico.com para votaciones anónimas (en testnet Sepolia) y gobiernopublico.org para votaciones verificadas con identidad (en Polygon). Ambas funcionan como DAOs gobernadas por smart contracts en Aragon y utilizan almacenamiento distribuido y tecnologías de privacidad como zk-SNARKs.

La plataforma sigue una arquitectura modular, donde cada componente puede ser auditado, actualizado o reemplazado sin afectar al resto del sistema. Esta arquitectura garantiza la

[www.gobiernopublico.com](http://www.gobiernopublico.com)

resiliencia, la posibilidad de escalar horizontalmente, y la compatibilidad con futuros estándares del ecosistema Web3.

Los módulos principales incluyen: gestión de identidades, motor de votación, creación y validación de propuestas, sistema de reputación, análisis de resultados, panel de transparencia, sistema de notificaciones, base de datos descentralizada y capa de frontend adaptativa (web/app).

Gobierno Público está compuesto por dos plataformas interconectadas: gobiernopublico.com para votaciones anónimas (en testnet Sepolia) y gobiernopublico.org para votaciones verificadas con identidad (en Polygon). Ambas funcionan como DAOs gobernadas por smart contracts en Aragon y utilizan almacenamiento distribuido y tecnologías de privacidad como zk-SNARKs.

La plataforma sigue una arquitectura modular, donde cada componente puede ser auditado, actualizado o reemplazado sin afectar al resto del sistema. Esta arquitectura garantiza la resiliencia, la posibilidad de escalar horizontalmente, y la compatibilidad con futuros estándares del ecosistema Web3.

Los módulos principales incluyen: gestión de identidades, motor de votación, creación y validación de propuestas, sistema de reputación, análisis de resultados, panel de transparencia, sistema de notificaciones, base de datos descentralizada y capa de frontend adaptativa (web/app).

**gobiernopublico**  
T U V O Z , T U V O T O

### **3. Tecnología Blockchain Utilizada**

Gobierno Público utiliza dos blockchains complementarias para garantizar eficiencia y seguridad: Sepolia Testnet (Ethereum) y Polygon Mainnet.

Sepolia es utilizada para pruebas y despliegue de la DAO anónima (.com), permitiendo una participación sin costos de gas. Esta cadena soporta zk-SNARKs a través de integración con Circom y SnarkJS.

Polygon es la red elegida para .org debido a sus bajos costos, alto rendimiento y compatibilidad con Ethereum. Sobre Polygon se despliegan DAOs con Aragon OSx, contratos Governor, y smart contracts personalizados para control de identidades, propuestas y votaciones con KYC.

Todos los contratos son escritos en Solidity, auditados externamente, y versionados con control de cambios. El sistema implementa patrones de seguridad avanzada como UUPS proxy, Guardas de acceso, Check-Effect-Interaction, e integridad de estado en Merkle Trees.

Gobierno Público utiliza dos blockchains complementarias para garantizar eficiencia y seguridad: Sepolia Testnet (Ethereum) y Polygon Mainnet.

Sepolia es utilizada para pruebas y despliegue de la DAO anónima (.com), permitiendo una participación sin costos de gas. Esta cadena soporta zk-SNARKs a través de integración con Circom y SnarkJS.

Polygon es la red elegida para .org debido a sus bajos costos, alto rendimiento y compatibilidad con Ethereum. Sobre Polygon se despliegan DAOs con Aragon OSx, contratos Governor, y smart contracts personalizados para control de identidades, propuestas y votaciones con KYC.

Todos los contratos son escritos en Solidity, auditados externamente, y versionados con control de cambios. El sistema implementa patrones de seguridad avanzada como UUPS proxy, Guardas de acceso, Check-Effect-Interaction, e integridad de estado en Merkle Trees.

Gobierno Público utiliza dos blockchains complementarias para garantizar eficiencia y seguridad: Sepolia Testnet (Ethereum) y Polygon Mainnet.

Sepolia es utilizada para pruebas y despliegue de la DAO anónima (.com), permitiendo una participación sin costos de gas. Esta cadena soporta zk-SNARKs a través de integración con Circom y SnarkJS.

Polygon es la red elegida para .org debido a sus bajos costos, alto rendimiento y compatibilidad con Ethereum. Sobre Polygon se despliegan DAOs con Aragon OSx, contratos Governor, y smart contracts personalizados para control de identidades, propuestas y votaciones con KYC.

Todos los contratos son escritos en Solidity, auditados externamente, y versionados con control de cambios. El sistema implementa patrones de seguridad avanzada como UUPS proxy, Guardas de acceso, Check-Effect-Interaction, e integridad de estado en Merkle Trees.

Gobierno Público utiliza dos blockchains complementarias para garantizar eficiencia y seguridad: Sepolia Testnet (Ethereum) y Polygon Mainnet.

Sepolia es utilizada para pruebas y despliegue de la DAO anónima (.com), permitiendo una participación sin costos de gas. Esta cadena soporta zk-SNARKs a través de integración con Circom y SnarkJS.

Polygon es la red elegida para .org debido a sus bajos costos, alto rendimiento y compatibilidad con Ethereum. Sobre Polygon se despliegan DAOs con Aragon OSx, contratos Governor, y smart contracts personalizados para control de identidades, propuestas y votaciones con KYC.

Todos los contratos son escritos en Solidity, auditados externamente, y versionados con control de cambios. El sistema implementa patrones de seguridad avanzada como UUPS proxy, Guardas de acceso, Check-Effect-Interaction, e integridad de estado en Merkle Trees.

Gobierno Público utiliza dos blockchains complementarias para garantizar eficiencia y seguridad: Sepolia Testnet (Ethereum) y Polygon Mainnet.

Sepolia es utilizada para pruebas y despliegue de la DAO anónima (.com), permitiendo una participación sin costos de gas. Esta cadena soporta zk-SNARKs a través de integración con Circom y SnarkJS.

Polygon es la red elegida para .org debido a sus bajos costos, alto rendimiento y compatibilidad con Ethereum. Sobre Polygon se despliegan DAOs con Aragon OSx, contratos Governor, y smart contracts personalizados para control de identidades, propuestas y votaciones con KYC.

Todos los contratos son escritos en Solidity, auditados externamente, y versionados con control de cambios. El sistema implementa patrones de seguridad avanzada como UUPS proxy, Guardas de acceso, Check-Effect-Interaction, e integridad de estado en Merkle Trees.

Gobierno Público utiliza dos blockchains complementarias para garantizar eficiencia y seguridad: Sepolia Testnet (Ethereum) y Polygon Mainnet.

Sepolia es utilizada para pruebas y despliegue de la DAO anónima (.com), permitiendo una participación sin costos de gas. Esta cadena soporta zk-SNARKs a través de integración con Circom y SnarkJS.

Polygon es la red elegida para .org debido a sus bajos costos, alto rendimiento y compatibilidad con Ethereum. Sobre Polygon se despliegan DAOs con Aragon OSx, contratos Governor, y smart contracts personalizados para control de identidades, propuestas y votaciones con KYC.

Todos los contratos son escritos en Solidity, auditados externamente, y versionados con control de cambios. El sistema implementa patrones de seguridad avanzada como UUPS proxy, Guardas de acceso, Check-Effect-Interaction, e integridad de estado en Merkle Trees.

Gobierno Público utiliza dos blockchains complementarias para garantizar eficiencia y seguridad: Sepolia Testnet (Ethereum) y Polygon Mainnet.

Sepolia es utilizada para pruebas y despliegue de la DAO anónima (.com), permitiendo una participación sin costos de gas. Esta cadena soporta zk-SNARKs a través de integración con Circom y SnarkJS.

Polygon es la red elegida para .org debido a sus bajos costos, alto rendimiento y compatibilidad con Ethereum. Sobre Polygon se despliegan DAOs con Aragon OSx, contratos Governor, y smart contracts personalizados para control de identidades, propuestas y votaciones con KYC.

Todos los contratos son escritos en Solidity, auditados externamente, y versionados con control de cambios. El sistema implementa patrones de seguridad avanzada como UUPS proxy, Guardas de acceso, Check-Effect-Interaction, e integridad de estado en Merkle Trees.

Gobierno Público utiliza dos blockchains complementarias para garantizar eficiencia y seguridad: Sepolia Testnet (Ethereum) y Polygon Mainnet.

Sepolia es utilizada para pruebas y despliegue de la DAO anónima (.com), permitiendo una participación sin costos de gas. Esta cadena soporta zk-SNARKs a través de integración con Circom y SnarkJS.

Polygon es la red elegida para .org debido a sus bajos costos, alto rendimiento y compatibilidad con Ethereum. Sobre Polygon se despliegan DAOs con Aragon OSx, contratos Governor, y smart contracts personalizados para control de identidades, propuestas y votaciones con KYC.

Todos los contratos son escritos en Solidity, auditados externamente, y versionados con control de cambios. El sistema implementa patrones de seguridad avanzada como UUPS proxy, Guardas de acceso, Check-Effect-Interaction, e integridad de estado en Merkle Trees.

Gobierno Público utiliza dos blockchains complementarias para garantizar eficiencia y seguridad: Sepolia Testnet (Ethereum) y Polygon Mainnet.

Sepolia es utilizada para pruebas y despliegue de la DAO anónima (.com), permitiendo una participación sin costos de gas. Esta cadena soporta zk-SNARKs a través de integración con Circom y SnarkJS.

Polygon es la red elegida para .org debido a sus bajos costos, alto rendimiento y compatibilidad con Ethereum. Sobre Polygon se despliegan DAOs con Aragon OSx, contratos Governor, y smart contracts personalizados para control de identidades, propuestas y votaciones con KYC.

[www.gobiernopublico.com](http://www.gobiernopublico.com)

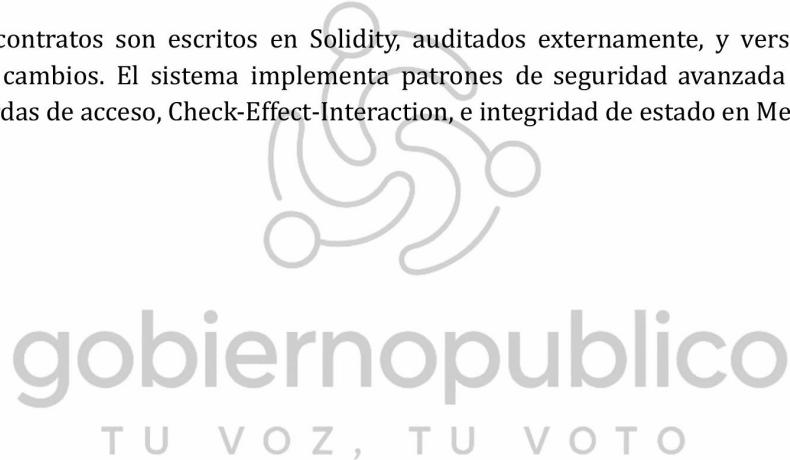
Todos los contratos son escritos en Solidity, auditados externamente, y versionados con control de cambios. El sistema implementa patrones de seguridad avanzada como UUPS proxy, Guardas de acceso, Check-Effect-Interaction, e integridad de estado en Merkle Trees.

Gobierno Público utiliza dos blockchains complementarias para garantizar eficiencia y seguridad: Sepolia Testnet (Ethereum) y Polygon Mainnet.

Sepolia es utilizada para pruebas y despliegue de la DAO anónima (.com), permitiendo una participación sin costos de gas. Esta cadena soporta zk-SNARKs a través de integración con Circom y SnarkJS.

Polygon es la red elegida para .org debido a sus bajos costos, alto rendimiento y compatibilidad con Ethereum. Sobre Polygon se despliegan DAOs con Aragon OSx, contratos Governor, y smart contracts personalizados para control de identidades, propuestas y votaciones con KYC.

Todos los contratos son escritos en Solidity, auditados externamente, y versionados con control de cambios. El sistema implementa patrones de seguridad avanzada como UUPS proxy, Guardas de acceso, Check-Effect-Interaction, e integridad de estado en Merkle Trees.



#### 4. zk-SNARKs y Voto Anónimo

Gobiernopublico.com utiliza pruebas de conocimiento cero (zk-SNARKs) para permitir que los usuarios voten sin revelar su identidad. La implementación incluye un circuito zk en Circom que valida la posesión de una clave única emitida al registrarse.

El proceso sigue estos pasos: (1) El usuario genera un proof localmente; (2) El proof es verificado off-chain; (3) El hash del voto es enviado a un contrato en Sepolia que verifica la validez del proof sin revelar el contenido.

El circuito zk implementa validación de identidad por grupo, previene votos múltiples y asegura unicidad criptográfica. Esta solución garantiza máxima privacidad incluso contra administradores del sistema.

Los votos son almacenados como commits de Merkle Tree, y las raíces actualizadas se guardan en IPFS, sincronizadas con un hash en blockchain para garantizar integridad de largo plazo.

Gobiernopublico.com utiliza pruebas de conocimiento cero (zk-SNARKs) para permitir que los usuarios voten sin revelar su identidad. La implementación incluye un circuito zk en Circom que valida la posesión de una clave única emitida al registrarse.

El proceso sigue estos pasos: (1) El usuario genera un proof localmente; (2) El proof es verificado off-chain; (3) El hash del voto es enviado a un contrato en Sepolia que verifica la validez del proof sin revelar el contenido.

El circuito zk implementa validación de identidad por grupo, previene votos múltiples y asegura unicidad criptográfica. Esta solución garantiza máxima privacidad incluso contra administradores del sistema.

Los votos son almacenados como commits de Merkle Tree, y las raíces actualizadas se guardan en IPFS, sincronizadas con un hash en blockchain para garantizar integridad de largo plazo.

Gobiernopublico.com utiliza pruebas de conocimiento cero (zk-SNARKs) para permitir que los usuarios voten sin revelar su identidad. La implementación incluye un circuito zk en Circom que valida la posesión de una clave única emitida al registrarse.

El proceso sigue estos pasos: (1) El usuario genera un proof localmente; (2) El proof es verificado off-chain; (3) El hash del voto es enviado a un contrato en Sepolia que verifica la validez del proof sin revelar el contenido.

El circuito zk implementa validación de identidad por grupo, previene votos múltiples y asegura unicidad criptográfica. Esta solución garantiza máxima privacidad incluso contra administradores del sistema.

Los votos son almacenados como commits de Merkle Tree, y las raíces actualizadas se guardan en IPFS, sincronizadas con un hash en blockchain para garantizar integridad de largo plazo.

Gobiernopublico.com utiliza pruebas de conocimiento cero (zk-SNARKs) para permitir que los usuarios voten sin revelar su identidad. La implementación incluye un circuito zk en Circom que valida la posesión de una clave única emitida al registrarse.

El proceso sigue estos pasos: (1) El usuario genera un proof localmente; (2) El proof es verificado off-chain; (3) El hash del voto es enviado a un contrato en Sepolia que verifica la validez del proof sin revelar el contenido.

El circuito zk implementa validación de identidad por grupo, previene votos múltiples y asegura unicidad criptográfica. Esta solución garantiza máxima privacidad incluso contra administradores del sistema.

Los votos son almacenados como commits de Merkle Tree, y las raíces actualizadas se guardan en IPFS, sincronizadas con un hash en blockchain para garantizar integridad de largo plazo.

Gobiernopublico.com utiliza pruebas de conocimiento cero (zk-SNARKs) para permitir que los usuarios voten sin revelar su identidad. La implementación incluye un circuito zk en Circom que valida la posesión de una clave única emitida al registrarse.

El proceso sigue estos pasos: (1) El usuario genera un proof localmente; (2) El proof es verificado off-chain; (3) El hash del voto es enviado a un contrato en Sepolia que verifica la validez del proof sin revelar el contenido.

El circuito zk implementa validación de identidad por grupo, previene votos múltiples y asegura unicidad criptográfica. Esta solución garantiza máxima privacidad incluso contra administradores del sistema.

Los votos son almacenados como commits de Merkle Tree, y las raíces actualizadas se guardan en IPFS, sincronizadas con un hash en blockchain para garantizar integridad de largo plazo.

Gobiernopublico.com utiliza pruebas de conocimiento cero (zk-SNARKs) para permitir que los usuarios voten sin revelar su identidad. La implementación incluye un circuito zk en Circom que valida la posesión de una clave única emitida al registrarse.

El proceso sigue estos pasos: (1) El usuario genera un proof localmente; (2) El proof es verificado off-chain; (3) El hash del voto es enviado a un contrato en Sepolia que verifica la validez del proof sin revelar el contenido.

El circuito zk implementa validación de identidad por grupo, previene votos múltiples y asegura unicidad criptográfica. Esta solución garantiza máxima privacidad incluso contra administradores del sistema.

Los votos son almacenados como commits de Merkle Tree, y las raíces actualizadas se guardan en IPFS, sincronizadas con un hash en blockchain para garantizar integridad de largo plazo.

Gobiernopublico.com utiliza pruebas de conocimiento cero (zk-SNARKs) para permitir que los usuarios voten sin revelar su identidad. La implementación incluye un circuito zk en Circom que valida la posesión de una clave única emitida al registrarse.

El proceso sigue estos pasos: (1) El usuario genera un proof localmente; (2) El proof es verificado off-chain; (3) El hash del voto es enviado a un contrato en Sepolia que verifica la validez del proof sin revelar el contenido.

El circuito zk implementa validación de identidad por grupo, previene votos múltiples y asegura unicidad criptográfica. Esta solución garantiza máxima privacidad incluso contra administradores del sistema.

Los votos son almacenados como commits de Merkle Tree, y las raíces actualizadas se guardan en IPFS, sincronizadas con un hash en blockchain para garantizar integridad de largo plazo.

Gobiernopublico.com utiliza pruebas de conocimiento cero (zk-SNARKs) para permitir que los usuarios voten sin revelar su identidad. La implementación incluye un circuito zk en Circom que valida la posesión de una clave única emitida al registrarse.

El proceso sigue estos pasos: (1) El usuario genera un proof localmente; (2) El proof es verificado off-chain; (3) El hash del voto es enviado a un contrato en Sepolia que verifica la validez del proof sin revelar el contenido.

El circuito zk implementa validación de identidad por grupo, previene votos múltiples y asegura unicidad criptográfica. Esta solución garantiza máxima privacidad incluso contra administradores del sistema.

Los votos son almacenados como commits de Merkle Tree, y las raíces actualizadas se guardan en IPFS, sincronizadas con un hash en blockchain para garantizar integridad de largo plazo.

Gobiernopublico.com utiliza pruebas de conocimiento cero (zk-SNARKs) para permitir que los usuarios voten sin revelar su identidad. La implementación incluye un circuito zk en Circom que valida la posesión de una clave única emitida al registrarse.

El proceso sigue estos pasos: (1) El usuario genera un proof localmente; (2) El proof es verificado off-chain; (3) El hash del voto es enviado a un contrato en Sepolia que verifica la validez del proof sin revelar el contenido.

El circuito zk implementa validación de identidad por grupo, previene votos múltiples y asegura unicidad criptográfica. Esta solución garantiza máxima privacidad incluso contra administradores del sistema.

[www.gobiernopublico.com](http://www.gobiernopublico.com)

Los votos son almacenados como commits de Merkle Tree, y las raíces actualizadas se guardan en IPFS, sincronizadas con un hash en blockchain para garantizar integridad de largo plazo.

Gobiernopublico.com utiliza pruebas de conocimiento cero (zk-SNARKs) para permitir que los usuarios voten sin revelar su identidad. La implementación incluye un circuito zk en Circom que valida la posesión de una clave única emitida al registrarse.

El proceso sigue estos pasos: (1) El usuario genera un proof localmente; (2) El proof es verificado off-chain; (3) El hash del voto es enviado a un contrato en Sepolia que verifica la validez del proof sin revelar el contenido.

El circuito zk implementa validación de identidad por grupo, previene votos múltiples y asegura unicidad criptográfica. Esta solución garantiza máxima privacidad incluso contra administradores del sistema.

Los votos son almacenados como commits de Merkle Tree, y las raíces actualizadas se guardan en IPFS, sincronizadas con un hash en blockchain para garantizar integridad de largo plazo.



## 5. Identidad Verificada y KYC en Polygon

Gobiernopublico.org requiere validación de identidad para participar. El sistema integra múltiples proveedores KYC como Civic, Jumio, Fractal y soluciones descentralizadas como Proof of Humanity.

El proceso de verificación no almacena datos personales en cadena. En cambio, se utiliza una firma criptográfica emitida por el proveedor KYC que se asocia a una wallet. Esta firma es validada por un contrato IdentityRegistry.sol.

El usuario verificado obtiene permisos para crear propuestas, votar, moderar y participar en gobernanza avanzada. Este sistema permite establecer pesos de voto según nivel de verificación, reputación, y constancia participativa.

Toda la lógica de permisos y accesos está gestionada en Aragon usando plugins DAO personalizados que integran lógica de reputación y pseudonimato seguro con logs visibles y auditables sin exponer datos sensibles.

Gobiernopublico.org requiere validación de identidad para participar. El sistema integra múltiples proveedores KYC como Civic, Jumio, Fractal y soluciones descentralizadas como Proof of Humanity.

El proceso de verificación no almacena datos personales en cadena. En cambio, se utiliza una firma criptográfica emitida por el proveedor KYC que se asocia a una wallet. Esta firma es validada por un contrato IdentityRegistry.sol.

El usuario verificado obtiene permisos para crear propuestas, votar, moderar y participar en gobernanza avanzada. Este sistema permite establecer pesos de voto según nivel de verificación, reputación, y constancia participativa.

Toda la lógica de permisos y accesos está gestionada en Aragon usando plugins DAO personalizados que integran lógica de reputación y pseudonimato seguro con logs visibles y auditables sin exponer datos sensibles.

Gobiernopublico.org requiere validación de identidad para participar. El sistema integra múltiples proveedores KYC como Civic, Jumio, Fractal y soluciones descentralizadas como Proof of Humanity.

El proceso de verificación no almacena datos personales en cadena. En cambio, se utiliza una firma criptográfica emitida por el proveedor KYC que se asocia a una wallet. Esta firma es validada por un contrato IdentityRegistry.sol.

El usuario verificado obtiene permisos para crear propuestas, votar, moderar y participar en gobernanza avanzada. Este sistema permite establecer pesos de voto según nivel de verificación, reputación, y constancia participativa.

[www.gobiernopublico.com](http://www.gobiernopublico.com)

Toda la lógica de permisos y accesos está gestionada en Aragon usando plugins DAO personalizados que integran lógica de reputación y pseudonimato seguro con logs visibles y auditables sin exponer datos sensibles.

Gobiernopublico.org requiere validación de identidad para participar. El sistema integra múltiples proveedores KYC como Civic, Jumio, Fractal y soluciones descentralizadas como Proof of Humanity.

El proceso de verificación no almacena datos personales en cadena. En cambio, se utiliza una firma criptográfica emitida por el proveedor KYC que se asocia a una wallet. Esta firma es validada por un contrato IdentityRegistry.sol.

El usuario verificado obtiene permisos para crear propuestas, votar, moderar y participar en gobernanza avanzada. Este sistema permite establecer pesos de voto según nivel de verificación, reputación, y constancia participativa.

Toda la lógica de permisos y accesos está gestionada en Aragon usando plugins DAO personalizados que integran lógica de reputación y pseudonimato seguro con logs visibles y auditables sin exponer datos sensibles.

Gobiernopublico.org requiere validación de identidad para participar. El sistema integra múltiples proveedores KYC como Civic, Jumio, Fractal y soluciones descentralizadas como Proof of Humanity.

El proceso de verificación no almacena datos personales en cadena. En cambio, se utiliza una firma criptográfica emitida por el proveedor KYC que se asocia a una wallet. Esta firma es validada por un contrato IdentityRegistry.sol.

El usuario verificado obtiene permisos para crear propuestas, votar, moderar y participar en gobernanza avanzada. Este sistema permite establecer pesos de voto según nivel de verificación, reputación, y constancia participativa.

Toda la lógica de permisos y accesos está gestionada en Aragon usando plugins DAO personalizados que integran lógica de reputación y pseudonimato seguro con logs visibles y auditables sin exponer datos sensibles.

Gobiernopublico.org requiere validación de identidad para participar. El sistema integra múltiples proveedores KYC como Civic, Jumio, Fractal y soluciones descentralizadas como Proof of Humanity.

El proceso de verificación no almacena datos personales en cadena. En cambio, se utiliza una firma criptográfica emitida por el proveedor KYC que se asocia a una wallet. Esta firma es validada por un contrato IdentityRegistry.sol.

El usuario verificado obtiene permisos para crear propuestas, votar, moderar y participar en gobernanza avanzada. Este sistema permite establecer pesos de voto según nivel de verificación, reputación, y constancia participativa.

[www.gobiernopublico.com](http://www.gobiernopublico.com)

Toda la lógica de permisos y accesos está gestionada en Aragon usando plugins DAO personalizados que integran lógica de reputación y pseudonimato seguro con logs visibles y auditables sin exponer datos sensibles.

Gobiernopublico.org requiere validación de identidad para participar. El sistema integra múltiples proveedores KYC como Civic, Jumio, Fractal y soluciones descentralizadas como Proof of Humanity.

El proceso de verificación no almacena datos personales en cadena. En cambio, se utiliza una firma criptográfica emitida por el proveedor KYC que se asocia a una wallet. Esta firma es validada por un contrato IdentityRegistry.sol.

El usuario verificado obtiene permisos para crear propuestas, votar, moderar y participar en gobernanza avanzada. Este sistema permite establecer pesos de voto según nivel de verificación, reputación, y constancia participativa.

Toda la lógica de permisos y accesos está gestionada en Aragon usando plugins DAO personalizados que integran lógica de reputación y pseudonimato seguro con logs visibles y auditables sin exponer datos sensibles.

Gobiernopublico.org requiere validación de identidad para participar. El sistema integra múltiples proveedores KYC como Civic, Jumio, Fractal y soluciones descentralizadas como Proof of Humanity.

El proceso de verificación no almacena datos personales en cadena. En cambio, se utiliza una firma criptográfica emitida por el proveedor KYC que se asocia a una wallet. Esta firma es validada por un contrato IdentityRegistry.sol.

El usuario verificado obtiene permisos para crear propuestas, votar, moderar y participar en gobernanza avanzada. Este sistema permite establecer pesos de voto según nivel de verificación, reputación, y constancia participativa.

Toda la lógica de permisos y accesos está gestionada en Aragon usando plugins DAO personalizados que integran lógica de reputación y pseudonimato seguro con logs visibles y auditables sin exponer datos sensibles.

Gobiernopublico.org requiere validación de identidad para participar. El sistema integra múltiples proveedores KYC como Civic, Jumio, Fractal y soluciones descentralizadas como Proof of Humanity.

El proceso de verificación no almacena datos personales en cadena. En cambio, se utiliza una firma criptográfica emitida por el proveedor KYC que se asocia a una wallet. Esta firma es validada por un contrato IdentityRegistry.sol.

El usuario verificado obtiene permisos para crear propuestas, votar, moderar y participar en gobernanza avanzada. Este sistema permite establecer pesos de voto según nivel de verificación, reputación, y constancia participativa.

[www.gobiernopublico.com](http://www.gobiernopublico.com)

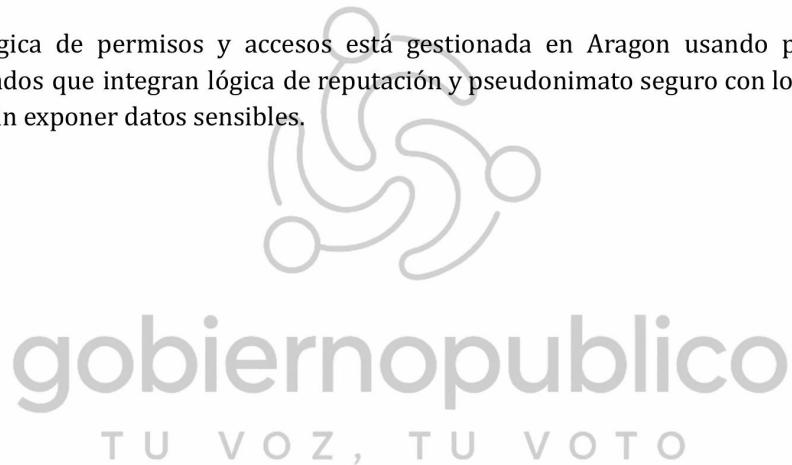
Toda la lógica de permisos y accesos está gestionada en Aragon usando plugins DAO personalizados que integran lógica de reputación y pseudonimato seguro con logs visibles y auditables sin exponer datos sensibles.

Gobiernopublico.org requiere validación de identidad para participar. El sistema integra múltiples proveedores KYC como Civic, Jumio, Fractal y soluciones descentralizadas como Proof of Humanity.

El proceso de verificación no almacena datos personales en cadena. En cambio, se utiliza una firma criptográfica emitida por el proveedor KYC que se asocia a una wallet. Esta firma es validada por un contrato IdentityRegistry.sol.

El usuario verificado obtiene permisos para crear propuestas, votar, moderar y participar en gobernanza avanzada. Este sistema permite establecer pesos de voto según nivel de verificación, reputación, y constancia participativa.

Toda la lógica de permisos y accesos está gestionada en Aragon usando plugins DAO personalizados que integran lógica de reputación y pseudonimato seguro con logs visibles y auditables sin exponer datos sensibles.

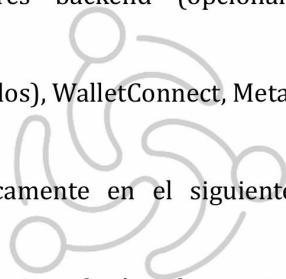


## 6. Mapamento y Esquema Global

Este apartado detalla los procesos, tecnologías y herramientas utilizadas, mediante un mapa mental estructurado del sistema Gobierno Público:

- Infraestructura base: Polygon + Sepolia, IPFS, Web3.Storage
- Módulos: DAO, identidad, votación, propuestas, comparador, reputación, analíticas, transparencia
- Tecnología: Solidity, Circom, React/Next.js, TailwindCSS, ethers.js, The Graph, Node.js
- Seguridad: multisig, auditorías, bug bounty, zk-SNARKs, KYC descentralizado
- Procesos: registro, validación, creación de propuestas, votación, auditoría, visualización
- Hardware mínimo: servidores backend (opcional), frontend CDN, nodos RPC, almacenamiento IPFS pinning
- Integraciones: Chainlink (oráculos), WalletConnect, Metamask, Alchemy API, IPFS gateway, GitHub

Todo esto se representa gráficamente en el siguiente esquema incluido al final del documento.



Este apartado detalla los procesos, tecnologías y herramientas utilizadas, mediante un mapa mental estructurado del sistema Gobierno Público:

- Infraestructura base: Polygon + Sepolia, IPFS, Web3.Storage
- Módulos: DAO, identidad, votación, propuestas, comparador, reputación, analíticas, transparencia
- Tecnología: Solidity, Circom, React/Next.js, TailwindCSS, ethers.js, The Graph, Node.js
- Seguridad: multisig, auditorías, bug bounty, zk-SNARKs, KYC descentralizado
- Procesos: registro, validación, creación de propuestas, votación, auditoría, visualización
- Hardware mínimo: servidores backend (opcional), frontend CDN, nodos RPC, almacenamiento IPFS pinning
- Integraciones: Chainlink (oráculos), WalletConnect, Metamask, Alchemy API, IPFS gateway, GitHub

Todo esto se representa gráficamente en el siguiente esquema incluido al final del documento.

Este apartado detalla los procesos, tecnologías y herramientas utilizadas, mediante un mapa mental estructurado del sistema Gobierno Público:

- Infraestructura base: Polygon + Sepolia, IPFS, Web3.Storage
- Módulos: DAO, identidad, votación, propuestas, comparador, reputación, analíticas, transparencia
- Tecnología: Solidity, Circom, React/Next.js, TailwindCSS, ethers.js, The Graph, Node.js
- Seguridad: multisig, auditorías, bug bounty, zk-SNARKs, KYC descentralizado
- Procesos: registro, validación, creación de propuestas, votación, auditoría, visualización
- Hardware mínimo: servidores backend (opcional), frontend CDN, nodos RPC, almacenamiento IPFS pinning
- Integraciones: Chainlink (oráculos), WalletConnect, Metamask, Alchemy API, IPFS gateway, GitHub

Todo esto se representa gráficamente en el siguiente esquema incluido al final del documento.

Este apartado detalla los procesos, tecnologías y herramientas utilizadas, mediante un mapa mental estructurado del sistema Gobierno Público:

- Infraestructura base: Polygon + Sepolia, IPFS, Web3.Storage
- Módulos: DAO, identidad, votación, propuestas, comparador, reputación, analíticas, transparencia
- Tecnología: Solidity, Circom, React/Next.js, TailwindCSS, ethers.js, The Graph, Node.js
- Seguridad: multisig, auditorías, bug bounty, zk-SNARKs, KYC descentralizado
- Procesos: registro, validación, creación de propuestas, votación, auditoría, visualización
- Hardware mínimo: servidores backend (opcional), frontend CDN, nodos RPC, almacenamiento IPFS pinning
- Integraciones: Chainlink (oráculos), WalletConnect, Metamask, Alchemy API, IPFS gateway, GitHub

Todo esto se representa gráficamente en el siguiente esquema incluido al final del documento.

Este apartado detalla los procesos, tecnologías y herramientas utilizadas, mediante un mapa mental estructurado del sistema Gobierno Público:

- Infraestructura base: Polygon + Sepolia, IPFS, Web3.Storage
- Módulos: DAO, identidad, votación, propuestas, comparador, reputación, analíticas, transparencia

[www.gobiernopublico.com](http://www.gobiernopublico.com)

- Tecnología: Solidity, Circom, React/Next.js, TailwindCSS, ethers.js, The Graph, Node.js
- Seguridad: multisig, auditorías, bug bounty, zk-SNARKs, KYC descentralizado
- Procesos: registro, validación, creación de propuestas, votación, auditoría, visualización
- Hardware mínimo: servidores backend (opcional), frontend CDN, nodos RPC, almacenamiento IPFS pinning
- Integraciones: Chainlink (oráculos), WalletConnect, Metamask, Alchemy API, IPFS gateway, GitHub

Todo esto se representa gráficamente en el siguiente esquema incluido al final del documento.

Este apartado detalla los procesos, tecnologías y herramientas utilizadas, mediante un mapa mental estructurado del sistema Gobierno Público:

- Infraestructura base: Polygon + Sepolia, IPFS, Web3.Storage
- Módulos: DAO, identidad, votación, propuestas, comparador, reputación, analíticas, transparencia
- Tecnología: Solidity, Circom, React/Next.js, TailwindCSS, ethers.js, The Graph, Node.js
- Seguridad: multisig, auditorías, bug bounty, zk-SNARKs, KYC descentralizado
- Procesos: registro, validación, creación de propuestas, votación, auditoría, visualización
- Hardware mínimo: servidores backend (opcional), frontend CDN, nodos RPC, almacenamiento IPFS pinning
- Integraciones: Chainlink (oráculos), WalletConnect, Metamask, Alchemy API, IPFS gateway, GitHub

Todo esto se representa gráficamente en el siguiente esquema incluido al final del documento.

Este apartado detalla los procesos, tecnologías y herramientas utilizadas, mediante un mapa mental estructurado del sistema Gobierno Público:

- Infraestructura base: Polygon + Sepolia, IPFS, Web3.Storage
- Módulos: DAO, identidad, votación, propuestas, comparador, reputación, analíticas, transparencia
- Tecnología: Solidity, Circom, React/Next.js, TailwindCSS, ethers.js, The Graph, Node.js
- Seguridad: multisig, auditorías, bug bounty, zk-SNARKs, KYC descentralizado

[www.gobiernopublico.com](http://www.gobiernopublico.com)

- Procesos: registro, validación, creación de propuestas, votación, auditoría, visualización
- Hardware mínimo: servidores backend (opcional), frontend CDN, nodos RPC, almacenamiento IPFS pinning
- Integraciones: Chainlink (oráculos), WalletConnect, Metamask, Alchemy API, IPFS gateway, GitHub

Todo esto se representa gráficamente en el siguiente esquema incluido al final del documento.

Este apartado detalla los procesos, tecnologías y herramientas utilizadas, mediante un mapa mental estructurado del sistema Gobierno Público:

- Infraestructura base: Polygon + Sepolia, IPFS, Web3.Storage
- Módulos: DAO, identidad, votación, propuestas, comparador, reputación, analíticas, transparencia
- Tecnología: Solidity, Circom, React/Next.js, TailwindCSS, ethers.js, The Graph, Node.js
- Seguridad: multisig, auditorías, bug bounty, zk-SNARKs, KYC descentralizado
- Procesos: registro, validación, creación de propuestas, votación, auditoría, visualización
- Hardware mínimo: servidores backend (opcional), frontend CDN, nodos RPC, almacenamiento IPFS pinning
- Integraciones: Chainlink (oráculos), WalletConnect, Metamask, Alchemy API, IPFS gateway, GitHub

Todo esto se representa gráficamente en el siguiente esquema incluido al final del documento.

Este apartado detalla los procesos, tecnologías y herramientas utilizadas, mediante un mapa mental estructurado del sistema Gobierno Público:

- Infraestructura base: Polygon + Sepolia, IPFS, Web3.Storage
- Módulos: DAO, identidad, votación, propuestas, comparador, reputación, analíticas, transparencia
- Tecnología: Solidity, Circom, React/Next.js, TailwindCSS, ethers.js, The Graph, Node.js
- Seguridad: multisig, auditorías, bug bounty, zk-SNARKs, KYC descentralizado
- Procesos: registro, validación, creación de propuestas, votación, auditoría, visualización
- Hardware mínimo: servidores backend (opcional), frontend CDN, nodos RPC, almacenamiento IPFS pinning

[www.gobiernopublico.com](http://www.gobiernopublico.com)

- Integraciones: Chainlink (oráculos), WalletConnect, Metamask, Alchemy API, IPFS gateway, GitHub

Todo esto se representa gráficamente en el siguiente esquema incluido al final del documento.

Este apartado detalla los procesos, tecnologías y herramientas utilizadas, mediante un mapa mental estructurado del sistema Gobierno Público:

- Infraestructura base: Polygon + Sepolia, IPFS, Web3.Storage
- Módulos: DAO, identidad, votación, propuestas, comparador, reputación, analíticas, transparencia
- Tecnología: Solidity, Circom, React/Next.js, TailwindCSS, ethers.js, The Graph, Node.js
- Seguridad: multisig, auditorías, bug bounty, zk-SNARKs, KYC descentralizado
- Procesos: registro, validación, creación de propuestas, votación, auditoría, visualización
- Hardware mínimo: servidores backend (opcional), frontend CDN, nodos RPC, almacenamiento IPFS pinning
- Integraciones: Chainlink (oráculos), WalletConnect, Metamask, Alchemy API, IPFS gateway, GitHub

Todo esto se representa gráficamente en el siguiente esquema incluido al final del documento.

