REPÚBLICA DEL PARAGUAY

Propuesta de Reforma Electoral

SISTEMA DE VOTO DIGITAL

Módulo Electoral sobre Plataforma Portal Paraguay

Versión 1.0 — Mayo 2026

Este documento propone la implementación de un módulo de voto digital complementario al sistema electoral físico vigente, aprovechando la infraestructura existente del Portal Paraguay y tecnología blockchain para garantizar transparencia, seguridad e inclusión juvenil.

1. Resumen Ejecutivo

Paraguay registra históricamente tasas de participación electoral inferiores al 70%, con el segmento juvenil (18-35 años) como el de mayor ausentismo. Las causas son múltiples: distancia a las mesas de votación, desconfianza en el sistema, y vulnerabilidad al voto asistido fraudulento (acompañamiento indebido en el cuarto oscuro).

Este documento propone un sistema de voto digital complementario al voto físico, construido sobre la plataforma Portal Paraguay ya existente, con verificación biométrica en dos fases, geolocalización registrada con antelación, y registro de votos en blockchain Solana para garantizar inmutabilidad y auditabilidad pública.

El sistema NO reemplaza el voto físico. Actúa como canal adicional accesible, especialmente diseñado para el votante joven y tecnológico, eliminando los vectores de fraude más comunes en Paraguay.

Indicador	Valor
Votantes potenciales	~6,000,000
Adopción digital estimada (primer ciclo)	~2,400,000 (40%)
Ventana de votación digital	2 horas el día de la elección
Plataforma base	Portal Paraguay (MITIC)
Registro blockchain	Red Solana
Costo total estimado de implementación	USD 80,000 – USD 150,000
Costo por transacción (blockchain)	USD 0.0006
Costo blockchain total (6M votos)	USD ~3,600
Fecha objetivo de implementación	Elecciones Generales 2028

2. Diagnóstico del Problema

2.1 Ausentismo Electoral

Paraguay no ha superado el 70% de participación electoral en sus últimas elecciones generales. El segmento de 18 a 35 años representa la mayor proporción del padrón y simultáneamente el grupo con menor concurrencia a las urnas. Las razones identificadas incluyen:

- Distancia física a las mesas de votación, especialmente en jóvenes que residen en departamentos distintos a su domicilio registrado.
- Pérdida de confianza en la integridad del proceso electoral.
- Incompatibilidad horaria con actividades laborales.
- Desconocimiento de la ubicación de la mesa asignada.

2.2 Fraude Electoral Estructural

El mecanismo de fraude más difundido en Paraguay es el voto asistido fraudulento: operadores partidarios que acompañan a votantes vulnerables (adultos mayores, personas analfabetas, ciudadanos en situación de dependencia económica) al interior del cuarto oscuro, exerciendo el voto en su nombre o dirigiendo su elección bajo presión.

Este modelo opera mediante redes de punteros locales que requieren transporte, coordinación territorial y tiempo para rotar entre múltiples votantes. El acarreo masivo a seccionales partidarias es una práctica documentada que distorsiona la representación democrática.

> *El voto digital individual desde dispositivo personal elimina la necesidad del votante de desplazarse, y por tanto elimina al intermediario físico por completo. No hay cuarto oscuro, no hay acompañante.*

2.3 Brecha Tecnológica y Oportunidad

Paradójicamente, el segmento con mayor ausentismo (jóvenes de 18-35 años) es el de mayor penetración de smartphones y el que ya utiliza masivamente la plataforma Portal Paraguay para trámites digitales. Esto representa una oportunidad directa de conversión de usuarios existentes en votantes digitales sin fricción adicional.

3. Descripción del Sistema Propuesto

3.1 Principios de Diseño

- Complementariedad: el voto digital coexiste con el voto físico, no lo reemplaza.
- Mínima fricción: el ciudadano usa una app que ya conoce (Portal Paraguay).
- Verificación de identidad irrepudiable: biometría facial en dos fases.
- Inmutabilidad del voto: registro en blockchain público.
- Resistencia al acarreo: geolocalización registrada con antelación.
- Auditabilidad total: cualquier ciudadano puede verificar el conteo sin ver votos individuales.

3.2 Flujo de Dos Fases

FASE 1 — Registro Previo (10 días hábiles antes de la elección, cierre 48 hs antes)

El ciudadano ingresa a Portal Paraguay y accede al módulo de voto digital. Debe completar:

- Selfie en vivo con detección de movimiento (anti-foto estática).
- Foto del anverso y reverso de la cédula de identidad en tiempo real.
- Registro de ubicación GPS (domicilio habitual o lugar donde votará).
- Confirmación de los datos y aceptación de términos.

El sistema valida la identidad contra la base de datos del Registro Civil y bloquea el registro si el ciudadano ya está inscrito. La ubicación registrada queda bloqueada 48 horas antes de la elección. No se permiten modificaciones posteriores a ese corte.

FASE 2 — Votación Digital (ventana de 2 horas el día de la elección)

Durante la ventana habilitada, el ciudadano registrado accede nuevamente al módulo de voto. El sistema ejecuta:

- Segunda verificación biométrica: selfie en vivo + foto cédula.
- Validación de ubicación GPS contra la ubicación registrada en Fase 1 (margen de tolerancia: 500 metros).
- Presentación de la boleta electoral digital.
- Emisión del voto, encriptado localmente con clave derivada de la cédula electrónica.
- Registro del hash del voto en la blockchain Solana. El voto es único e irrevocable.

> *El voto viaja encriptado. Nadie, ni el Estado ni el TSJE, puede leer el contenido del voto individual. El conteo es verificable matemáticamente mediante pruebas de conocimiento cero (ZK-proofs), sin revelar el voto de ningún ciudadano.*

3.3 Arquitectura Técnica

La arquitectura es híbrida, diseñada para manejar el pico de tráfico electoral sin sobrecargar la infraestructura existente de Portal Paraguay:

Capa	Componente	Responsabilidad
Frontend	Portal Paraguay (app existente)	Interfaz de usuario, cámara, GPS — sin desarrollo nuevo
API Gateway	Microservicio electoral dedicado	Manejo de requests de votación, separado del tráfico normal
Compute	Cloud Burst (AWS/GCP — solo día electoral)	Escala automáticamente de 0 a 100,000 usuarios simultáneos
Identidad	Nube PY + MITIC (Identidad Electrónica)	Validación biométrica y registro civil
Persistencia	Blockchain Solana	Registro inmutable e irrevocable de cada voto emitido
Auditoría	Nodos públicos (TSJE + UNA + Veedores)	Verificación independiente del conteo final

3.4 Gestión del Tráfico Pico

Portal Paraguay opera normalmente con cientos de usuarios simultáneos. El día de una elección general, el módulo de votación digital podría enfrentar entre 80,000 y 100,000 requests simultáneos durante el pico de la ventana de 2 horas. Para esto:

- El módulo de votación corre en infraestructura separada de Portal Paraguay. La app actúa únicamente como puerta de entrada (frontend).
- El procesamiento real del voto se delega a un microservicio en cloud burst, activado 2 horas antes de la ventana y desactivado 2 horas después.
- El resto de los servicios de Portal Paraguay (trámites, documentos) funcionan con normalidad ese día.
- Se realizan pruebas de carga previas simulando 150,000 usuarios simultáneos para certificar resistencia.

4. Mecanismos de Seguridad Anti-Fraude

Vector de Fraude	Mecanismo de Mitigación
Voto asistido / acompañante en cuarto oscuro	El voto es individual desde celular propio. No hay cuarto oscuro ni desplazamiento.
Acarreo a seccional partidaria	La ubicación de voto se registra con 48 hs de antelación. No se puede cambiar el día de la elección.
Voto múltiple con cédulas falsas	Verificación biométrica facial en tiempo real. Una cédula = una cara = un voto.
Coerción frente al dispositivo	El voto es único e irrevocable. Si alguien te obliga a votar delante suyo, no hay forma de modificarlo — pero tampoco de probar qué votaste.
Manipulación del sistema central	Los votos se registran en blockchain descentralizada. No existe servidor central que manipular.
Padrón inflado con fallecidos/emigrados	Cruce automático con Registro Civil e IPS antes de habilitar registros.
Suplantación de identidad digital	Selfie en vivo con prueba de vida (movimiento aleatorio). Imposible usar foto estática.
Ataque al GPS	El GPS es una verificación secundaria. La biométrica es la verificación primaria e irrepudiable.

5. Estructura de Costos de Implementación

5.1 Desglose por Segmento

Segmento 1 — Módulo de Votación (desarrollo de software)

Ítem	Detalle	Costo Estimado (USD)
Desarrollo módulo electoral en Portal Paraguay	Pantallas de registro, votación, confirmación	20,000 – 35,000
API Gateway microservicio electoral	Backend dedicado, separado de Portal Paraguay	20,000 – 30,000
Smart contract Solana	Lógica de votación + auditoría ZK-proof	25,000 – 40,000
Auditoría de seguridad externa	Penetration testing + revisión de código	30,000 – 50,000
Testing de carga	Simulación de 150,000 usuarios simultáneos	5,000 – 10,000

Segmento 2 — Infraestructura (operación)

Ítem	Detalle	Costo Estimado (USD)
Cloud burst día electoral	AWS/GCP — activación de 4 horas (2 antes + 2 ventana)	10,000 – 20,000
Infraestructura base registro previo	10 días sobre Nube PY (tráfico moderado)	2,000 – 5,000
Nodos observadores blockchain	TSJE + UNA + veedores internacionales	5,000 – 10,000
Transacciones Solana (6M votos)	USD 0.0006 x 6,000,000	~3,600

Segmento 3 — Comunicación y Soporte

Ítem	Detalle	Costo Estimado (USD)
Campaña de registro ciudadano	Difusión digital y en medios durante los 10 días de registro	50,000 – 100,000
Soporte técnico (call center + tutoriales)	Atención durante el registro y el día electoral	20,000 – 40,000

5.2 Resumen de Costos Totales

Escenario	Costo Total Estimado (USD)	Observación
Mínimo	80,000 – 100,000	Equipo local, contratos institucionales
Realista	120,000 – 150,000	Incluye auditoría externa y campaña de comunicación
Con campaña de comunicación amplia	200,000 – 250,000	TV, radio y medios digitales a escala nacional

Referencia: una elección general en Paraguay demanda aproximadamente USD 15,000,000 – USD 20,000,000 en logística física. Este sistema complementario representa entre el 0.5% y el 1.5% de ese presupuesto.

6. Marco Legal e Institucional

6.1 Normativa Existente Relevante

- Decreto 8709/2018 — Base legal del Portal Único de Gobierno (www.paraguay.gov.py).
- Ley 7177/2023 — Portación obligatoria de documentos en formato digital.
- Convenio MITIC-TSJE (vigente) — Cooperación institucional para modernización electoral.

6.2 Modificaciones Legales Necesarias

La implementación del sistema requiere las siguientes reformas al marco normativo:

Reforma necesaria	Instrumento legal	Complejidad política
Reconocimiento del voto digital como canal válido	Modificación del Código Electoral	Alta — requiere mayoría parlamentaria
Habilitación de ventana de 2 horas de voto digital	Resolución del TSJE + respaldo legal	Media
Uso de blockchain para registro oficial de votos	Reglamentación específica del TSJE	Baja — competencia institucional
Obligatoriedad del registro previo para acceder al voto digital	Resolución del TSJE	Baja

6.3 Hoja de Ruta Institucional

Etapa	Período	Hito
Presentación de propuesta	2026	Entrega al TSJE y al Congreso Nacional
Debate legislativo	2026 – 2027	Reforma del Código Electoral
Desarrollo técnico	2027	Construcción del módulo sobre Portal Paraguay
Piloto en elecciones internas	2027	Prueba controlada con partidos voluntarios
Auditoría y certificación	Inicio 2028	Revisión técnica y legal pre-elección
Implementación general	Elecciones Generales 2028	Primer ciclo electoral con voto digital nacional

7. Estado de la Infraestructura Nacional

7.1 Infraestructura Existente

El Estado paraguayo cuenta hoy con los siguientes activos tecnológicos relevantes para este sistema:

Activo	Estado actual	Relevancia para el sistema
Portal Paraguay (app)	Operativa — iOS y Android	Frontend del módulo de votación
Identidad Electrónica MITIC	Operativa — integrada en Portal PY	Verificación biométrica ya implementada
Nube PY	2,500 máquinas virtuales (2025)	Infraestructura base para registro previo
Convenio MITIC-TSJE	Firmado y vigente	Marco institucional de colaboración
CERT-PY 24/7	Operativo desde 2025	Respuesta a incidentes de ciberseguridad
Data Center Tier III (Chaco'i)	Licitado — operativo en dic. 2027	Infraestructura definitiva post-2027

7.2 Brecha de Capacidad y Solución

Portal Paraguay está dimensionado para tráfico administrativo cotidiano distribuido a lo largo del día. El día de una elección general, el módulo de votación enfrentaría un pico de 80,000 a 100,000 usuarios simultáneos, aproximadamente 200 veces el tráfico habitual máximo estimado.

La solución es una arquitectura de cloud burst: el módulo electoral corre en infraestructura elástica separada (AWS o GCP), activada exclusivamente durante el período electoral. Portal Paraguay actúa únicamente como interfaz de usuario. El costo de esta capacidad adicional es de USD 10,000 a USD 20,000 por elección.

> *El Data Center Tier III del MITIC, con capacidad para 5,000 máquinas virtuales y certificación internacional, estará operativo en diciembre de 2027 — justo a tiempo para soportar las elecciones generales de 2028 con soberanía tecnológica plena.*

8. Experiencias Internacionales Comparadas

El voto digital no es un experimento sin antecedentes. Varios países llevan años o décadas implementando sistemas similares, con resultados documentados que validan la propuesta y ofrecen lecciones concretas para Paraguay.

8.1 Estonia — El caso de referencia mundial

Indicador	Dato
Año de inicio del voto por internet	2005
Años de experiencia acumulada	20+ años
Porcentaje de votos digitales en 2023	51.1% — primera vez que superó al voto físico
Participación total en elecciones 2023	63.5% del padrón registrado
Evaluación internacional (OSCE/ODIHR 2023)	"Proceso organizado profesionalmente y con transparencia"
Canal de cambio de voto	Múltiples cambios permitidos durante la ventana — solo cuenta el último
Verificación de identidad	Cédula electrónica con chip + PIN

Estonia comenzó con apenas el 1.9% de votos digitales en 2005 y llegó al 51.1% en 2023, convirtiéndose en el primer país del mundo donde el voto por internet superó al voto físico en una elección nacional. El sistema funciona sobre infraestructura de identidad digital estatal, exactamente el modelo que Paraguay ya tiene con la Identidad Electrónica del MITIC.

> *Lección clave para Paraguay: Estonia no construyó una plataforma electoral desde cero. Construyó el voto digital sobre su infraestructura de identidad electrónica preexistente — el mismo camino que este sistema propone con Portal Paraguay.*

8.2 Brasil — Digitalización del voto físico con resultados probados

Indicador	Dato
Año de implementación completa	2000 — 100% de elecciones digitales
Años de experiencia	25+ años
Fraudes eliminados con la digitalización	Falsificación de cédulas, urnas sustituidas, mapismo, compra de actas
Auditorías de seguridad realizadas	7 ediciones desde 2009 con 148 profesionales especializados

Indicador	Dato
Vulnerabilidades capaces de alterar resultados encontradas	Ninguna en 25 años de auditorías
Modelo de auditoría	Votación paralela pública el día de la elección + hash verificable por partidos

Brasil es el caso más relevante para Paraguay por proximidad geográfica, cultural e institucional. La digitalización del voto eliminó fraudes estructurales que eran sistemáticos en el sistema de papel: sustitución de urnas físicas, adulteración de mapas de resultados, y coerción organizada en zonas rurales. En 25 años de auditorías independientes, nunca se encontró una vulnerabilidad capaz de alterar el resultado de una elección.

Lección clave para Paraguay: Brasil tenía exactamente los mismos problemas de fraude estructural que hoy afectan al sistema paraguayo. La digitalización no los eliminó todos, pero redujo drásticamente los mecanismos más masivos de manipulación.

8.3 Suiza — Implementación gradual con verificabilidad total

Indicador	Dato
Inicio de los primeros ensayos	2003
Cantons actualmente con e-voting activo	4 (Basel-Stadt, St. Gallen, Thurgau, Graubünden)
Adopción en votaciones habilitadas (2024)	~17% de los electores autorizados
Modelo de verificación	Verificabilidad completa individual y universal
Infraestructura	Sistema del Correo Suizo (Swiss Post) — código fuente abierto
Evaluación del gobierno federal	Favorable — expansión continua a nuevos cantones
Data Center Tier III operativo en 2027	Coincide con la hoja de ruta paraguaya

Suiza opera el sistema más auditado del mundo: el código fuente del sistema de votación electrónica es público y cualquier investigador puede revisarlo. El modelo de verificabilidad completa permite a cada ciudadano confirmar que su voto fue registrado tal como lo emitió, y a cualquier observador verificar que el conteo es correcto sin acceder a votos individuales — exactamente el modelo de ZK-proofs propuesto para Paraguay sobre Solana.

Lección clave para Paraguay: la transparencia radical del código y del proceso es lo que genera confianza ciudadana, no los discursos institucionales. Suiza publica el código fuente de sus urnas. La blockchain de Solana es pública por naturaleza.

8.4 Cuadro Comparativo Regional

País	Sistema	Años activo	Resultado principal	Relevancia para PY
Estonia	Voto por internet con cédula electrónica	20+	51% de votos digitales en 2023	Modelo directo — misma arquitectura de identidad
Brasil	Urna electrónica (voto físico digital)	25+	Eliminación de fraudes masivos de papel	Proximidad cultural e institucional
Suiza	E-voting con verificabilidad total	20+	17% adopción en fase piloto; expansión continua	Modelo de código abierto y auditoría
Paraguay (propuesto)	Módulo digital sobre Portal Paraguay + Solana	0 (inicio 2028)	Meta: +15-20% participación juvenil	—

8.5 Advertencias y Lecciones Aprendidas

Los casos internacionales también ofrecen advertencias que el sistema paraguayo debe considerar desde el diseño:

- **Confianza ciudadana:** Estonia registró cierta erosión de confianza en el voto digital cuando partidos políticos cuestionaron su integridad sin evidencia técnica. Comunicación institucional permanente y auditorías abiertas son esenciales.
- **Gradualismo obligatorio:** Suiza detuvo sus ensayos en 2019 tras descubrir vulnerabilidades en una versión experimental. Las reinició en 2023 con un sistema completamente rediseñado. El ritmo gradual y las auditorías externas antes del lanzamiento son no negociables.
- **Resistencia política:** Brasil sigue recibiendo cuestionamientos políticos a pesar de 25 años de auditorías sin hallazgos. La transparencia técnica no elimina el debate político. El sistema debe estar preparado para resistir cuestionamientos sin evidencia.
- **Implementación gradual:** Ninguno de estos países implementó el sistema completo en una sola elección. Los tres comenzaron con pilotos limitados, expandieron gradualmente y solo generalizaron tras múltiples ciclos exitosos. Paraguay debe seguir el mismo camino.

9. Arquitectura Blockchain y Verificación Ciudadana

9.1 Cómo se registra el voto en Solana

El voto no se almacena como una transferencia financiera común. Utiliza dos mecanismos nativos de Solana combinados: un smart contract con lógica electoral y el Memo Program para adjuntar datos permanentes a cada transacción.

Campo en blockchain	Contenido	Visible públicamente
Timestamp	Fecha y hora exacta del voto	✅ Sí
Estado	Válido / Rechazado	✅ Sí
Tipo	Voto Electoral PY-2028	✅ Sí
Wallet emisora	Dirección desechable anónima — no vinculada al nombre del ciudadano	✅ Sí — pero irrastreable
Candidato elegido	Encriptado con clave privada de la cédula del ciudadano	❌ Ilegible sin clave privada
Fee	~USD 0.0006	✅ Sí

La wallet emisora es desechable: se genera una dirección única por ciudadano exclusivamente para esa elección. No tiene historial previo ni conexión pública con la identidad del votante. Solscan la muestra como una dirección anónima sin nombre ni datos personales.

9.2 El Boletín Electoral como NFT

Al cierre de la ventana de votación, el smart contract genera automáticamente un NFT de boletín por cada agrupación de mesas digitales. Este NFT es el equivalente digital del acta física tradicional, con una diferencia fundamental: es inmutable, público y permanente en la blockchain para siempre.

Campo del boletín NFT	Detalle
Identificador	Mesa Digital #00847 — Circunscripción Central / Lambaré
Votos emitidos	Total de votos válidos recibidos en esa agrupación
Resultado por candidato	Nombre, votos absolutos y porcentaje — público y verificable
Votos nulos	Cantidad y porcentaje
Hash raíz	Hash criptográfico que vincula todos los votos individuales del boletín
Timestamp de cierre	Fecha y hora exacta del cierre de la ventana electoral

Campo del boletín NFT	Detalle
Firmas multisig	Firma de cada partido político inscripto (mínimo 60% requerido para mintear)
Firma TSJE	Firma institucional del ente rector — una firma más, no la única

Cualquier ciudadano puede sumar todos los boletines NFT manualmente y verificar que el total nacional coincide con el resultado oficial publicado. Si existe discrepancia, es pública, irrefutable y permanente en la blockchain.

9.3 Gobernanza Multisig — Ningún partido actúa solo

El smart contract de boletines solo puede mintear un NFT si recibe firmas de un mínimo del 60% de los partidos políticos inscritos en esa elección. Cada partido inscripto recibe una wallet oficial registrada en el contrato antes de la elección.

Escenario	Resultado del smart contract
TSJE firma solo	Rechazado automáticamente — quórum insuficiente
Partido dominante + 2 aliados (3 de 10)	Rechazado automáticamente — quórum insuficiente
6 de 10 partidos firman incluyendo oposición	Boletín minteado automáticamente sin intervención humana
Partido se niega a firmar para bloquear proceso	Timeout 4 horas: minteo con firmas recibidas + registro público de quién no firmó
Intento de modificar boletín ya minteado	Imposible — el NFT es inmutable una vez emitido

El TSJE pasa de ser árbitro único a ser un firmante más entre varios. Sin complicidad documentada y públicamente registrada de al menos el 60% de los partidos, ningún resultado puede ser publicado ni modificado.

9.4 Verificación Personal del Ciudadano — Flujo Completo

Momento	Qué puede ver el ciudadano	Dónde
Inmediatamente al votar	Confirmación de registro — sin hash todavía	Portal Paraguay
Al cierre de la ventana (mismo día)	Boletín NFT de su mesa digital con resultados	Solscan / Portal Paraguay
48 horas después	Su hash personal habilitado	Portal Paraguay

Momento	Qué puede ver el ciudadano	Dónde
48 horas después	Confirmación de existencia e integridad del voto	Solscan con el hash
48 horas después (opcional)	Candidato que eligió — requiere su clave privada	Portal Paraguay
Permanente	Conteo total nacional verificable	Solscan — colección de NFT boletines

El hash individual se libera 48 horas después deliberadamente. Esto destruye el modelo de compra de votos: el puntero no puede verificar en tiempo real a quién votó el ciudadano, por lo que no puede garantizar el pago. Sin verificación garantizada, el negocio de la compra de votos colapsa económicamente.

10. Análisis de Vulnerabilidades y Contramedidas

Todo sistema de seguridad debe ser evaluado desde la perspectiva del atacante. A continuación se presentan los cinco vectores de ataque más peligrosos y factibles contra este sistema, ordenados por severidad, junto con sus contramedidas específicas.

> *Principio de diseño: el objetivo no es hacer el fraude imposible — ningún sistema electoral en el mundo lo logra. El objetivo es hacer el fraude exponencialmente más caro, más visible y más difícil de escalar que el beneficio que produce.*

10.1 Infiltración del Registro Civil

Campo	Detalle
Descripción	Un partido con décadas en el poder tiene funcionarios propios en el Registro Civil. Emiten cédulas legítimas con chip NFC válido para identidades ficticias o fallecidos recientes. Todo ocurre por canales oficiales — no hay anomalía técnica detectable.
Severidad	CRÍTICA
Contramedida 1	Cruce en tiempo real con IPS, ANDE y ESSAP: una identidad fabricada no tiene historial de aportes al seguro social ni consumo de servicios públicos. El sistema rechaza registros sin huella de actividad en al menos dos servicios estatales independientes.
Contramedida 2	Auditoría internacional independiente del Registro Civil en los 6 meses previos a cada elección, con acceso completo a los registros de emisión de cédulas del período reciente.
Contramedida 3	Publicación del padrón digital completo en la blockchain 48 horas antes del cierre de registro. Todos los partidos tienen acceso para impugnar registros sospechosos públicamente. Una oposición motivada revisará línea por línea.
Nivel de protección	Alto — requiere complicidad simultánea en Registro Civil, IPS y ANDE, con evidencia digital permanente en múltiples sistemas.

10.2 Compra de Votos con Verificación en Tiempo Real

Campo	Detalle
Descripción	El puntero no falsifica nada. Le paga al ciudadano real para que vote X y muestre el comprobante como prueba. Sin hackeo — solo pobreza y efectivo. El ciudadano es cómplice voluntario, no hay víctima que denuncie.
Severidad	ALTA

Campo	Detalle
Contramedida 1 — Principal	Hash individual diferido 48 horas: el puntero no puede verificar el voto en tiempo real. Sin verificación garantizada no hay pago. Sin pago no hay negocio. El modelo económico del fraude colapsa por sí solo.
Contramedida 2	Campaña educativa masiva: nadie tiene derecho a pedirte tu hash ni tu clave privada. Solicitarlos como condición de pago es delito electoral tipificado específicamente.
Contramedida 3	Reforma penal específica: solicitar, recibir o mostrar el hash o clave privada de un voto como condición de transacción económica es un agravante del delito de compra de votos.
Nivel de protección	Medio-alto — el hash diferido elimina la verificabilidad en tiempo real. El residuo requiere respuesta socioeconómica y legal que excede lo tecnológico.

10.3 Registro Masivo con Identidades Reales Ajenas

Campo	Detalle
Descripción	El atacante identifica ciudadanos reales que no votarán digitalmente (adultos mayores, personas sin smartphone) y se registra en su nombre con sus datos de cédula, controlando la wallet electoral resultante. Las identidades son 100% reales — pasan todos los cruces institucionales.
Severidad	ALTA
Contramedida 1	Confirmación activa por SMS: el ciudadano recibe un código de 6 dígitos en su número registrado en el Registro Civil y debe ingresarlo en 24 horas para activar el registro. Sin confirmación, el registro se cancela automáticamente.
Contramedida 2	Lectura obligatoria del chip NFC de la cédula física durante el registro: el chip contiene datos firmados criptográficamente por el Estado que no pueden replicarse sin la cédula física. Elimina el registro remoto sin posesión del documento original.
Contramedida 3	Liveness detection con acciones aleatorias en tiempo real: parpadeo, movimiento de cabeza, repetición de frase generados aleatoriamente en el momento. Imposible de automatizar masivamente para miles de registros simultáneos.
Nivel de protección	Muy alto — requiere posesión física de la cédula con chip activo, acceso al número de teléfono del ciudadano y su presencia física en tiempo real. Las tres simultáneamente.

10.4 Ataque de Denegación de Servicio (DDoS)

Campo	Detalle
Descripción	No robar votos sino impedir que lleguen. Bombardeo masivo de requests contra el microservicio electoral durante la ventana de 2 horas. Si el sistema cae 40 minutos, millones no pueden votar. La ventana cierra igual. No hay evidencia de fraude, solo 'problemas técnicos'.
Severidad	MEDIA-ALTA
Contramedida 1	Rate limiting por IP: más de 100 requests desde la misma IP en 60 segundos genera bloqueo automático inmediato. Neutraliza ataques de origen concentrado.
Contramedida 2	Cloud burst en AWS/GCP con protección DDoS nativa: ambas plataformas incluyen mitigación volumétrica a escala de infraestructura que absorbe ataques sin impacto al usuario final.
Contramedida 3	Protocolo de extensión de ventana multisig: si el sistema registra caída superior al 30% de disponibilidad por más de 10 minutos consecutivos, se activa automáticamente una extensión. La extensión requiere aprobación por multisig de partidos — el TSJE no puede activarla ni bloquearla unilateralmente.
Nivel de protección	Alto — rate limiting + infraestructura elástica + extensión automática neutralizan el impacto electoral del ataque incluso si técnicamente ocurre.

10.5 Código Malicioso en el Smart Contract

Campo	Detalle
Descripción	El más silencioso. Un desarrollador comprometido introduce una vulnerabilidad microscópica antes del despliegue: una condición que bajo circunstancias específicas cuenta votos diferente a lo declarado. Históricamente el ataque más efectivo en sistemas electorales digitales — no deja huella visible en uso normal.
Severidad	CRÍTICA
Contramedida 1	Código fuente 100% público desde el primer día de desarrollo. Cualquier modificación genera automáticamente un registro inmutable con identidad del autor, timestamp y diff completo del cambio. No existe modificación anónima posible.
Contramedida 2	Mínimo tres auditorías de seguridad independientes por empresas diferentes antes del despliegue, una de reputación internacional. Todos los reportes de auditoría son públicos.
Contramedida 3	Smart contract inmutable post-despliegue: una vez desplegado, el contrato no puede ser modificado por nadie. Cualquier corrección requiere despliegue de nuevo contrato con proceso completo de auditoría y aprobación multisig de todos los partidos.
Contramedida 4	Bug bounty público: recompensa económica oficial para investigadores que encuentren y reporten vulnerabilidades antes del despliegue. Incentiva la revisión externa masiva y descentralizada.

Campo	Detalle
Nivel de protección	Muy alto — transparencia radical + múltiples auditorías + inmutabilidad post-despliegue hacen que cualquier vulnerabilidad intencional sea extremadamente difícil de introducir sin detección previa.

10.6 Matriz Resumen de Vulnerabilidades

Ataque	Severidad	Mitigación principal	Protección
Infiltración del Registro Civil	Crítica	Cruce IPS/ANDE + auditoría internacional + padrón público	Alta
Compra de votos con verificación	Alta	Hash diferido 48hs — sin verificación no hay pago	Medio-alta
Registro masivo con identidades ajenas	Alta	SMS + chip NFC + liveness detection simultáneos	Muy alta
Ataque DDoS día electoral	Media-alta	Rate limiting + cloud burst + extensión multisig	Alta
Código malicioso en smart contract	Crítica	Código público + 3 auditorías + inmutabilidad	Muy alta

11. Preguntas Frecuentes

P: ¿Este sistema reemplaza al voto físico tradicional?

R: No. Es un canal adicional y complementario. El ciudadano siempre podrá concurrir a su mesa de votación física como lo hace hoy. El voto digital es una opción, no una obligación.

P: ¿Qué pasa si no tengo smartphone?

R: El sistema está pensado para ampliar la participación, no para excluir. Quien no tenga smartphone o acceso a internet vota de forma física como siempre. No se pierde ningún derecho.

P: ¿Cómo sé que mi voto no fue alterado?

R: Tu voto queda registrado en la blockchain Solana, una red descentralizada e inmutable. Cada voto genera un hash único que cualquier ciudadano puede verificar públicamente. El contenido del voto está encriptado, pero la existencia y la integridad del registro son auditables por cualquier persona con acceso a internet.

P: ¿El Estado puede saber a quién voté?

R: No. El sistema utiliza encriptación de extremo a extremo: el voto se encripta en tu dispositivo con una clave derivada de tu cédula electrónica antes de ser enviado. Ni el TSJE ni el MITIC tienen acceso al contenido de votos individuales. El conteo se realiza mediante pruebas matemáticas (ZK-proofs) que demuestran el resultado correcto sin revelar ningún voto.

P: ¿Qué pasa si alguien me obliga a votar con el celular delante suyo?

R: El hash de tu voto no es visible hasta 48 horas después de la elección. El puntero no puede verificar en tiempo real a quién votaste, por lo tanto no puede confirmar el pago. Sin confirmación garantizada el negocio de compra de votos colapsa económicamente por sí solo. Adicionalmente, solicitar o recibir el hash de otra persona como condición de pago es un delito electoral tipificado específicamente en la reforma propuesta.

P: ¿Por qué solo 2 horas de ventana de votación?

R: La ventana corta es un mecanismo anti-fraude deliberado. Los operadores de acarreo necesitan tiempo para coordinar redes de punteros en todo el país. Con 2 horas de ventana simultánea en todo el territorio, es logísticamente imposible para cualquier organización cubrir el volumen necesario para influir en el resultado. La ventana corta también simplifica la infraestructura técnica y reduce la superficie de riesgo operacional.

P: ¿Por qué necesito registrarme con 10 días de anticipación?

R: El registro previo tiene dos funciones: (1) permite verificar tu identidad biométrica con tiempo suficiente para detectar irregularidades, y (2) registra tu ubicación de voto con antelación,

haciendo imposible que te trasladen a votar en otro lugar el día de la elección. El corte de 48 horas antes cierra la ventana de manipulación de último momento.

P: ¿Qué pasa si me mudé o estoy de viaje el día de la elección?

R: Durante los 10 días de registro, puedes registrar cualquier ubicación válida como tu punto de voto — incluso si es diferente a tu domicilio registrado en la cédula. Puedes modificarla hasta 48 horas antes de la elección. Esto le da flexibilidad al ciudadano genuino sin abrir una ventana de manipulación de último momento.

P: ¿Qué blockchain se usa y por qué?

R: Se propone la red Solana, que en 2026 procesa aproximadamente 5,500 transacciones por segundo con un costo de USD 0.0006 por transacción. Para 6 millones de votos, el costo total en blockchain es de aproximadamente USD 3,600. Solana fue seleccionada por su velocidad, bajo costo y madurez técnica probada en entornos de alto volumen.

P: ¿Por qué no se construye una app nueva exclusiva para votar?

R: Usar Portal Paraguay como base elimina el costo de desarrollo de una app completa (USD 80,000 – USD 120,000), aprovecha una base de usuarios existente, reutiliza la infraestructura de Identidad Electrónica ya construida y auditada, y genera mayor confianza ciudadana al usar una plataforma estatal ya conocida. Solo se desarrolla el módulo específico de votación.

P: ¿Qué organismos supervisarían el sistema?

R: Se propone un esquema de nodos observadores independientes: el TSJE como ente rector, la Universidad Nacional de Asunción como veedor técnico académico, y veedores internacionales (OEA, misiones electorales). Todos los nodos tienen acceso de lectura a la blockchain en tiempo real durante la elección.

P: ¿Cuándo podría estar listo el sistema?

R: La hoja de ruta propuesta contempla debate legislativo en 2026-2027, desarrollo técnico en 2027, un piloto en elecciones internas partidarias en 2027, y primera implementación nacional en las Elecciones Generales de 2028. Esta fecha coincide con la disponibilidad del nuevo Data Center Tier III del MITIC, que estará operativo en diciembre de 2027.

P: ¿Qué pasa si hay un corte de luz o de internet el día de la elección?

R: El voto digital es complementario. Si hay fallas técnicas, el ciudadano puede concurrir a la mesa física y votar de forma tradicional — siempre que no haya emitido ya su voto digital, lo cual queda registrado en el sistema. El voto físico y el digital son mutuamente excluyentes: quien vota digitalmente queda marcado en el padrón y no puede votar físicamente, y viceversa.

12. Conclusión y Recomendaciones

El sistema de voto digital propuesto representa una solución técnicamente sólida, económicamente accesible y políticamente viable para los dos problemas centrales del sistema electoral paraguayo: el ausentismo juvenil y el fraude por acarreo.

Su fortaleza principal es que no propone construir desde cero: aprovecha una plataforma estatal existente, una base de usuarios activa, y una infraestructura de identidad electrónica ya operativa. El desarrollo incremental necesario es mínimo en comparación con su impacto potencial.

Se recomienda al TSJE y al Congreso Nacional iniciar en 2026 el proceso de reforma del Código Electoral que habilite este canal, con miras a un piloto en elecciones internas de 2027 y la implementación plena en las Elecciones Generales de 2028.

Acción recomendada	Responsable	Plazo
Presentar propuesta al TSJE para evaluación técnica	Proponentes	2026
Iniciar proceso de reforma del Código Electoral en el Congreso	Bloque parlamentario	2026
Conformar comisión técnica MITIC-TSJE-UNA	TSJE + MITIC	2026
Desarrollo del módulo de votación sobre Portal Paraguay	MITIC + proveedor	2027
Piloto en elecciones internas voluntarias	TSJE + partidos	2027
Auditoría técnica y legal internacional	TSJE + OEA	Inicio 2028
Primera elección general con voto digital	TSJE	2028

"Nombrar bien algo es el primer paso para construirlo bien."

Propuesta elaborada con metodología de análisis institucional y tecnológico — Paraguay, Mayo 2026