

CGTS

Abril 2026

Resumen Analítico

Resultados del Predictamen 2

Auditoría para la Solución Tecnológica del Voto Digital EG 2026



Tabla de Contenido

Índice de Tablas	3
Siglas y Acrónimos	4
1. Introducción	5
2. Metodología	6
2.1. Metodología aplicada.....	6
2.1.1. Metodología de Evaluación de Funcionalidades.....	6
2.1.2. Metodología de Análisis de Amenazas y Vulnerabilidades (Seguridad)	7
2.1.3. Metodología de Evaluación del Código Fuente y Documentación	8
3. Alcance a la Auditoría a realizar a la Solución Tecnológica de Voto Digital (STVD)	9
3.1. Alcance de la Evaluación de Funcionalidades	9
3.2. Alcance del Análisis de Amenazas y Vulnerabilidades	10
3.3. Alcance de la Evaluación del Código Fuente y Documentación.....	11
4. Matriz de los Hallazgos Evidenciados en la Auditoría	12
5. Pre-dictamen de la Auditoría	13
Sustento de la Idoneidad.....	13
Salvedad Estratégica y Salvaguardas.....	14
Fase 1: Consolidación y Aseguramiento.....	18
Fase 2: Observación y Protección Avanzada	18
Fase 3: Innovación en Integridad y Confianza.....	18
6. Conclusión General.....	19
7. Referencias Documentales.....	21
8. Glosario de Términos	23

Índice de Tablas

Tabla 1. Cantidad de hallazgos encontrados por proceso	12
--	----

Siglas y Acrónimos

Sigla/Acrónimo	Significado
APIs	Interfaces de Programación de Aplicaciones
BD	Base de Datos
CAPEC	Common Attack Pattern Enumeration and Classification
DNIE	Documento Nacional de Identificación Electrónico
ISSAF	Information Systems Security Assessment Framework
ISTQB	International Software Testing Qualifications Board
ONPE	Oficina Nacional de Procesos Electorales
OWASP	Open Web Application Security Project
PenTest	Prueba de Penetración
RENIEC	Registro Nacional de Identificación y Estado Civil
SDLC	Ciclo de Vida del Desarrollo de Software
STVD	Solución Tecnológica del Voto Digital

1. Introducción

En el contexto del proyecto de auditoría a la Solución Tecnológica de Voto Digital (STVD), el presente informe expone de manera integral el enfoque metodológico, técnico y analítico adoptado por la firma auditora para llevar a cabo su evaluación. Este análisis se desarrolla como un proceso sistemático, independiente y sustentado en criterios técnicos, orientado a determinar el nivel de madurez funcional, la solidez de la seguridad de la información, la calidad del código fuente y la capacidad de sostenibilidad operativa de la solución.

El contenido que se presenta a continuación detalla, de forma estructurada y progresiva, las metodologías aplicadas, el alcance definido en cada línea de evaluación, así como los hallazgos identificados y su impacto en la integridad, disponibilidad y confiabilidad del proceso electoral digital. Asimismo, se incluyen los marcos normativos, estándares internacionales y criterios de referencia considerados, junto con el análisis técnico y estratégico que respalda el pre-dictamen emitido.

Este apartado constituye el sustento técnico y argumentativo sobre el cual se construyen las conclusiones, recomendaciones estratégicas y acciones propuestas, brindando a la ONPE una visión objetiva, clara y orientada a la toma de decisiones respecto al estado actual de la STVD y a las condiciones necesarias para su implementación en futuros procesos electorales de carácter nacional.

2. Metodología

El marco metodológico que se aplicó para llevar a cabo la auditoría a la Solución Tecnológica del Voto Digital se estructuró de manera rigurosa para garantizar la eficacia y la completitud del proceso de revisión y análisis.

En primer lugar, se realizó una fase de planificación detallada, donde se establecieron los objetivos de la auditoría, se definieron los alcances y se identificaron los recursos necesarios. Esta documentación fue entregada a la ONPE para su información. Adicionalmente, se elaboró un cronograma que permitió organizar las actividades y asignar responsabilidades a los miembros del equipo auditor.

Posteriormente, se realizó una fase de recopilación de información, en la que se obtuvo acceso al código fuente del software y se recabaron los documentos y registros relevantes. Se realizaron entrevistas con los responsables del desarrollo y la implementación del software, así como con los encargados de la seguridad de la información.

Al disponer del código fuente y la documentación se procedió al análisis y evaluación de la solución. Esto incluyó la revisión del ciclo de desarrollo de software, la arquitectura de la aplicación, la evaluación de las funcionalidades y el detalle del código fuente. Se aplicaron técnicas de revisión de código, se verificó la implementación de controles de acceso y se evaluó la seguridad del software en términos de protección de datos y prevención de intrusiones. Los hallazgos y las vulnerabilidades identificadas fueron documentados y se elaboraron recomendaciones para mejorar la seguridad y la integridad del software. Finalmente, se generó un informe de auditoría completo que resume los resultados obtenidos y proporcionó orientación para fortalecer la confiabilidad y la protección de la información en el contexto del voto digital.

2.1. Metodología aplicada

2.1.1. Metodología de Evaluación de Funcionalidades

El proceso de auditoría de las funcionalidades de la Solución Tecnológica del Voto Digital (STVD) se ejecutó siguiendo una metodología integral que combina rigurosamente la revisión documental y la observación directa del sistema. Esta aproximación se inició con la revisión y el análisis de la documentación, compuesta por las Especificaciones de Requisitos de Software (ERS), las Reglas de Negocio (RN), las Historias de Usuario (HU), el Manual Técnico (MT) y el Manual de

Usuario (MU). El propósito de esta fase fue validar la existencia, coherencia, actualidad y trazabilidad de toda la documentación funcional de la STVD, asegurando que esta sirva como una fuente de fidedigna, completa, consistente y confiable para el sistema.

La lectura y la revisión documental se basó en la identificación de la consistencia entre la definición de las reglas de negocio, los requerimientos especificados, la definición detallada en las historias de usuario y la implementación final en la Solución Tecnológica del Voto Digital. Además, la revisión consistió en el ordenamiento y la clasificación metódica de todos los requisitos, tanto funcionales como no funcionales, para establecer la correspondencia precisa entre estos, las reglas de negocio y el producto desarrollado. Posteriormente, se realizó un análisis que correspondió a la interpretación técnica y sistémica de los componentes del producto, fundamentado siempre en los requisitos validados, las reglas de negocio aprobadas y el comportamiento observado del producto.

Finalmente, la observación directa se desarrolló detallando el comportamiento de cada funcionalidad en tiempo real. Durante esta etapa se realizaron las validaciones de los requerimientos, la correcta aplicación de las reglas de negocio y la fiel correspondencia con la definición establecida en las historias de usuario, tanto para la versión de Escritorio como para la Móvil de la Solución Tecnológica del Voto Digital.

2.1.2. Metodología de Análisis de Amenazas y Vulnerabilidades (Seguridad)

El proceso de análisis de seguridad de la solución tecnológica se llevó a cabo mediante una metodología integral, estructurada y basada en estándares internacionales, orientada a identificar vulnerabilidades técnicas, debilidades de configuración, fallas de diseño y riesgos asociados a la operación de los sistemas evaluados. La metodología aplicada tuvo como objetivo evaluar de forma sistemática la confidencialidad, integridad y disponibilidad de la información, así como la resiliencia de la solución frente a escenarios de ataque reales.

El análisis de seguridad abarcó de forma integral las aplicaciones web, aplicaciones de escritorio, aplicaciones móviles y los entornos cloud que soportan la operación de la solución, considerando las particularidades técnicas, los vectores de ataque específicos y los modelos de amenaza propios de cada componente.

La aplicación de esta metodología permitió no sólo identificar vulnerabilidades puntuales, sino también detectar patrones de riesgo, debilidades sistémicas y oportunidades de mejora en la

arquitectura, los procesos de desarrollo y la operación de la solución, proporcionando una visión clara, consistente y accionable del estado de seguridad global del sistema evaluado.

2.1.3. Metodología de Evaluación del Código Fuente y Documentación

La auditoría tanto del código fuente como de las aplicaciones que conforman la Solución Tecnológica de Voto Digital (STVD) orientó a garantizar la seguridad, calidad y correcto funcionamiento del software, con el fin de prevenir ciberataques y asegurar el cumplimiento normativo. La auditoría tuvo como objetivo identificar vulnerabilidades, errores de seguridad y brechas potenciales en el código y en las aplicaciones, así como evaluar el nivel general de seguridad tanto del código fuente como de los ejecutables antes de su despliegue. Para ello, se aplicaron enfoques de caja blanca mediante análisis estático de código (SAST), complementados con técnicas de caja negra como pruebas de penetración, alineados con la Guía de Revisión de Código de OWASP. El análisis incluyó la revisión de mecanismos de autenticación y autorización, validación de entradas, gestión de cookies y registros de auditoría, así como la identificación de errores, control de calidad, optimización del mantenimiento y aplicación de estándares y buenas prácticas de desarrollo. Este enfoque permitió fortalecer la arquitectura interna del software, mejorar su mantenibilidad y asegurar que la solución sea robusta, interoperable y sostenible en el tiempo. ☒

3. Alcance a la Auditoría a realizar a la Solución Tecnológica de Voto Digital (STVD)

El presente apartado establece el alcance técnico y operativo de la auditoría realizada sobre la Solución Tecnológica del Voto Digital (STVD), específicamente en lo referido al Predictamen 2 correspondiente a la segunda fase del proceso de auditoría, desarrollado en función de la Etapa 3 y la Etapa 4 de revisión de la STVD. Su finalidad es delimitar los componentes, fronteras y niveles de análisis considerados por la firma auditora durante la ejecución del proceso, asegurando una evaluación integral y objetiva de los aspectos funcionales, de seguridad y de calidad del software.

3.1. Alcance de la Evaluación de Funcionalidades

La evaluación de funcionalidades de la Solución Tecnológica del Voto Digital (STVD) tuvo como objetivo verificar que el sistema haya sido concebido, desarrollado e implementado conforme a metodologías reconocidas de ingeniería de software y a estándares internacionales de calidad, en alineación con la normativa electoral vigente y las directrices establecidas por la ONPE. En este contexto, se efectuó el análisis del ciclo de desarrollo de software definido por la ONPE, con el propósito de determinar su nivel de alineamiento con buenas prácticas y metodologías internacionalmente reconocidas en ingeniería de software.

Asimismo, se evaluó el desempeño y los tiempos de respuesta del sistema durante las etapas de instalación, sufragio y escrutinio, identificando posibles factores que pudieran impactar su eficiencia operativa. De manera complementaria, se analizó la recopilación, distribución y utilización de los datos generados, verificando la consistencia entre la información procesada, almacenada y presentada en los distintos módulos y reportes del sistema.

La revisión incluyó la verificación de la integridad, consistencia y correcta interpretación de los datos a lo largo de todo el flujo operativo, así como la validación de los mecanismos de confidencialidad implementados para proteger la información en cada una de las etapas del proceso electoral digital. Adicionalmente, se examinó que los datos fueran correctamente registrados, procesados y retroalimentados dentro del sistema, garantizando su trazabilidad y coherencia funcional.

Finalmente, la evaluación consideró la revisión de los controles y estándares aplicables a la STVD, tomando como referencia marcos normativos y buenas prácticas internacionales en materia de seguridad de la información y desarrollo seguro, incluyendo ISO/IEC 27001:2022 (Anexo A), ISO/IEC 27002, ISO/TS 54001:2019, OWASP, NIST Cybersecurity Framework, así como metodologías especializadas como ISSAF, SANS y CAPEC.

3.2. Alcance del Análisis de Amenazas y Vulnerabilidades

La evaluación de funcionalidades desde la perspectiva de la seguridad de la información tuvo como finalidad asegurar que la Solución Tecnológica del Voto Digital (STVD) cuente con los controles necesarios para protegerse frente a amenazas internas y externas que puedan afectar la integridad del proceso electoral, la continuidad del servicio y la confianza ciudadana. Dado el carácter crítico de los sistemas electorales, la auditoría abordó la seguridad no solo como un requisito técnico, sino como un elemento esencial para garantizar la legitimidad democrática y el cumplimiento de los principios constitucionales del sufragio.

En este contexto, se realizó la identificación de posibles defectos o deficiencias en la solución, complementada con la ejecución de análisis de vulnerabilidades orientados a detectar exposiciones técnicas en los distintos componentes del sistema. Asimismo, se llevaron a cabo pruebas de penetración sobre la capa web de la solución, utilizando como referencia la Guía de Evaluación de OWASP, así como otras metodologías reconocidas. De igual manera, se efectuó un diagnóstico de seguridad sobre los componentes de escritorio, evaluados conforme a buenas prácticas como OWASP Desktop Application Security.

La evaluación incluyó la aplicación de técnicas de pruebas de caja blanca, caja gris y caja negra, con el objetivo de identificar vulnerabilidades tanto en la lógica interna como en el comportamiento externo del sistema. Adicionalmente, se realizaron ejercicios de explotación controlada de vulnerabilidades para determinar escenarios de riesgo, considerando aspectos como la naturaleza de la amenaza, la vulnerabilidad asociada, la probabilidad de ocurrencia, el impacto potencial y el nivel de riesgo resultante, así como las medidas de mitigación correspondientes.

Finalmente, se llevó a cabo una revisión de la infraestructura tecnológica que soporta la STVD, con el fin de identificar posibles vulnerabilidades en su configuración, operación o arquitectura que pudieran afectar la seguridad de la información. Este análisis permitió obtener una visión integral del estado de seguridad de la solución, así como de los riesgos asociados a su operación en entornos críticos.

3.3. Alcance de la Evaluación del Código Fuente y Documentación

La auditoría al código fuente y a la documentación técnica de la Solución Tecnológica del Voto Digital (STVD) constituye un componente esencial para evaluar la calidad, seguridad y sostenibilidad del software más allá de su funcionalidad superficial.

En este sentido, se realizó una revisión del código desde la perspectiva de ingeniería de software, evaluando su consistencia, legibilidad y estructura, con el propósito de identificar oportunidades de mejora y asegurar su sostenibilidad a largo plazo. Asimismo, se verificó la existencia de posibles vulnerabilidades o funciones susceptibles de ser explotadas, complementando este análisis con la evaluación de la arquitectura del sistema, incluyendo aspectos como la modularidad, la organización de componentes y su capacidad de reutilización. Este enfoque permitió identificar fortalezas y áreas de optimización en el diseño técnico de la solución.

De manera complementaria, se efectuó un análisis estático del código fuente mediante herramientas especializadas, con el fin de obtener una visión cuantitativa y cualitativa del estado del software. Este análisis incluyó la identificación y clasificación de errores (bugs), vulnerabilidades y prácticas deficientes (código sucio), considerando su nivel de severidad; la detección de puntos críticos de seguridad (security hotspots); la medición de indicadores clave como cobertura de análisis, duplicidad de código, complejidad estructural, nivel de documentación interna (comentarios) y deuda técnica asociada a los hallazgos identificados.

Finalmente, la evaluación contempló la revisión de la documentación técnica y funcional asociada a la STVD, considerando como mínimo las Especificaciones de Requisitos de Software, las Reglas de Negocio, el Manual de Usuario y el Manual Técnico. Este análisis permitió determinar el grado de alineamiento entre la documentación y la implementación real del sistema, así como su nivel de completitud, claridad y utilidad para los distintos actores involucrados en el ciclo de vida de la solución.

4. Matriz de los Hallazgos Evidenciados en la Auditoría

En lo que respecta a la presentación de los distintos hallazgos, se debe tener en cuenta que el análisis y revisión a la **Solución Tecnológica del Voto Digital (STVD)** se realizaron de acuerdo a lo establecido por la Oficina Nacional de Procesos Electorales (ONPE), con el fin de garantizar seguridad y transparencia, evaluando el cumplimiento de los procedimientos establecidos y su alineación con los estándares requeridos. Como resultado de la auditoría, se identificaron hallazgos de carácter general que afectan el desempeño global de los procesos evaluados, los cuales fueron subsanados y verificados en la etapa correspondiente, para observar mayor detalle se debe revisar en el informe respectivo del proceso auditado.

Proceso/Criticidad	Total de Hallazgos	Subsanados	Pendientes	% de Subsanación
Evaluación de Funcionalidades	14	14	0	100%
Análisis de Amenazas y Vulnerabilidades (Seguridad)	39	39	0	100%
Evaluación del Código Fuente	68	68	0	100%
Evaluación de Documentación	111	111	0	100%
Total	232	232	0	100%

Tabla 1. Cantidad de hallazgos encontrados por proceso

5. Pre-dictamen de la Auditoría

Introducción

El presente predictamen sintetiza los resultados del proceso de auditoría realizado a la Solución Tecnológica del Voto Digital (STVD), integrando el análisis técnico, funcional y de seguridad desarrollado a lo largo de las distintas etapas de evaluación. Su propósito es emitir una valoración objetiva y fundamentada sobre el estado actual de la solución, considerando el nivel de madurez alcanzado, la efectividad de las acciones de mejora implementadas y las condiciones necesarias para su utilización en contextos electorales. Este pronunciamiento se sustenta en la evidencia recopilada, los hallazgos identificados y su correspondiente validación, constituyéndose como un insumo clave para la toma de decisiones estratégicas por parte de la ONPE.

Tras la culminación de la fase de verificación de remediaciones, este **Pre-Dictamen** se emite con carácter **FAVORABLE**. Desde la perspectiva de ingeniería de software y seguridad criptográfica, la **Solución Tecnológica de Voto Digital (STVD)** ha demostrado una evolución técnica satisfactoria, transitando de un estado de "funcionalidad operativa" a uno de "certeza técnica verificable".

Viabilidad: La STVD es considerada **apta** desde el punto de vista técnico para su implementación en futuros procesos electorales.

Evolución: Se ha evidenciado una mejora sustancial en los procesos de desarrollo, seguridad y gobernanza tecnológica, alcanzando un nivel de madurez alineado con las mejores prácticas internacionales.

Sustento de la Idoneidad

La calificación se fundamenta en la resolución del **100%** de los **232 hallazgos** identificados inicialmente. Este proceso de remediación ha blindado los tres pilares de la seguridad de la información:

- **Confidencialidad:** Implementación de protocolos de anonimización mediante **Mixnet** y cifrado en reposo y tránsito en la infraestructura AWS.

- **Integridad:** Uso de firmas digitales basadas en el **DNle (ONPEID)**, algoritmos de resumen **SHA-512** y un esquema de inalterabilidad mediante **Blockchain** .
- **Disponibilidad:** Arquitectura *cloud-native* multirregión con servicios asíncronos y cómputo *serverless* que garantiza la resiliencia ante contingencias.

Salvedad Estratégica y Salvaguardas

A pesar de la aptitud técnica actual evidenciada en las pruebas funcionales y de integridad realizadas, resulta necesario reforzar la consistencia del sistema para garantizar que estos niveles de precisión se mantengan incluso frente a volúmenes de datos considerablemente mayores. En este sentido, se recomienda implementar un ciclo adicional de validación preventiva orientado a escenarios de carga. Este ciclo debe incluir:

- **Pruebas de Estrés Masivo:** Validar el comportamiento del sistema ante una concurrencia superior a los **20,000 usuarios**, mitigando riesgos de degradación de latencia.

A la fecha del presente predictamen, la STVD se considera **técnicamente apta** para su implementación en procesos electorales, incluyendo su utilización en próximas elecciones. La madurez alcanzada no es solo el resultado de un desarrollo funcional, sino de un compromiso con la Gobernanza Tecnológica y la Integridad Electoral bajo el estándar **ISO/TS 54001:2019**.

Es destacable el esfuerzo de refactorización realizado por la ONPE, logrando hitos de calidad que superan los estándares promedio de la industria:

- **Cobertura de Código:** Incremento radical de la cobertura de pruebas unitarias del **5%** inicial a niveles superiores al **80%** en módulos críticos.
- **Higiene Técnica:** Eliminación de 37 hallazgos de "código sucio" (*code smells*) y reducción de la complejidad cognitiva en validadores de alta sensibilidad.
- **Blindaje Documental:** Consolidación de Especificaciones de Requisitos (ERS) y Manuales Técnicos con una trazabilidad bidireccional del **100%**.

Análisis cualitativo sobre el impacto social y político de la solución.

Es importante señalar que, más allá del código y la infraestructura, un sistema de votación debe cumplir con la confianza del proceso electoral digital, entendido como la garantía integral de

certeza, transparencia y legitimidad ante todos los actores del proceso electoral. En su estado actual, la Solución Tecnológica del Voto Digital (STVD) no solo se sustenta en una base sólida, sino que ha logrado cerrar la brecha previamente identificada entre la “funcionalidad operativa” y la “certeza incuestionable”, mediante la atención y cierre total de los hallazgos derivados de las auditorías.

1. **La Certeza ante el Elector:** Como resultado del proceso de remediación y validación, los aspectos técnicos que en etapas anteriores podían dar lugar a interpretaciones adversas han sido debidamente corregidos. Esto fortalece la percepción de transparencia, reduce significativamente los riesgos de cuestionamientos en escenarios de alta sensibilidad política y contribuye a preservar la confianza ciudadana y la estabilidad del proceso electoral.
2. **Auditabilidad como Garantía:** La solución ha evolucionado hacia un modelo más transparente, trazable y verificable, facilitando su auditoría por parte de organizaciones políticas, observadores nacionales e internacionales y demás actores relevantes. La incorporación de mejoras orientadas a la claridad operativa y a la verificabilidad independiente permite que el sistema no solo sea técnicamente robusto, sino también comprensible y confiable más allá del ámbito estrictamente especializado.
3. **El Valor de la Consolidación Técnica:** En materia electoral, la excelencia no es un punto de llegada, sino un proceso continuo. Si bien la STVD ha alcanzado un nivel de madurez que la hace apta para su implementación, resulta altamente recomendable la ejecución de **nuevos ciclos integrales de pruebas** que refuercen su robustez, seguridad, resiliencia operativa y transparencia verificable. Este enfoque no responde a deficiencias actuales, sino a una práctica de aseguramiento continuo orientada a consolidar la confianza pública y garantizar que la solución opere bajo los más altos estándares internacionales. En este sentido, la evolución de la STVD reafirma un principio institucional fundamental: la seguridad, integridad y confiabilidad del voto constituyen valores innegociables.

Marco Metodológico Aplicado

El presente análisis se sustenta en la convergencia de los siguientes estándares internacionales de auditoría y seguridad, exigidos por la ONPE en las distintas etapas ejecutadas en el proyecto al corte de la entrega del presente informe.

- **ISO/TS 54001:2019:** Específico para requisitos de calidad en sistemas de votación electrónica.
- **ISO/IEC 27002:** Es un estándar internacional que actúa como un catálogo de "mejores prácticas" para la implementación de controles de seguridad de la información.
- **ISO/IEC 27001 (Anexo A de dicha norma):** Es una lista de referencia de controles de seguridad de la información que las organizaciones deben usar para proteger sus activos de información.
- **NIST Cybersecurity Framework (CSF) 2.0:** Evaluando las funciones de *Gobernanza, Identificación, Protección, Detección, Respuesta y Recuperación*.
- **OWASP ASVS & Top 10:** Para la verificación de seguridad en aplicaciones web y riesgos de seguridad.
- **CAPEC (Common Attack Pattern Enumeration and Classification):** Para el modelado de amenazas y vectores de ataque.
- **CIS Controls (SANS):** Para la evaluación de la postura de seguridad de la infraestructura crítica.
- **ISSAF (Information Systems Security Assessment Framework):** Para la metodología de evaluación de penetración y procesos.

Recomendaciones Estratégicas Prioritarias

En atención a la evolución positiva evidenciada en la Solución Tecnológica del Voto Digital (STVD) y al cierre satisfactorio de la totalidad de los hallazgos identificados previamente, el presente apartado ya no se orienta a un plan de remediación correctiva, sino a un esquema de fortalecimiento continuo y aseguramiento de calidad, con el objetivo de consolidar la solución como un referente de excelencia en entornos electorales.

Las recomendaciones que se presentan a continuación responden a buenas prácticas internacionales y tienen como finalidad reforzar atributos clave como la robustez, la seguridad integral, la transparencia verificable y la resiliencia operativa del sistema, especialmente en escenarios de alta criticidad como procesos electorales.

Fortalecimiento de Seguridad

- Mantener una política activa de actualización de dependencias, asegurando la mitigación temprana de vulnerabilidades (CVEs), bajo un enfoque preventivo y de mejora continua.
- Consolidar la gestión de accesos y credenciales sensibles mediante herramientas especializadas como AWS Secrets Manager, incluyendo esquemas periódicos de rotación y auditoría de credenciales.

Consolidación de la Integridad Electoral

- Continuar optimizando los componentes de firma digital (ONPEID), asegurando su estabilidad, determinismo y trazabilidad completa en todos los flujos operativos.

Endurecimiento y Observación de la Infraestructura

- Reforzar los esquemas de monitoreo y detección temprana con énfasis en la identificación de cambios de configuración y eventos de seguridad.
- Mantener y ampliar las configuraciones de inmutabilidad y versionamiento en almacenamiento crítico (como S3), incorporando prácticas avanzadas de protección de datos.

Aseguramiento de Calidad y Pruebas

- Consolidar un modelo de integración y despliegue continuo (CI/CD) que preserve altos estándares de calidad, incluyendo cobertura de pruebas unitarias, pruebas de integración y validaciones automatizadas.
- Complementar con ciclos periódicos de pruebas avanzadas (carga, estrés, resiliencia, pruebas de seguridad ofensiva), orientadas a validar el comportamiento del sistema bajo condiciones reales y exigentes.

Evolución de Arquitectura y Código

- Mantener la actualización continua de frameworks y componentes críticos garantizando su alineación con versiones seguras y soportadas.
- Continuar con procesos de refactorización orientados a mejorar la mantenibilidad, reducir la complejidad y fortalecer la auditabilidad del código.

Hoja de Ruta de Fortalecimiento Estratégico

Como parte del enfoque de mejora continua, esta firma auditora propone una hoja de ruta evolutiva, priorizada no por la existencia de brechas críticas ya subsanadas sino por la oportunidad de elevar el nivel de madurez del sistema:

Fase 1: Consolidación y Aseguramiento

1. Verificación continua de actualizaciones de seguridad en componentes críticos.
2. Validación integral del sistema de firma digital para garantizar consistencia operativa.
3. Auditoría periódica de gestión de credenciales.
4. Revisión sistemática de mecanismos de autenticación (incluyendo tokens y controles criptográficos).

Fase 2: Observación y Protección Avanzada

1. Fortalecimiento de monitoreo activo y respuesta temprana ante eventos de seguridad.
2. Optimización de políticas de protección de datos, versionamiento e inmutabilidad.
3. Mejora continua en la calidad del código, manteniendo estándares de simplicidad, trazabilidad y auditabilidad.

Fase 3: Innovación en Integridad y Confianza

1. Evaluación e implementación progresiva de mecanismos de verificabilidad cruzada basados en tecnologías de registro inmutable.
2. Mejora continua de estrategias de testing automatizado, incorporando pruebas avanzadas y escenarios de validación independientes.

6. Conclusión General

A la fecha del presente dictamen, y tras un riguroso proceso de remediación integral y verificación de la subsanación de la totalidad de los 232 hallazgos identificados en las fases previas de la auditoría, la **Solución Tecnológica de Voto Digital (STVD)** es considerada **APTA y FAVORABLE** desde el punto de vista técnico para su implementación en procesos electorales. La arquitectura del sistema ha demostrado una transición exitosa desde un estado de observación hasta consolidarse como una plataforma robusta y alineada con las exigencias de integridad electoral.

La evolución técnica evidenciada en dimensiones críticas como la seguridad de la información, la calidad del software, la gobernanza tecnológica y la integridad operativa permite afirmar que la solución ha alcanzado un nivel de madurez significativo. Este estado de cumplimiento se sustenta en el alineamiento estricto con marcos de referencia de rango internacional, tales como las normas **ISO/TS 54001:2019** para calidad de procesos electorales, **ISO/IEC 27001** para la gestión de la seguridad, y los lineamientos de ciberseguridad de **NIST** y **OWASP**.

La firma auditora reconoce en la STVD una solución innovadora basada en una arquitectura moderna de microservicios y despliegue *cloud-native* sobre infraestructura AWS. El sistema garantiza atributos de seguridad de alto nivel, tales como:

- **Autenticación de identidad:** Mediante el componente ONPEID y el uso del DNI electrónico (DNle).
- **Secreto y Anonimato:** Asegurados a través de procesos criptográficos de mezcla (*Mixnet*) que impiden la correlación entre la identidad del elector y su voto.
- **Inalterabilidad de Resultados:** Fortalecida por el uso de firmas digitales, sellos de tiempo y la publicación de resultados en una red Blockchain para garantizar una trazabilidad innegable.

No obstante, la calificación favorable, y en estricta concordancia con los estándares de excelencia y el principio de aseguramiento continuo, esta auditoría recomienda de manera imperativa la ejecución de un **nuevo ciclo integral de pruebas** previo a un despliegue masivo. Este ciclo debe profundizar en escenarios de carga extrema, resiliencia ante fallos de conectividad, pruebas de seguridad ofensiva (*pentesting*) y validación operativa en condiciones reales. Tales medidas **no**

responden a deficiencias actuales, sino al objetivo de reforzar la robustez operativa, la transparencia verificable y la confiabilidad sistémica del proceso electoral.

La Solución Tecnológica del Voto Digital constituye un activo estratégico de alto valor para la democracia peruana. Los resultados de este dictamen deben interpretarse como la confirmación de una evolución técnica exitosa, fruto del compromiso de la institución con la mejora continua y la adopción proactiva de recomendaciones especializadas.

Finalmente, la **ONPE** ha demostrado un alto grado de madurez, responsabilidad y liderazgo al adoptar un enfoque sostenido de fortalecimiento tecnológico. Por tanto, la STVD no solo se consolida como un sistema funcional, sino como una plataforma robusta, segura, transparente y legítima, plenamente capaz de generar y sostener la confianza de la ciudadanía en la modernización del sistema electoral.

Como parte de la mejora continua, se proponen las siguientes fases:

1. **Consolidación y Aseguramiento:** Verificación periódica de actualizaciones de seguridad en componentes críticos y validación del sistema de firma digital.
2. **Protección Avanzada:** Fortalecimiento del monitoreo activo y optimización de políticas de inmutabilidad de datos en almacenamiento.
3. **Innovación en Confianza:** Mejora Continua de estrategias de testing automatizado e integración de mecanismos adicionales de verificabilidad cruzada.
4. **Realización de Auditoria Adicional:** Aunque se realizó la validación de la STVD a través de dos iteraciones, es importante la ejecución de un nuevo proceso de auditoria para dar continuidad preventiva a través de una ejecución técnica de pruebas basada en los estándares utilizados a lo largo del proyecto, para afianzar la STVD para que sea usada en procesos electorales venideros.

7. Referencias Documentales

1. Constitución Política del Perú (1993).
Disponible en: <https://www.tc.gob.pe/wp-content/uploads/2021/05/Constitucion-Politica-del-Peru-1993.pdf>
2. Ley N.º 26859 – Ley Orgánica de Elecciones (1997).
Disponible en: <https://pdba.georgetown.edu/Electoral/Peru/leyelecciones.pdf>
3. Ley N.º 26486 – Ley Orgánica de la Oficina Nacional de Procesos Electorales (ONPE).
Disponible en: <https://www.onpe.gob.pe/wp-content/uploads/2019/11/Ley-Organica-ONPE-Ley-26486.pdf>
4. Ley N.º 32270 – Ley que modifica la Ley N.º 26859, Ley Orgánica de Elecciones, a fin de incorporar el Voto Digital (10 de marzo de 2025).
Disponible en: <https://busquedas.elperuano.pe/download/url/ley-que-modifica-la-ley-26859-ley-organica-de-ley-32270.pdf>
5. Resolución Jefatural N.º 000131-2025-JN/ONPE (11 de agosto de 2025).
Disponible en: <https://www.onpe.gob.pe/wp-content/uploads/2025/08/RJ-000131-2025-JN-ONPE.pdf>
6. Resolución Jefatural N.º 000143-2025-JN/ONPE (09 de setiembre de 2025).
Disponible en: <https://www.onpe.gob.pe/wp-content/uploads/2025/09/RJ-000143-2025-JN-ONPE.pdf>
7. Resolución Jefatural N.º 000051-2025-JN/ONPE (07 de abril de 2025).
Disponible en: <https://www.onpe.gob.pe/wp-content/uploads/2025/04/RJ-000051-2025-JN-ONPE.pdf>
8. Pliego de Condiciones N.º ONPE-AUD-001-2025.
Disponible en: <https://www.onpe.gob.pe/transparencia/contrataciones/2025/ONPE-AUD-001-2025.pdf>
9. ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información (incluye Anexo A).
Disponible en: <https://www.iso.org/standard/27001>
10. ISO/IEC 27002:2022 – Controles de seguridad y buenas prácticas para la gestión de la información.
Disponible en: <https://www.iso.org/standard/75652.html>

11. ISO/TS 54001:2019 – Requisitos de calidad aplicables a sistemas de voto electrónico.
Disponible en: <https://www.iso.org/standard/74532.html>
12. OWASP – Seguridad en aplicaciones web y de escritorio, mitigación de vulnerabilidades y revisión de código seguro (Code Review Guide).
Disponible en: <https://owasp.org/www-project-code-review-guide/>
13. NIST Cybersecurity Framework (CSF) – Marco de ciberseguridad para sistemas críticos.
Disponible en: <https://www.nist.gov/cyberframework>
14. NIST SP 800-115 – Technical Guide to Information Security Testing and Assessment.
Disponible en: <https://csrc.nist.gov/publications/detail/sp/800-115/final>
15. NIST SP 800-53 – Security and Privacy Controls for Information Systems and Organizations.
Disponible en: <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
16. ISSAF, SANS y CAPEC – Referenciales para pruebas, auditoría técnica, análisis de amenazas y evaluación de vulnerabilidades.
Disponible en:
 - a. ISSAF: <https://www.oisssg.org/issaf>
 - b. SANS: <https://www.sans.org>
 - c. CAPEC: <https://capec.mitre.org>
17. PR12, PR13 y PR14 bajo la NTP 12207 – Procedimientos institucionales y procesos del ciclo de vida del software.
Disponible en: <https://www.gob.pe/institucion/inacal/normas-legales>

8. Glosario de Términos

Término	Definición
Acta Electoral	Documento digital generado por el sistema que certifica etapas del proceso (instalación, sufragio, escrutinio, etc.).
API (Application Programming Interface)	Conjunto de servicios o puntos de conexión que permiten la comunicación entre diferentes módulos o sistemas.
Backend	Parte del sistema que maneja la lógica de negocio, base de datos y servicios del servidor. No visible directamente para el usuario final.
Base de Datos	Es un conjunto de datos organizados a los que se puede tener acceso y que se pueden administrar, indexar, buscar y actualizar con facilidad.
Cédula de Votación Digital	Documento electrónico que presenta las opciones electorales al elector. Se cifra con llaves electorales que garantizan confidencialidad y protección contra alteraciones.
Certificado Digital del DNle	Certificado criptográfico contenido en el chip del DNle. Permite la autenticación del ciudadano y la firma digital de documentos con validez legal.
Dispositivos	Son instrumentos tecnológicos que interpretan la información y permiten la comunicación entre las personas y las computadoras.
DNle (Documento Nacional de Identidad Electrónico)	Documento oficial que contiene un chip criptográfico con certificados que permiten la autenticación del ciudadano y

Término	Definición
	la firma digital. Su lectura se realiza mediante lectores físicos o NFC.
Elector	Ciudadano habilitado que se autentica mediante su DNle y participa en la emisión del voto digital dentro de la plataforma.
Frontend	Interfaz de usuario del sistema, encargada de la presentación visual y la interacción directa con el usuario.
Hash	Algoritmo que consigue crear a partir de una entrada (un texto, una contraseña o un archivo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado.
Integridad	Mantenimiento de la exactitud y validez de la información, protegiéndola de modificaciones o alteraciones no autorizadas.
Mezcla (Mixnet)	Proceso criptográfico que anonimiza votos para impedir cualquier correlación entre identidad del elector y su elección. Garantiza privacidad y confidencialidad del sufragio.
Observación	Omisiones, incumplimientos normativos o deficiencias de control interno detectados en la auditoría practicada.
ONPE Firma (Firma ONPE)	Módulo de firma digital utilizado para validar electrónicamente documentos y constancias dentro del proceso electoral.
Padrón Electoral	Registro oficial de los ciudadanos habilitados para votar en un proceso electoral.

Término	Definición
PIN del DNle	Clave personal utilizada para habilitar el uso del chip criptográfico del DNle. Posee intentos limitados controlados por el chip.
PostgreSQL	Sistema de gestión de bases de datos relacional (RDBMS) de código abierto usado para almacenar información estructurada del sistema.
Recomendación	Propuesta hecha al auditado con la finalidad de prevenir o corregir la reincidencia de las observaciones determinadas, que elimine las causas que las originaron o que promuevan una mejora.
Riesgo	Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
Seguimiento	Es la acción de constatar que las recomendaciones planteadas se hayan cumplido en tiempo y forma, verificando el avance en la atención o solución definitiva a la problemática detectada.
Sistema	Es un conjunto de elementos organizados y relacionados que interactúan entre sí para lograr un objetivo. Los sistemas reciben (entrada) datos, energía o materia del ambiente y proveen (salida) información, energía o materia.
Votante	Ciudadano que, en el ejercicio del sufragio permitido por la ley, ha participado efectivamente en la votación.