

Ley orgánica que fortalece la ciberseguridad de los sistemas informáticos electorales mediante auditorías independientes, pruebas públicas de seguridad y un equipo de respuesta electoral, y modifica las Leyes 26487, 26486 y 26497

Con votación de ley orgánica, incorpora en las leyes orgánicas de la ONPE, el JNE y el RENIEC el deber de someter los sistemas de padrón, cómputo, transmisión y publicación de resultados y de voto electrónico a auditorías independientes con congelamiento y compilación reproducible de versiones, pruebas públicas en entorno réplica, huellas criptográficas verificables por personeros y respaldo verificable; organiza un equipo de respuesta electoral presidido por la ONPE; y rige conforme al artículo 4 de la Ley Orgánica de Elecciones.

Comisión (Cámara de Diputados): Constitución, Reglamento y Relaciones Exteriores (+ Ciencia, Innovación Tecnológica y Sociedad Digital) · **Revisora (Senado):** Constitución, Reglamento y Relaciones Exteriores · **Prioridad:** media · **Costo fiscal:** bajo · **Plazo:** corto
Plan Perú 2050: Ciber Seguridad, Institucionalidad, Ética

I. Exposición de motivos

La confianza en los resultados electorales depende cada vez más de sistemas informáticos: padrones, cómputo, transmisión de actas, publicación de resultados y el voto electrónico autorizado por la Ley 29603, ampliado en el periodo 2021-2026 por leyes de voto digital para peruanos en el extranjero. Las leyes orgánicas de la ONPE (Ley 26487), del JNE (Ley 26486) y del RENIEC (Ley 26497) y la Ley Orgánica de Elecciones (Ley 26859) no establecen un régimen legal de ciberseguridad con auditorías independientes obligatorias, congelamiento de versiones, pruebas públicas de seguridad ni publicación verificable de huellas criptográficas antes de cada proceso. En contextos de alta polarización, la ausencia de verificaciones independientes deja espacio para la desinformación sobre supuestos fraudes informáticos y para riesgos reales como ataques de denegación de servicio a portales de resultados o suplantación de canales oficiales. Otras autoridades electorales trabajan con agencias de ciberseguridad (programa de seguridad electoral de la CISA en Estados Unidos) u organizan pruebas públicas en las que expertos externos intentan vulnerar los sistemas (Teste Público de Segurança del TSE de Brasil, desde 2009). Esta propuesta no se pronuncia sobre la extensión del voto electrónico; busca que cualquier sistema empleado sea verificable. Por regular el funcionamiento de organismos constitucionalmente autónomos, requiere votación de ley orgánica.

II. Fórmula legal

EL CONGRESO DE LA REPÚBLICA ha dado la Ley siguiente:

LEY ORGÁNICA QUE FORTALECE LA CIBERSEGURIDAD DE LOS SISTEMAS INFORMÁTICOS ELECTORALES MEDIANTE AUDITORÍAS INDEPENDIENTES, PRUEBAS PÚBLICAS DE SEGURIDAD Y UN EQUIPO DE RESPUESTA ELECTORAL, Y MODIFICA LAS LEYES 26487, 26486 Y 26497

Artículo 1. Objeto

La presente ley orgánica tiene por objeto fortalecer la ciberseguridad, verificabilidad y transparencia de los sistemas informáticos empleados en los procesos electorales, de referéndum y otras consultas populares, en el marco de los artículos 176 a 183 de la Constitución Política del Perú.

Artículo 2. Sistemas comprendidos

Están comprendidos los sistemas de gestión del padrón electoral, de cómputo y transmisión de resultados, de publicación de resultados, de voto electrónico presencial o no presencial, y los portales y canales digitales oficiales de la Oficina Nacional de Procesos Electorales (ONPE), del Jurado Nacional de Elecciones (JNE) y del Registro Nacional de Identificación y Estado Civil (RENIEC).

Artículo 3. Auditoría independiente y congelamiento de versiones

3.1. La ONPE, el JNE y el RENIEC someten los sistemas comprendidos a su cargo a una auditoría independiente de ciberseguridad y de código fuente con una anticipación no menor de noventa días calendario

a cada elección general, regional o municipal. Los auditores son universidades o entidades especializadas seleccionadas conforme a la Ley 32069, Ley General de Contrataciones Públicas, con participación de la Contraloría General de la República como veedora, y suscriben compromisos de confidencialidad.

3.2. Toda modificación posterior a la auditoría se somete a una auditoría complementaria antes de su despliegue. La versión final se congela, se compila de forma reproducible a partir del código auditado y se firma digitalmente en acto público con presencia de personeros y observadores.

3.3. Los contratos de adquisición de componentes de los sistemas comprendidos incluyen el acceso de los auditores al código fuente bajo confidencialidad o, cuando no sea posible, la certificación del componente conforme a estándares internacionales reconocidos.

Artículo 4. Pruebas públicas de seguridad

4.1. Antes de cada elección general, la ONPE organiza una prueba pública de seguridad en la que expertos inscritos pueden intentar vulnerar, en un entorno réplica aislado de los sistemas de producción, los sistemas que se emplearán, conforme a reglas de participación publicadas.

4.2. La participación conforme a dichas reglas constituye prueba autorizada para efectos del artículo 12 de la Ley 30096, Ley de Delitos Informáticos.

4.3. Los hallazgos se publican en forma general una vez corregidos; el detalle técnico de las vulnerabilidades no corregidas se reserva hasta su corrección o hasta la conclusión del proceso electoral.

Artículo 5. Transparencia y verificación de huellas

Los informes ejecutivos de las auditorías, las versiones del software utilizadas y sus huellas criptográficas se publican en los portales institucionales. Los personeros acreditados y los observadores pueden verificar dichas huellas en los equipos de cómputo con herramientas de verificación independientes, de código abierto, publicadas por la ONPE con anticipación conforme al procedimiento que esta apruebe.

Artículo 6. Equipo de respuesta ante incidentes electorales

6.1. Durante cada proceso electoral funciona un equipo de respuesta ante incidentes electorales convocado y presidido por la ONPE e integrado por el JNE y el RENIEC, que monitorea, responde y comunica públicamente los incidentes relevantes. El equipo funciona como CSIRT sectorial y notifica sus incidentes por el canal nacional de notificación de incidentes de seguridad digital.

6.2. Los organismos electorales pueden solicitar el apoyo técnico de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital y del Centro Nacional de Seguridad Digital, que actúa sin acceso a los sistemas de cómputo salvo autorización expresa del organismo electoral.

6.3. El equipo coordina con la Policía Nacional del Perú y el Ministerio Público y, cuando el incidente pueda afectar la seguridad nacional, con el Comando Conjunto de las Fuerzas Armadas conforme a la Ley 30999, Ley de Ciberdefensa.

Artículo 7. Protección de canales oficiales

Los organismos electorales implementan medidas contra la suplantación de sus portales, perfiles en redes sociales y números de contacto, y coordinan con los proveedores de servicios digitales el retiro expedito de las cuentas que los suplanten, sin perjuicio de los procedimientos de retiro de contenido previstos en la ley de la materia.

Artículo 8. Respaldo verificable y voto no presencial

8.1. Todo sistema de cómputo o voto electrónico, incluidas las modalidades de voto digital para peruanos en el extranjero, permite verificar sus resultados contra un respaldo físico o un registro independiente auditable, conforme al reglamento que apruebe la ONPE.

8.2. El voto electrónico no presencial solo puede emplearse en procesos vinculantes si garantiza verificabilidad de extremo a extremo y secreto del voto, acreditados por la auditoría independiente del artículo 3; en caso contrario, solo puede utilizarse en consultas no vinculantes o pilotos.

Primera. Disposición Complementaria Final

Reglamentación. La ONPE, el JNE y el RENIEC, en ejercicio de su autonomía, adecúan sus reglamentos en un plazo no mayor de ciento veinte días hábiles contados a partir del día siguiente de la publicación de la presente ley.

Segunda. Disposición Complementaria Final

Aplicación temporal. La presente ley rige conforme a lo dispuesto en el artículo 4 de la Ley 26859, Ley Orgánica de Elecciones.

Tercera. Disposición Complementaria Final

Financiamiento. La implementación de la presente ley se financia con cargo al presupuesto institucional de la ONPE, el JNE y el RENIEC asignado a cada proceso electoral, sin demandar recursos adicionales al Tesoro Público.

Primera. Disposición Complementaria Modificatoria

Incorporación del artículo 5-A a la Ley 26487. Se incorpora el artículo 5-A a la Ley 26487, Ley Orgánica de la Oficina Nacional de Procesos Electorales, en los términos siguientes:

«Artículo 5-A. Seguridad de los sistemas informáticos electorales

La Oficina Nacional de Procesos Electorales somete sus sistemas informáticos electorales a auditoría independiente, organiza pruebas públicas de seguridad, publica las huellas criptográficas de las versiones empleadas, garantiza un respaldo verificable y preside el equipo de respuesta ante incidentes electorales, conforme a la ley orgánica de la materia.»

Segunda. Disposición Complementaria Modificatoria

Incorporación del artículo 5-A a la Ley 26486. Se incorpora el artículo 5-A a la Ley 26486, Ley Orgánica del Jurado Nacional de Elecciones, en los términos siguientes:

«Artículo 5-A. Seguridad de los sistemas informáticos

El Jurado Nacional de Elecciones somete sus sistemas informáticos vinculados a los procesos electorales a auditoría independiente e integra el equipo de respuesta ante incidentes electorales, conforme a la ley orgánica de la materia.»

Tercera. Disposición Complementaria Modificatoria

Incorporación del artículo 7-B a la Ley 26497. Se incorpora el artículo 7-B a la Ley 26497, Ley Orgánica del Registro Nacional de Identificación y Estado Civil, en los términos siguientes:

«Artículo 7-B. Seguridad del sistema del padrón electoral

El Registro Nacional de Identificación y Estado Civil somete el sistema de gestión del padrón electoral a auditoría independiente e integra el equipo de respuesta ante incidentes electorales, conforme a la ley orgánica de la materia.»

III. Análisis costo-beneficio

Gasto público bajo: las auditorías, la auditoría complementaria, la compilación reproducible y la prueba pública representan una fracción menor del presupuesto de cada proceso electoral; el editor estima S/ 2 a 5 millones por elección general y S/ 1 a 3 millones por elección regional y municipal. Se financian con el presupuesto institucional asignado a cada proceso; por el criterio de la STC 00018-2023-PI/TC, el dictamen debe contar con opinión de los organismos electorales e informe del MEF. El beneficio es institucional: verificaciones independientes y públicas reducen la incertidumbre y el espacio para la desinformación sobre fraudes informáticos y permiten corregir vulnerabilidades reales antes de cada elección. La reserva de vulnerabilidades no corregidas evita convertir la transparencia en un riesgo. La norma respeta la autonomía de los organismos electorales, que reglamentan su aplicación y conducen el equipo de respuesta.

Normas que modifica

- Ley 26487, Ley Orgánica de la ONPE, art. 5-A — *incorpora*
- Ley 26486, Ley Orgánica del JNE, art. 5-A — *incorpora*
- Ley 26497, Ley Orgánica del RENIEC, art. 7-B — *incorpora*
- Ley 26859, Ley Orgánica de Elecciones, art. 4 (aplicación temporal) — *complementa*
- Ley 29603, voto electrónico, respaldo verificable (art. 8) — *complementa*

Entidades implicadas (quién hace qué)

- **ONPE** (ejecutora): Audita sus sistemas, organiza la prueba pública, publica huellas y herramientas, preside el equipo de respuesta y reglamenta el respaldo verificable (arts. 3 a 6 y 8).
- **JNE** (ejecutora): Audita sus sistemas e integra el equipo de respuesta (arts. 3 y 6; DCM Segunda).
- **RENIEC** (ejecutora): Audita el sistema del padrón e integra el equipo de respuesta (arts. 3 y 6; DCM Tercera).
- **CGR** (supervisora): Veedora en la selección de auditores (art. 3.1).
- **PCM-SGTD / CNSD** (consultiva): Apoyo técnico a solicitud, sin acceso a sistemas de cómputo salvo autorización (art. 6.2).
- **PNP / MP / CCFFAA** (consultiva): Coordinación ante incidentes con indicios de delito o que afecten la seguridad nacional (art. 6.3).

Sujetos obligados: ONPE, JNE y RENIEC respecto de sus sistemas informáticos electorales; proveedores de componentes de esos sistemas (acceso al código o certificación).

Beneficiarios: Electores, organizaciones políticas, personeros y observadores electorales; el sistema democrático en su conjunto. No cuantificable con información pública.

Impacto económico estimado (confianza baja; referencial, no oficial)

Tipo: gasto

Costo para el Estado: S/ 2–5 millones por elección general y S/ 1–3 millones por elección regional y municipal (estimación del editor)

Horizonte: por proceso electoral (2030 y 2031)

Financiamiento: Presupuesto institucional de ONPE, JNE y RENIEC asignado a cada proceso, sin demandar recursos adicionales al Tesoro Público. Por provenir mayoritariamente de recursos ordinarios, requiere coordinación con el Poder Ejecutivo, opinión de los organismos electorales e informe previo de sostenibilidad fiscal del MEF antes del dictamen.

Supuestos: Auditorías independientes de código y ciberseguridad de los sistemas de tres organismos, auditorías complementarias, compilación reproducible, prueba pública en entorno réplica y herramientas de verificación de huellas. Costos supuestos por el editor, sin fuente oficial; no incluye el costo de los sistemas en sí.

Beneficio para el Estado: Mayor legitimidad de los resultados y menor costo institucional de controversias postelectorales. No cuantificable con información pública.

Beneficio para la sociedad: Confianza verificable en los resultados y menor espacio para la desinformación sobre fraudes informáticos. No cuantificable con información pública.

Inversión privada: No aplica.

Costo para privados: Proveedores de componentes: acceso de auditores al código bajo confidencialidad o certificación.

Riesgos: Plazos ajustados entre cierre de listas y congelamiento de versiones; oferta limitada de auditores independientes; uso político de hallazgos menores (mitigado por publicación tras corrección).

Revisión especializada (asistida por IA, sobre la versión anterior)

- **Constitucional** — Observaciones graves: Las auditorías independientes, pruebas públicas y verificación por personeros fortalecen el derecho de sufragio (art. 31) y la transparencia electoral. Pero imponen obligaciones sobre el núcleo funcional de ONPE, JNE y RENIEC (cómputo, padrón, voto electrónico), materia de sus leyes orgánicas (arts. 106, 177-183), por lo que debe tramitarse y votarse como ley orgánica.
- **Técnica legislativa** — Observaciones graves: Las garantías de auditoría, pruebas públicas y verificabilidad son valiosas, pero imponen deberes de funcionamiento a la ONPE, al JNE y al RENIEC, cuyas leyes orgánicas deben modificarse con votación calificada (art. 106 de la Constitución). Además, la regla de aplicación temporal no se ajusta al art. 4 de la Ley 26859, que difiere la vigencia de las normas electorales.
- **Concordancia normativa** — Con observaciones: Normas verificadas en lo esencial (Ley 26487, LOONPE; Ley 29603, voto electrónico). Omite las leyes recientes de voto digital para peruanos en el extranjero (originadas en los PL 05879/2023-CR y 09359/2024-CR, publicadas), que modificaron la Ley 26859. Al imponer funciones a organismos constitucionalmente autónomos con leyes orgánicas, debe tramitarse como modificación de sus leyes orgánicas (art. 106 de la Constitución).

- **Seguridad** — Con observaciones: Medidas acertadas: auditoría independiente de código, pruebas públicas, huellas criptográficas verificables y respaldo físico. Debe evitarse publicar vulnerabilidades no corregidas antes de la elección, exigir nueva auditoría ante cambios posteriores, y no admitir el voto electrónico no presencial sin verificabilidad equivalente.
- **Derecho tecnológico** — Con observaciones: Propuesta técnicamente sólida (auditoría de código, huellas criptográficas, prueba pública de seguridad, respaldo verificable) que no toma posición sobre el voto electrónico. Debe resolver la congelación de versiones (lo auditado 90 días antes no es necesariamente lo desplegado), definir un procedimiento confiable de verificación de huellas, prever el acceso al código de componentes de terceros e incorporar el referente más próximo (Prueba Pública de Seguridad del TSE de Brasil). Al imponer deberes a órganos constitucionales autónomos, conviene tramitarla como ley orgánica.

IV. Efecto de la vigencia de la norma

Ley orgánica: requiere el voto de más de la mitad del número legal de miembros de cada cámara (art. 106 de la Constitución, modificado por la Ley 31988) y opinión previa de la ONPE, el JNE y el RENIEC. Incorpora el artículo 5-A a la Ley 26487, el artículo 5-A a la Ley 26486 y el artículo 7-B a la Ley 26497 (verificar en SPIJ que la numeración esté libre y su compatibilidad con el artículo 7-A propuesto en CIB-08); complementa la Ley 26859 (rige conforme a su artículo 4), la Ley 29603 y las leyes de voto digital para peruanos en el extranjero, la Ley 30096 (art. 12), la Ley 30999, la Ley 32069 y el Decreto de Urgencia 007-2020. Aplicable, como mínimo, desde las elecciones regionales y municipales de 2030.

V. Indicador de éxito al 2031

Para las elecciones regionales y municipales de 2030 y las generales de 2031, informes de auditoría independiente, acta pública de congelamiento de versiones y resultados generales de la prueba pública de seguridad publicados con al menos sesenta días de anticipación.

Normas relacionadas

- Ley 26487, Ley Orgánica de la Oficina Nacional de Procesos Electorales — <https://www.leyes.congreso.gob.pe/Documentos/Leyes/26487.pdf>
- Ley 26486, Ley Orgánica del Jurado Nacional de Elecciones — <https://www.leyes.congreso.gob.pe/Documentos/Leyes/26486.pdf>
- Ley 26859, Ley Orgánica de Elecciones — <https://www.leyes.congreso.gob.pe/Documentos/Leyes/26859.pdf>
- Ley 29603, que autoriza a la ONPE a emitir normas para la implementación gradual y progresiva del voto electrónico — <https://www.leyes.congreso.gob.pe/Documentos/Leyes/29603.pdf>
- Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento — https://www3.congreso.gob.pe/Docs/comisiones2020/ConstitucionReglamento/files/du_interregno_2020/du-007-2020.pdf

Antecedentes

Periodo 2021-2026 (según verificación en SPLEY del revisor normativo): PL 05879/2023-CR, modifica la Ley 26859 para el voto digital de peruanos en el exterior (publicado como ley); PL 09359/2024-CR, voto electrónico semipresencial en el distrito electoral 27 (publicado como ley); PL 10410/2024-CR, voto electrónico de peruanos en el extranjero (en comisión); PL 12204/2025-CR, transparencia del escrutinio mediante registro audiovisual y transmisión en tiempo real (en comisión). Los números oficiales de las leyes publicadas deben verificarse en El Peruano.

Referencias internacionales

- Estados Unidos: CISA: programa de seguridad electoral para autoridades electorales — <https://www.cisa.gov/topics/election-security>
- Brasil: Tribunal Superior Electoral: Teste Público de Segurança do Sistema Eletrônico de Votação — <https://www.tse.jus.br/comunicacao/noticias/2020/Abril/voce-sabia-urna-eletronica-e-colocada-a-prova-por-hackers-em-um-teste-publico-de-seguranca>

Fuentes

- gob.pe: Oficina Nacional de Procesos Electorales — <https://www.gob.pe/onpe>

- gob.pe: Reportar incidentes de seguridad digital (Centro Nacional de Seguridad Digital) — <https://www.gob.pe/14084-reportar-incidentes-de-seguridad-digital>
- CiberLATAM: Perú avanza con ciberseguridad sin ley general — <https://ciberlatam.com/noticias/peru-avanza-ciberseguridad-ley-general>

Propuesta ciudadana de libre uso — no es un proyecto presentado. Versión web:
<https://unimauro.github.io/agenda-legislativa-tech/p/CIB-13.html>