

Ley que regula la divulgación coordinada de vulnerabilidades y protege a los investigadores de seguridad de buena fe

Modifica el artículo 12 de la Ley 30096 para eximir de responsabilidad penal a quien identifica y reporta vulnerabilidades de buena fe bajo condiciones fijadas en la propia ley (sin daño, sin exigir pago, reporte en setenta y dos horas, minimización y eliminación de datos, exclusión de sistemas de control industrial y de defensa), obliga a las entidades públicas a publicar políticas de divulgación, excluye la responsabilidad administrativa y civil del investigador que cumple las condiciones y habilita recompensas como supuesto excluido de la Ley 32069.

Comisión (Cámara de Diputados): Justicia y Derechos Humanos (+ Ciencia, Innovación Tecnológica y Sociedad Digital) ·

Revisora (Senado): Justicia y Derechos Humanos · **Prioridad:** media · **Costo fiscal:** nulo · **Plazo:** corto

Plan Perú 2050: Ciber Seguridad, Capital Del Conocimiento

I. Exposición de motivos

El artículo 12 de la Ley 30096, incorporado por la Ley 30171, exime de responsabilidad penal solo a quien realiza pruebas autorizadas para proteger sistemas informáticos. Un ciudadano o investigador que detecta una falla en un portal público y la reporta sin autorización previa queda expuesto a una denuncia por acceso ilícito (artículo 2) o, si conserva una muestra de los datos expuestos, por el delito del artículo 12-A (incorporado por el Decreto Legislativo 1700 y modificado por el Decreto Legislativo 1741), lo que desincentiva el reporte y favorece que las vulnerabilidades se vendan o exploten. El Decreto Supremo 126-2025-PCM (art. 18.1, literal i) incluye entre los deberes de los proveedores la realización proactiva de pruebas de vulnerabilidades, pero no existe un canal legal para que terceros reporten de buena fe ni obligación de las entidades públicas de tener una política de divulgación. Las entidades tampoco pueden pagar recompensas, porque la Ley 32069 exige procedimientos de selección incompatibles con pagos por resultado a personas no identificadas de antemano. En Estados Unidos, la directiva BOD 20-01 obligó a las agencias federales a publicar políticas de divulgación, y la Directiva NIS2 encarga a los CSIRT actuar como coordinadores.

II. Fórmula legal

EL CONGRESO DE LA REPÚBLICA ha dado la Ley siguiente:

LEY QUE REGULA LA DIVULGACIÓN COORDINADA DE VULNERABILIDADES Y PROTEGE A LOS INVESTIGADORES DE SEGURIDAD DE BUENA FE

Artículo 1. Objeto

La presente ley tiene por objeto regular la divulgación coordinada de vulnerabilidades en sistemas informáticos, proteger a los investigadores de seguridad que actúan de buena fe y habilitar programas de recompensas en las entidades públicas.

Artículo 2. Modificación del artículo 12 de la Ley 30096

Se modifica el artículo 12 de la Ley 30096, Ley de Delitos Informáticos, incorporado por la Ley 30171, en los términos siguientes:

«Artículo 12. Exención de responsabilidad penal

Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2, 3, 4, 7 y 10:

- a) con el propósito de llevar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos; o
- b) con el propósito exclusivo de identificar y reportar una vulnerabilidad, siempre que concurran las condiciones siguientes: 1) no altere ni destruya datos ni interrumpa el servicio; 2) no acceda a datos más allá de lo necesario para demostrar la vulnerabilidad y elimine los obtenidos una vez reportada; 3) la reporte al titular del sistema o al Centro Nacional de Seguridad Digital dentro de las setenta y dos horas de haberla identificado; 4) no condicione el reporte ni la no divulgación a pago alguno fuera de un programa de recompensas del titular; y 5) no la divulgue públicamente antes de su corrección o del vencimiento del plazo de noventa días o de su prórroga autorizada por el Centro Nacional de Seguridad Digital, previa coordinación con este.

La exención del literal b) comprende la posesión temporal de la muestra mínima de datos necesaria para demostrar la vulnerabilidad, sin perjuicio de lo dispuesto en el artículo 12-A respecto de cualquier otra conducta de adquisición, comercialización o tráfico de datos.

La exención del literal b) no comprende las pruebas activas sobre sistemas de control industrial de operadores de servicios esenciales o de activos críticos nacionales, ni sobre sistemas de defensa e inteligencia, salvo que se realicen en el marco de un programa de divulgación del titular que expresamente los incluya.

Las políticas de divulgación solo establecen canales y plazos de reporte, sin ampliar ni restringir las condiciones de la exención.»

Artículo 3. Política nacional de divulgación coordinada

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, aprueba mediante resolución la política nacional de divulgación coordinada de vulnerabilidades. El Centro Nacional de Seguridad Digital, o el órgano que haga sus veces, actúa como coordinador entre investigadores y titulares de sistemas y mantiene la reserva de la identidad del investigador que lo solicite.

Artículo 4. Políticas de divulgación en entidades públicas

Las entidades de la administración pública publican en su sede digital una política de divulgación de vulnerabilidades con un canal de reporte, el alcance de los sistemas incluidos, los compromisos de respuesta y el plazo de corrección, conforme al formato que apruebe la Secretaría de Gobierno y Transformación Digital.

Artículo 5. Plazos de respuesta

La entidad que recibe un reporte acusa recibo en un plazo no mayor de cinco días hábiles y corrige o mitiga la vulnerabilidad en un plazo no mayor de noventa días calendario, prorrogable por razones técnicas debidamente justificadas ante el Centro Nacional de Seguridad Digital.

Artículo 6. Programas de recompensas

6.1. Las entidades públicas pueden implementar programas de recompensas por vulnerabilidades con bases públicas que fijen montos por severidad, con cargo a su presupuesto institucional, o contratar plataformas especializadas conforme a la Ley 32069, Ley General de Contrataciones Públicas.

6.2. El pago directo de recompensas por vulnerabilidades validadas, hasta el monto máximo por reporte que fije el reglamento, constituye un supuesto excluido del ámbito de aplicación de la Ley 32069, está sujeto al control del Sistema Nacional de Control y al régimen tributario vigente.

Artículo 7. Ausencia de responsabilidad y prohibición de represalias

7.1. La conducta del investigador que cumpla las condiciones del literal b) del artículo 12 de la Ley 30096 no constituye infracción administrativa, incluida la prevista en la Ley 29733 por el acceso incidental a datos, ni genera responsabilidad civil por los mismos hechos, salvo daño causado con dolo o culpa inexcusable.

7.2. Las entidades públicas no formulan denuncia ni inician procedimientos administrativos o acciones civiles contra dicho investigador, ni adoptan represalias contractuales o de acceso a servicios. Si se inicia una investigación, la entidad informa al Ministerio Público del cumplimiento de las condiciones de la exención.

Artículo 8. Sector privado

Se promueve la adopción voluntaria de políticas de divulgación en el sector privado. Los proveedores de servicios digitales comprendidos en el numeral 9.1 del artículo 9 del Decreto de Urgencia 007-2020 están obligados a adoptarlas; los fabricantes e importadores de dispositivos conectados lo están conforme a la ley de la materia.

Primera. Disposición Complementaria Final

Reglamentación. El Poder Ejecutivo, mediante decreto supremo refrendado por el presidente del Consejo de Ministros, el ministro de Justicia y Derechos Humanos y el ministro de Economía y Finanzas, reglamenta la presente ley en un plazo no mayor de noventa días hábiles contados a partir del día siguiente de su publicación.

Segunda. Disposición Complementaria Final

Financiamiento. La implementación de la presente ley se financia con cargo al presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al Tesoro Público. Los programas de recompensas son facultativos.

Única. Disposición Complementaria Transitoria

Plazo de adecuación. Las entidades del Poder Ejecutivo publican sus políticas de divulgación en un plazo de seis meses y los gobiernos regionales y locales en un plazo de dieciocho meses, contados desde la aprobación de la política nacional.

III. Análisis costo-beneficio

Costo fiscal nulo: publicar una política y un canal de reporte tiene costo marginal absorbible por las oficinas de tecnologías de la información existentes; los programas de recompensas son facultativos y se financian con presupuesto institucional. El beneficio es identificar vulnerabilidades antes de que sean explotadas, a un costo muy inferior a la respuesta ante un incidente. La reforma del artículo 12 da seguridad jurídica a la comunidad técnica sin crear una licencia para atacar: las condiciones están en la ley (sin daño, sin exigir pago, minimización y eliminación de datos, reporte en setenta y dos horas) y se excluyen los sistemas de control industrial y de defensa. El régimen de recompensas como supuesto excluido de la Ley 32069 permite pagar por resultado con control posterior.

Normas que modifica

- Ley 30096, Ley de Delitos Informáticos (art. incorporado por Ley 30171), art. 12 — *modifica*
- Ley 30096, art. 12-A (D.Leg. 1700 y 1741), art. 12-A (salvedad expresa) — *complementa*
- Ley 32069, Ley General de Contrataciones Públicas, supuesto excluido (art. 6.2 de la ley) — *complementa*
- Ley 29733, Ley de Protección de Datos Personales, exclusión de responsabilidad por acceso incidental (art. 7.1 de la ley) — *complementa*

Entidades implicadas (quién hace qué)

- **PCM-SGTD / CNSD** (rectora): Aprueba la política nacional y el formato de políticas (arts. 3 y 4), coordina reportes, autoriza prórrogas y reserva la identidad del investigador (arts. 3 y 5).
- **Entidades** (ejecutora): Publican políticas, responden en cinco días y corrigen en noventa (arts. 4 y 5); pueden pagar recompensas (art. 6).
- **MP** (supervisora): Valora la exención del art. 12 en cada caso, como titular de la acción penal (art. 7.2).
- **CGR** (supervisora): Controla los pagos de recompensas excluidos de la Ley 32069 (art. 6.2).
- **MEF** (reglamentadora): Corefrenda el reglamento que fija el monto máximo de recompensa (DCF Primera).

Sujetos obligados: Entidades de la administración pública; proveedores de servicios digitales del numeral 9.1 del art. 9 del D.U. 007-2020; investigadores que invoquen la exención (deben cumplir sus condiciones).

Beneficiarios: Comunidad técnica e investigadores de seguridad; entidades y usuarios de sistemas públicos que se benefician de la corrección temprana de vulnerabilidades. No cuantificable con información pública.

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

Tipo: neutro

Costo para el Estado: S/ 0 (sin gasto obligatorio); recompensas facultativas no cuantificables

Horizonte: anual

Financiamiento: Presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al Tesoro Público.

Supuestos: La publicación de políticas y la atención de reportes se absorben en las oficinas de tecnologías de la información existentes; las recompensas dependen de la decisión de cada entidad.

Beneficio para el Estado: Detección temprana de vulnerabilidades en sistemas públicos a costo muy inferior al de un incidente. No cuantificable con información pública.

Beneficio para la sociedad: Seguridad jurídica para la comunidad técnica y menor exposición de datos ciudadanos. No cuantificable con información pública.

Inversión privada: No aplica.

Costo para privados: Proveedores del art. 9.1 del D.U. 007-2020: publicar una política y un canal de reporte (costo marginal).

Riesgos: Abuso de la exención como cobertura de intrusiones (mitigado por condiciones taxativas y exclusión de sistemas críticos); demoras de corrección en entidades con baja capacidad.

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

- **Constitucional** — Con observaciones: La exención penal condicionada para investigadores de buena fe es una opción de política criminal válida y respeta la legalidad penal al fijar condiciones verificables. Pero la prohibición a las entidades de 'iniciar acciones' civiles o penales es una barrera procesal que afecta el acceso a la justicia (art. 139.3) y no puede limitar al Ministerio Público (art. 159).
- **Técnica legislativa** — Con observaciones: La modificación del art. 12 de la Ley 30096 se hace correctamente sobre el texto vigente (que incorporó la Ley 30171) y es la vía adecuada. Sin embargo, el régimen de recompensas choca con la Ley 32069, la cláusula de no represalia está mal dirigida y la obligación de los operadores de servicios esenciales remite a una categoría que no existe en la ley vigente.
- **Concordancia normativa** — Con observaciones: Cita correcta: el art. 12 de la Ley 30096 fue incorporado por la Ley 30171 (exención por pruebas autorizadas). No hay duplicidad con norma vigente. Debe preservar el art. 12-A (incorporado por D.Leg. 1700, modificado por D.Leg. 1741), resolver el pago de recompensas en el marco de la Ley 32069 y armonizar con CIB-07 y CIB-02.
- **Seguridad** — Con observaciones: Propuesta muy valiosa que corrige un vacío de la Ley 30096. Debe excluir de la exención las pruebas activas no autorizadas sobre sistemas de control industrial de infraestructuras críticas y de defensa, extender la protección frente a acciones de privados y por la Ley 29733, y evitar que el investigador quede impedido indefinidamente de divulgar si la entidad no corrige.
- **Derecho tecnológico** — Con observaciones: Reforma necesaria y bien diseñada (buena fe, no daño, minimización, reporte sin demora), con referentes correctos (BOD 20-01 de CISA, NIS2 art. 12). Debe extender la exención al tráfico/posesión de datos del art. 12-A (DL 1700) en lo estrictamente necesario, excluir la exigencia de pago como condición (que es extorsión), definir 'operadores de servicios esenciales' y ordenar el régimen de pago de recompensas.

IV. Efecto de la vigencia de la norma

Modifica el artículo 12 de la Ley 30096 (incorporado por la Ley 30171); deja a salvo el artículo 12-A (incorporado por el D.Leg. 1700 y modificado por el D.Leg. 1741) salvo la posesión temporal de la muestra mínima; establece un supuesto excluido del ámbito de la Ley 32069; complementa la Ley 29733, el Decreto de Urgencia 007-2020, el Decreto Supremo 126-2025-PCM y el Decreto Legislativo 1412. No requiere votación de ley orgánica.

V. Indicador de éxito al 2031

A 2029, 100 % de ministerios y organismos públicos del Poder Ejecutivo con política de divulgación publicada; informe anual del CNSD sobre vulnerabilidades reportadas y corregidas.

Normas relacionadas

- Ley 30171, Ley que modifica la Ley 30096 (incorpora el artículo 12, exención por pruebas autorizadas) — <https://leyes.congreso.gob.pe/Documentos/Leyes/30171.pdf>
- Ley 30096, Ley de Delitos Informáticos (2013) — <https://leyes.congreso.gob.pe/Documentos/Leyes/30096.pdf>
- Decreto Legislativo 1700, que incorpora el artículo 12-A a la Ley 30096 — <https://busquedas.elperuano.pe/dispositivo/NL/2480387-2>
- Decreto Supremo 126-2025-PCM, Reglamento del Decreto de Urgencia 007-2020 (Marco de Confianza Digital) — <https://busquedas.elperuano.pe/dispositivo/EX/2455024-1>

- 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

Según verificación en SPLEY del revisor normativo, no se identificaron proyectos del periodo 2021-2026 sobre divulgación coordinada de vulnerabilidades o protección de investigadores de seguridad.

Referencias internacionales

- Estados Unidos: CISA Binding Operational Directive 20-01: políticas de divulgación de vulnerabilidades en agencias federales — <https://www.cisa.gov/news-events/directives/bod-20-01-develop-and-publish-vulnerability-disclosure-policy>
- Unión Europea: ENISA: Coordinated Vulnerability Disclosure Policies in the EU — <https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu>
- Reino Unido: NCSC: política de reporte de vulnerabilidades — <https://www.ncsc.gov.uk/information/vulnerability-reporting>
- Unión Europea: Directiva (UE) 2022/2555 (NIS2), medidas para un elevado nivel común de ciberseguridad — <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

Fuentes

- Apaxi (07-09-2026): Normas de ciberseguridad para empresas en el Perú — <https://apaxi.info/2026/09/07/normas-ciberseguridad-empresas-peru/>
- gob.pe: Reportar incidentes de seguridad digital (Centro Nacional de Seguridad Digital) — <https://www.gob.pe/14084-reportar-incidentes-de-seguridad-digital>
- Texto del DS 126-2025-PCM (copia LP Derecho) — <https://img.lpderecho.pe/wp-content/uploads/2025/11/Decreto-Supremo-126-2025-PCM-LPDerecho.pdf>

Propuesta ciudadana de libre uso — no es un proyecto presentado. Versión web:
<https://unimauro.github.io/agenda-legislativa-tech/p/CIB-11.html>