

**PROYECTO DE LEY QUE AMPLÍA LA
RESPONSABILIDAD ADMINISTRATIVA DE LAS
PERSONAS JURÍDICAS FRENTE A DELITOS
INFORMÁTICOS Y VULNERACIONES DE DATOS
PERSONALES**

El Grupo Parlamentario PODEMOS PERÚ, a iniciativa del congresista **GUIDO BELLIDO UGARTE**, en ejercicio de iniciativa legislativa que le confiere el artículo 107 de la Constitución Política del Perú y conforme lo establecen los artículos 22 literal c), 67, 75 y 76 numeral 2 del Reglamento del Congreso de la República, proponen el siguiente proyecto de ley.

FÓRMULA LEGAL

El Congreso de la República
Ha dado la siguiente ley:

**LEY QUE AMPLÍA LA RESPONSABILIDAD ADMINISTRATIVA DE LAS PERSONAS
JURÍDICAS FRENTE A DELITOS INFORMÁTICOS Y VULNERACIONES DE DATOS
PERSONALES**

Artículo 1. Objeto de la Ley

La presente Ley tiene por objeto fortalecer la responsabilidad administrativa de las personas jurídicas frente a los delitos informáticos y la filtración de datos personales, incorporando determinados ilícitos previstos en la Ley N° 30096, Ley de Delitos Informáticos, al ámbito de aplicación de la Ley N° 30424, Ley que regula la responsabilidad administrativa de las personas jurídicas por el delito de cohecho activo transnacional, a fin de promover la prevención, el cumplimiento normativo y la protección de los derechos fundamentales en el entorno digital.

Artículo 2. Finalidad de la Ley

La presente Ley tiene por finalidad fortalecer el régimen de responsabilidad administrativa de las personas jurídicas frente a los delitos informáticos y la filtración indebida de datos personales, promoviendo la adopción obligatoria de modelos de prevención que incorporen medidas efectivas de ciberseguridad y protección de la información, con el objeto de salvaguardar los derechos fundamentales de las personas, garantizar la confianza digital, prevenir riesgos tecnológicos y contribuir al fortalecimiento de la integridad corporativa en el país.

**Artículo 3. Modificación del artículo 1° de la Ley N° 30424, Ley que regula la
responsabilidad administrativa de las personas jurídicas por el delito de cohecho
activo transnacional**

Modifícase el artículo 1° de la Ley N° 30424, Ley que regula la responsabilidad administrativa de las personas jurídicas por el delito de cohecho activo transnacional, en los términos siguientes:

Artículo 1. Objeto de la Ley

La presente ley regula la responsabilidad administrativa de las personas jurídicas nacionales o extranjeras en el proceso penal por los delitos previstos en los artículos:

- a. 199, 226, 228, 384, 397, 397-A, 398 y 400 del Código Penal.
- b. 1, 2, 3, 4, 5 y 6 del Decreto Legislativo 1106, Decreto Legislativo de lucha eficaz contra el lavado de activos y otros delitos relacionados a la minería ilegal y el crimen organizado.
- c. 1, 2, 3, 4, 5, 6, 7, 8 y 10 de la Ley 28008, Ley de los delitos aduaneros.
- d. 1, 2, 4, 5, 5-A, 5-B, 5-C y 5-D del Decreto Legislativo 813, Ley Penal Tributaria.
- e. 2, 3, 4, 4-A, 5, 6, 6-A, 6-B y 8 del Decreto Ley 25475, Decreto Ley que establece la penalidad para los delitos de terrorismo y los procedimientos para la investigación, la instrucción y el juicio.
- f. 2, 3, 4, 7, 8, 9 y 10 de la Ley N° 30096, Ley de Delitos Informáticos.

El régimen de consecuencias accesorias, previsto en el Código Penal, se aplica a las personas jurídicas involucradas en los delitos no comprendidos en el presente artículo.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Adecuación de la reglamentación

El Poder Ejecutivo adecuará el reglamento de la Ley N° 30424 en un plazo no mayor de noventa (90) días calendario, contados desde la publicación de la presente Ley, incorporando lineamientos técnicos mínimos en materia de ciberseguridad y protección de datos personales para los modelos de prevención.

Lima, febrero del 2026


Francisco Porales


GUIDO BELLIDO UGARTE
CONGRESISTA DE LA REPÚBLICA


Horacio Anco


Edgar Riebel Monto



EXPOSICIÓN DE MOTIVOS

I. FUNDAMENTOS DE LA PROPUESTA

1.1. ANTECEDENTES

En los últimos años, el Perú ha experimentado un incremento sostenido de delitos informáticos y filtraciones masivas de datos personales que han afectado a millones de ciudadanos y a diversas entidades públicas y privadas. La exposición indebida de información sensible, como nombres, domicilios, números de DNI, firmas, fotografías, correos electrónicos y datos financieros, se ha convertido en un fenómeno recurrente que evidencia debilidades estructurales en los sistemas de seguridad digital. Estos eventos revelan que el riesgo digital no proviene únicamente de ataques externos sofisticados, sino también de accesos internos indebidos, fallas operativas, ausencia de cifrado y carencia de mecanismos efectivos de supervisión.

El marco normativo vigente se sustenta principalmente en la Ley N° 30096, Ley de Delitos Informáticos, y la Ley N° 30424, que regula la responsabilidad administrativa de las personas jurídicas. No obstante, esta última no incorpora dentro de su catálogo los delitos informáticos, lo que impide atribuir responsabilidad a las empresas cuando la ausencia de controles o sistemas de prevención facilita la comisión de estos ilícitos o la filtración masiva de datos personales.

Esta omisión genera un vacío legal que debilita la protección de derechos fundamentales y reduce los incentivos para que las organizaciones adopten estándares adecuados de ciberseguridad y gestión de riesgos digitales.

Por ello, la presente iniciativa legislativa tiene por finalidad cerrar dicha brecha normativa, fortaleciendo el régimen de responsabilidad administrativa de las personas jurídicas y estableciendo obligaciones claras de prevención y diligencia en materia de ciberseguridad, a fin de garantizar una protección efectiva de los datos personales y de los derechos fundamentales en el entorno digital.

El Proyecto de Ley presenta en similar materia el siguiente antecedente:

NRO. DE PROYECTO DE LEY	DENOMINACIÓN
13035/2025-CR	PROYECTO DE LEY QUE REFUERZA LA RESPONSABILIDAD DE LAS PERSONAS JURÍDICAS POR DELITOS INFORMÁTICOS Y FILTRACIÓN DE DATOS PERSONALES

1.2. IDENTIFICACIÓN DEL PROBLEMA

En octubre de 2024, el banco reconoció que datos personales de un grupo de sus clientes fueron expuestos por un tercero sin autorización, lo que llevó a la intervención y supervisión por parte de la Superintendencia de Banca, Seguros y AFP (SBS) ante la preocupación por la información expuesta y la interrupción de servicios digitales¹.

En junio de 2025, la compañía inició investigaciones tras la difusión en internet de presuntas brechas de seguridad que habrían expuesto registros de usuarios peruanos, incluyendo nombres, DNI y números de teléfono, como muestra de prueba de un posible hackeo masivo de datos, lo que motivó alerta y análisis técnico sobre la gestión de ciberseguridad de la empresa²

Reportes de investigación de seguridad digital señalaron que bases de datos antiguas de la empresa incluían millones de registros de clientes con información sensible, como nombres, DNI, correos electrónicos, teléfonos y hasta datos parciales de tarjetas, expuestos por vulnerabilidades de configuración. Aunque la empresa ha negado filtraciones recientes, estos incidentes han generado preocupación pública sobre el resguardo de datos personales.³

Informes oficiales y de la Agencia Andina señalan que en los últimos años se incrementaron las denuncias por vulneraciones de datos personales en empresas del sector financiero, telecomunicaciones y comercio electrónico, reflejando la existencia de fallas en la protección de información sensible de usuarios y consumidores.⁴

Ejemplos como estos generan una creciente preocupación social, pues ponen en evidencia que la normativa vigente no permite exigir responsabilidad administrativa a las personas jurídicas por delitos informáticos ni por filtraciones de datos personales derivadas de negligencia corporativa, produciendo un escenario de impunidad estructural en el cual las organizaciones que administran grandes volúmenes de información sensible no están legalmente obligadas a implementar modelos robustos de prevención en materia de ciberseguridad.

Como consecuencia, las vulneraciones de datos se repiten en sectores clave como el financiero, telecomunicaciones, educación y servicios digitales, generando suplantaciones de identidad, fraudes electrónicos, extorsiones, afectaciones patrimoniales y daños psicológicos a miles de ciudadanos. Actualmente, la respuesta estatal se limita, en muchos casos, a sanciones administrativas o exhortaciones públicas, las cuales resultan insuficientes frente al impacto colectivo de estos incidentes, mientras que la ausencia de responsabilidad corporativa

¹ <https://www.tvperu.gob.pe/noticias/nacionales/interbank-reconoce-que-datos-de-sus-clientes-fueron-expuestos-por-un-tercero>

² https://latinanoticias.pe/mundo/alerta-por-hackeo-masivo-millones-de-datos-de-clientes-de-movistar-peru-habrian-sido-robados-adp-noticia_20250604/

³ <https://andina.pe/agencia/noticia-investigacion-reporta-brecha-expone-datos-bancarios-clientes-cineplanet-782966.aspx>

⁴ <https://andina.pe/agencia/noticia-crecen-denuncias-vulnerar-datos-personales-sector-financiero-y-comercio-electronico-926904.aspx>

efectiva debilita el derecho constitucional a la protección de datos personales y erosiona progresivamente la confianza ciudadana en el entorno digital.

Por ello, el presente Proyecto de Ley resulta necesario y oportuno, al incorporar los delitos informáticos al ámbito de aplicación de la Ley N° 30424, fortalecer la responsabilidad administrativa de las personas jurídicas y establecer la obligación de adoptar modelos de prevención con estándares mínimos de ciberseguridad, con el objeto de cerrar vacíos normativos, promover una cultura empresarial de diligencia digital y garantizar una protección real y efectiva de los derechos fundamentales en la sociedad de la información.

JUSTIFICACIÓN LEGAL

La presente iniciativa legislativa se encuentra plenamente justificada desde el punto de vista constitucional y legal, al estar orientada a fortalecer la tutela efectiva de derechos fundamentales y a cerrar un vacío normativo que actualmente impide atribuir responsabilidad administrativa a las personas jurídicas por delitos informáticos y filtraciones masivas de datos personales derivadas de negligencia corporativa. El artículo 2°, inciso 6)⁶ de la Constitución Política del Perú reconoce el derecho fundamental de toda persona a que los servicios informáticos, públicos o privados, no suministren informaciones que afecten su intimidad personal y familiar, consagrando así el principio de autodeterminación informativa. Este derecho impone al Estado el deber de adoptar medidas normativas que garanticen el uso legítimo, seguro y controlado de los datos personales, así como de establecer mecanismos eficaces de sanción frente a su vulneración.

En ese marco, si bien la Ley N° 30096 tipifica los delitos informáticos y la Ley N° 29733 regula la protección de datos personales, el régimen actual resulta incompleto, pues la Ley N° 30424 no incluye dentro de su ámbito de aplicación dichos ilícitos, lo que impide exigir responsabilidad administrativa a las personas jurídicas cuando la comisión del delito o la filtración de datos se ve facilitada por la ausencia de controles internos, políticas de seguridad o sistemas de prevención.

Esta omisión normativa debilita la eficacia del ordenamiento jurídico, favorece escenarios de impunidad estructural y reduce los incentivos para que las organizaciones adopten estándares adecuados de ciberseguridad.

La propuesta legislativa corrige esta deficiencia mediante la incorporación de los delitos informáticos previstos en la Ley N° 30096 al catálogo de la Ley N° 30424, estableciendo un vínculo directo entre la conducta delictiva y la obligación

⁶ Constitución Política del Perú:

Artículo 2.- Toda persona tiene derecho:

6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

empresarial de prevención. De este modo, se refuerza el principio de responsabilidad corporativa, conforme al cual las personas jurídicas deben responder no solo por la participación activa en un ilícito, sino también por la omisión de deberes de supervisión y diligencia razonable, criterio ya reconocido en el derecho comparado y en instrumentos internacionales de lucha contra el crimen organizado y la corrupción.

Asimismo, la iniciativa respeta el principio de legalidad, al delimitar de manera expresa los delitos comprendidos, y el principio de proporcionalidad, al circunscribirse a un régimen de responsabilidad administrativa que prioriza la prevención mediante modelos de cumplimiento, sin criminalizar la actividad empresarial ni obstaculizar el desarrollo tecnológico. La reforma se orienta a promover una cultura de cumplimiento digital, incentivando la adopción de medidas técnicas y organizativas acordes con la naturaleza y volumen de los datos administrados.

1.3. PROPUESTA DE SOLUCIÓN

El presente proyecto de ley propone incorporar los delitos informáticos previstos en los artículos 2, 3, 4, 7, 8, 9 y 10 de la Ley N° 30096 al ámbito de aplicación de la Ley N° 30424, fortaleciendo así el régimen de responsabilidad administrativa de las personas jurídicas.

Asimismo, establece la obligación de implementar modelos de prevención que incluyan medidas efectivas de ciberseguridad y protección de datos personales, promoviendo una cultura empresarial de cumplimiento normativo, supervisión interna y gestión de incidentes digitales.

1.5. MARCO NORMATIVO

- Constitución Política del Perú
- Reglamento del Congreso de la República
- Ley N° 30096, Ley de Delitos Informáticos
- Ley N° 30424, Ley de responsabilidad administrativa de personas jurídicas
- Ley N° 29733, Ley de Protección de Datos Personales

II. EFECTOS DE LA VIGENCIA DE LA NORMA SOBRE LA LEGISLACIÓN NACIONAL

La presente iniciativa legislativa no colisiona con ninguna norma constitucional, no contraviene ninguna disposición legal del ordenamiento jurídico peruano. Por el contrario, con la vigencia de la presente iniciativa legislativa permitirá ampliar el catálogo de delitos que generan responsabilidad administrativa de las personas jurídicas, incorporando expresamente los delitos informáticos al ámbito de aplicación de la Ley N° 30424, lo que obligará a las empresas a implementar modelos de prevención que contemplen estándares mínimos de ciberseguridad y protección de

datos personales, fortalecerá la coordinación entre las autoridades penales y los organismos de supervisión, consolidará un régimen preventivo orientado a reducir riesgos sistémicos en los entornos digitales y garantizará una tutela efectiva del derecho constitucional a la protección de datos personales, contribuyendo así al fortalecimiento del Estado de Derecho y a la construcción de un ecosistema digital más seguro, transparente y responsable.

III. ANÁLISIS COSTO BENEFICIO

Esta propuesta legislativa, no irroga gastos adicionales en el presupuesto del sector público, ajustándose a lo dispuesto en literal a) del inciso 2) del artículo 76° del Reglamento del Congreso de la República, de igual manera su aplicación se plantea en el marco de lo establecido, que se financia con cargo a los presupuestos institucionales de los sectores involucrados para el cumplimiento de sus funciones, en el marco de sus competencias y sin demandar recursos adicionales al tesoro público. Los beneficios del Proyecto de Ley serán los siguientes:

ACTORES INVOLUCRADOS		ANÁLISIS	
	BENEFICIO	COSTO	
ESTADO	- Fortalecerá la capacidad sancionadora frente a delitos informáticos. - Reducirá los costos institucionales derivados de filtraciones masivas. - Mejorará la confianza en los servicios públicos digitales. - Alineará el marco legal peruano con estándares internacionales de responsabilidad corporativa. - Contribuirá a consolidar un entorno favorable para la inversión digital. - Incrementará la protección efectiva de los datos personales.	Aprobación de la Ley y adecuación de la reglamentación	
	- Reducirá el riesgo de fraudes electrónicos y suplantaciones de identidad. - Fortalecerá la confianza ciudadana en el ecosistema digital. - Promoverá una cultura de prevención y transparencia empresarial. - Generará mecanismos reales de sanción frente a la negligencia corporativa. - Facilitará la reparación del daño.		
SOCIEDAD		Ninguno	
		Ninguno	

**VÍCTIMAS DE
DELITOS
INFORMÁTICOS**

- Disminuirá la repetición de incidentes similares.
- Reafirmará el carácter fundamental del derecho a la autodeterminación informativa.

IV. RELACIÓN CON LA AGENDA LEGISLATIVA Y LAS POLÍTICAS DE ESTADO DEL ACUERDO NACIONAL

La presente iniciativa legislativa tiene relación directa con las políticas de Estado en función a la Agenda Legislativa para el periodo anual de sesiones 2024-2025, contenida en RESOLUCIÓN LEGISLATIVA DEL CONGRESO N° 006-2024-2025-CR, según se detalla:

OBJETIVO: IV. ESTADO EFICIENTE, TRANSPARENTE Y DESCENTRALIZADO

- **Política de Estado 24. AFIRMACIÓN DE UN ESTADO EFICIENTE Y TRANSPARENTE**, respecto al siguiente tema:

93. TRANSPARENCIA EN EL ESTADO

- **Política de Estado 26. PROMOCIÓN DE LA ÉTICA Y LA TRANSPARENCIA, Y ERRADICACIÓN DE LA CORRUPCIÓN, EL LAVADO DE DINERO, LA EVASIÓN TRIBUTARIA Y EL CONTRABANDO EN TODAS SUS FORMAS**, respecto al siguiente tema:

95. LUCHA CONTRA LA CORRUPCIÓN

- **Política de Estado 28. PLENA VIGENCIA DE LA CONSTITUCIÓN Y DE LOS DERECHOS HUMANOS Y ACCESO A LA JUSTICIA E INDEPENDENCIA JUDICIAL**, respecto al siguiente tema:

97. MODERNIZACIÓN Y ACCESO EN EL SISTEMA DE JUSTICIA

98. MODIFICACIÓN EN TRÁMITES LEGALES Y EN PROCEDIMIENTOS JUDICIALES Y PROCESOS ADMINISTRATIVOS