PROYECTO DE LEY QUE REFUERZA LA RESPONSABILIDAD DE LAS PERSONAS JURÍDICAS POR DELITOS INFORMÁTICOS Y FILTRACIÓN DE DATOS PERSONALES

El congresista de la República que suscribe, **ALEJANDRO SOTO REYES**, integrante del **Grupo Parlamentario Alianza para el Progreso**, en ejercicio del derecho de iniciativa legislativa que le confiere el artículo 107 de la Constitución Política y los artículos 74 y 75 del Reglamento, propone el siguiente **PROYECTO DE LEY**:

FÓRMULA LEGAL

LEY QUE REFUERZA LA RESPONSABILIDAD DE LAS PERSONAS JURÍDICAS POR DELITOS INFORMÁTICOS Y FILTRACIÓN DE DATOS PERSONALES

Artículo 1. Objeto de la Ley

La presente ley tiene como objetivo garantizar la protección efectiva de los datos personales de los ciudadanos, estableciendo un mejor marco de responsabilidad que obligue a las personas jurídicas a adoptar medidas adecuadas de ciberseguridad, prevención y respuesta ante incidentes informáticos.

Artículo 2. Finalidad

La presente ley tiene por finalidad proteger la integridad de los datos personales de los ciudadanos, promoviendo una cultura de responsabilidad y prevención en las personas jurídicas frente a los riesgos derivados de los delitos informáticos y las filtraciones de información.

Artículo 3. Modificar el artículo 1 de la Ley 30424, Ley que regula la responsabilidad administrativa de las personas jurídicas en el proceso penal

Se modifica el artículo 1 de la Ley 30424, Ley que regula la responsabilidad administrativa de las personas jurídicas en el proceso penal, con el siguiente texto:

> ***"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:*
>
> *(…)*
>
> ***f) 2, 3, 4, 7, 8, 9 y 10 de la Ley 30096, Ley de Delitos Informáticos.***
>
> *(…)."*

Lima, 16 de octubre del 2025

FIRMA DIGITAL

Firmado digitalmente por: SOTO REYES Alejandro FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 29/10/2025 18:32:31-0500

ALEJANDRO SOTO REYES
Congresista de la República

FIRMA DIGITAL

Firmado digitalmente por: GARCIA CORREA Idelso Manuel FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 28/10/2025 11:50:00-0500

FIRMA DIGITAL

Firmado digitalmente por: SALHUANA CAVIDES Eduardo FAU 20161749126 hard
Motivo: Soy el autor del documento
Fecha: 28/10/2025 11:42:18-0500

FIRMA DIGITAL

Firmado digitalmente por: RUIZ RODRIGUEZ Magaly Rosmery FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 28/10/2025 12:48:25-0500

Firmado digitalmente por: SALHUANA CAVIDES Eduardo FAU 20161749126 hard
Motivo: En señal de conformidad
Fecha: 28/10/2025 11:42:36-0500

FIRMA DIGITAL

Firmado digitalmente por: CAMONES SORIANO Lady Mercedes FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 29/10/2025 17:00:16-0500

FIRMA DIGITAL

Firmado digitalmente por: JULON IRIGOIN Elva Edhit FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 29/10/2025 17:18:43-0500

EXPOSICIÓN DE MOTIVOS

En los últimos años, el Perú ha experimentado un crecimiento sostenido de incidentes vinculados a ciberataques y filtraciones masivas de datos personales, afectando tanto a entidades públicas como privadas. Estas vulneraciones no solo comprometen la intimidad y la autodeterminación informativa de los ciudadanos, sino que también erosionan la confianza en los servicios digitales y en la capacidad del Estado y de las empresas para resguardar información sensible. Casos recientes han expuesto bases de datos de millones de peruanos, evidenciando que las estructuras actuales de protección y responsabilidad resultan insuficientes frente a los nuevos riesgos del entorno digital.

El vertiginoso avance de las tecnologías de información y comunicación ha generado nuevas oportunidades de desarrollo social, pero también ha incrementado los riesgos vinculados a la seguridad, integridad y confidencialidad de los datos personales de los ciudadanos. En el Perú, la exposición de información sensible como credenciales, huellas, fotografías, direcciones o firmas a través de plataformas digitales ilegales o por accesos internos no autorizados revela una brecha normativa que exige atención legislativa.

El marco legal vigente en materia de protección de datos se encuentra principalmente contenido en la Ley 30096, Ley de Delitos Informáticos y la Ley 30424, Ley que regula la responsabilidad administrativa de las personas jurídicas en el proceso penal.

En abril de este año, la filtración masiva de datos de más de quince millones de peruanos desde las bases del RENIEC, en la cual se incluyeron nombres, domicilios, fotografías y firmas, evidenció que no sólo los ataques externos representan una amenaza, sino también el uso impropio de acceso interno[1]. Este acontecimiento subrayó la existencia de vacíos en la supervisión, control interno y responsabilidad empresarial de las entidades que manejan información personal.

Asimismo, en junio del mismo año, se hizo pública una alerta mundial acerca de la exposición de hasta dieciséis mil millones de credenciales de usuario, que podrían pertenecer a ciudadanos peruanos y de otros países[2]. Este hecho evidencia la interconectividad de las amenazas digitales y la necesidad de normas modernas que trasciendan el ámbito puramente

---

1 Obtenido de: https://larepublica.pe/sociedad/2025/04/12/filtran-datos-personales-de-15-millones-de-peruanos-de-la-reniec-trabajadora-del-mininter-bajo-sospecha-194376

2 Obtenido de: https://www.infobae.com/peru/2025/06/20/gobierno-peruano-replica-alerta-mundial-por-filtracion-de-16-mil-millones-de-contrasenas-y-datos-de-usuarios/

administrativo y prevengan eventuales perjuicios colectivos derivados de filtraciones o accesos ilegítimos a datos.

En este contexto, la normativa vigente presenta deficiencias relevantes. La Ley 30096, Ley de Delitos Informáticos, junto con la Ley 30424, que regula la responsabilidad administrativa de las personas jurídicas, resultan insuficientes para contemplar los escenarios de negligencia o falta de diligencia empresarial en materia de ciberseguridad. La ausencia de criterios específicos sobre la responsabilidad de las personas jurídicas por filtraciones de datos y delitos informáticos deja desprotegidos a los ciudadanos y debilita los incentivos para que las empresas adopten mecanismos de control eficaces.

Por tanto, resulta imprescindible dotar al marco legal de una regulación que refuerce la responsabilidad empresarial frente a los riesgos digitales, estableciendo obligaciones claras de prevención, supervisión, gestión de incidentes y reparación del daño. La presente iniciativa legislativa tiene por objeto precisamente delimitar dicha responsabilidad, promoviendo una cultura empresarial de cumplimiento digital, y hacerlo de forma coherente con derechos fundamentales como la protección de datos personales, la dignidad de la persona y el interés colectivo.

Debe destacarse que los delitos informáticos, tipificados en la Ley 30096, fueron concebidos para sancionar conductas como el acceso ilícito, la interceptación de comunicaciones o el fraude informático, ley que ha ido actualizándose con el pasar de los años. Del mismo modo, si bien la Ley 30424, regula la responsabilidad administrativa de las personas jurídicas por ciertos delitos, su catálogo actual no incorpora los delitos informáticos previstos en la Ley 30096, lo que impide exigir a las empresas un estándar de diligencia acorde con los desafíos tecnológicos contemporáneos. Esta omisión merece ser corregida mediante una modificación legislativa que permita imputar responsabilidad a las personas jurídicas cuando la ausencia de controles o sistemas de prevención haya facilitado o no impedido la comisión de delitos informáticos o la filtración masiva de información personal.

Los sectores privado y público del país han visto cómo las filtraciones de datos se vuelven un evento recurrente; entidades financieras, empresas de telecomunicaciones, instituciones educativas y plataformas de servicios han estado expuestas a vulnerabilidades que, según reportes de LP Pasión por el Derecho[3] sobre ciberseguridad en el ámbito financiero, se generan no necesariamente por sofisticados ataques externos sino por fallas operativas, ausencia de cifrado y falta de monitoreo en sistemas informáticos. Este panorama obliga a

[3] Obtenido de: https://lpderecho.pe/ciberseguridad-vulneracion-datos-personales-entidades-financieras/

repensar la responsabilidad que deben asumir las personas jurídicas distintas de la acción penal individual.

Los efectos de estos vacíos normativos trascienden lo técnico, afectan la confianza pública, incrementan el riesgo de suplantaciones de identidad, fraudes electrónicos, pérdida de datos sensibles e impactos económicos para los ciudadanos. El caso de una empresa de entretenimiento peruana, como fue el caso de Cineplanet[4] que negó inicialmente una vulneración de su base de datos, muestra cómo la opacidad empresarial agrava la sensación de impunidad y exige un marco de control más claro. Es por ello que, la presente reforma atiende esta necesidad, estableciendo mecanismos que incentiven la transparencia empresarial ante incidentes digitales.

Desde la perspectiva constitucional, la protección de los datos personales forma parte del derecho a la intimidad, al honor y a la autodeterminación informativa. La falta de regulación adecuada en materia de responsabilidad empresarial frente a delitos informáticos debilita estos derechos, al dejar en el limbo legal la vía de reparación o sanción de conductas corporativas. Al reforzar el régimen de sanción administrativa de las personas jurídicas, mediante la modificación de la Ley 30424, esta iniciativa contribuye a restituir el equilibrio entre tecnología, mercado y derechos fundamentales.

Se aprecia además que, a nivel comparado, las legislaciones de países de la región como Chile o Colombia han adoptado marcos normativos donde se exige a las empresas operar con estándares mínimos de ciberseguridad y donde la responsabilidad corporativa frente a incidentes informáticos no está limitada a la sanción penal individual. Esta iniciativa permite que el Perú se alinee con dichos estándares, fortalezca su competitividad y asegure que el riesgo digital no sea una externalidad social, sino parte de la gobernanza corporativa responsable.

La filtración de datos personales no es un incidente menor, sus efectos se extienden a la suplantación de identidad, fraudes bancarios, extorsiones, acoso digital y afectaciones a la integridad patrimonial de miles de familias. Informes nacionales señalan que las entidades financieras y empresas de servicios han enfrentado múltiples vulneraciones, como lo documenta la Autoridad Nacional de Protección de Datos Personales (ANPD) en procedimientos sancionadores a entidades que no notificaron incidentes[5]. Estos hechos no

[4] Obtenido de: https://www.infobae.com/peru/2025/09/27/cineplanet-sobre-filtracion-de-datos-la-base-de-datos-no-ha-sido-vulnerada/

[5] Obtenido de: https://www.gob.pe/institucion/anpd/noticias/305427-anpd-sanciona-a-entidad-bancaria-con-s-166-mil-40-uits-por-no-resguardar-la-confidencialidad-de-los-datos-personales-de-sus-clientes

sólo erosionan la confianza ciudadana en el entorno digital, sino que generan cargas psicológicas y económicas para los afectados, quienes muchas veces carecen de mecanismos legales para exigir reparación. La ANPD, ha advertido públicamente que gran parte de las filtraciones en el país responde a la ausencia de protocolos básicos de resguardo y monitoreo.

En el ámbito privado, las entidades financieras y grandes corporaciones tampoco han estado exentas de incidentes de seguridad que comprometen información sensible de los usuarios. Diversos reportes difundidos[6], han advertido sobre vulneraciones que habrían afectado a bancos como Interbank, BCP, BBVA y Scotiabank, donde se reportó la exposición de correos electrónicos, nombres, números de DNI, direcciones, números telefónicos, datos financieros e incluso patrones de consumo. En muchos casos, estos hechos no fueron el resultado de un ataque informático altamente sofisticado, sino de fallas operativas internas, ausencia de cifrado, configuraciones erróneas de servidores o falta de monitoreo oportuno, evidenciando que el riesgo no proviene únicamente de agentes externos, sino de la debilidad de las propias políticas de ciberseguridad. A pesar de la gravedad potencial de estas filtraciones, la respuesta estatal suele limitarse a la imposición de sanciones administrativas o a exhortaciones públicas, lo cual resulta insuficiente para reparar el daño causado a los ciudadanos. Esta situación refuerza la necesidad de un marco penal que obligue a adoptar medidas efectivas para prevenir y responder a este tipo de incidente.

Los delitos informáticos como el acceso ilícito, la interceptación de datos, la suplantación de identidad o la comercialización indebida de información, se han sofisticado mediante el uso de aplicaciones móviles falsas y vulneración de sistemas en la nube. La ciberdelincuencia transnacional aprovecha la insuficiencia normativa para operar sin freno, y el perjuicio se multiplica cuando quienes tienen la obligación legal de proteger los datos de los ciudadanos no adoptan medidas mínimas de seguridad.

Por ello, la presente iniciativa se orienta a reforzar el régimen de responsabilidad administrativa aplicable a las personas jurídicas, ampliando la cobertura de la Ley 30424 para incluir los delitos informáticos previstos en los artículos 2, 3, 4, 7, 8, 9 y 10 de la Ley 30096. Con ello se asegura que las organizaciones respondan no solo cuando participan activamente en un delito, sino también cuando la falta de controles internos, políticas de seguridad o sistemas de prevención facilita la comisión de estas conductas delictivas.

---

6 Obtenido de: https://lpderecho.pe/ciberseguridad-vulneracion-datos-personales-entidades-financieras/, https://elcomercio.pe/noticias/filtracion-de-datos/?ref=ecr

Adicionalmente, la presente propuesta fortalece la prevención de riesgos sistémicos en entornos digitales, al establecer incentivos legales para que las empresas implementen estándares de seguridad ajustados a la naturaleza y volumen de los datos administrados. Ello contribuye a una cultura de gestión preventiva en materia de seguridad de la información, reduciendo la probabilidad de incidentes que deriven en perjuicios económicos, patrimoniales o reputacionales para miles de ciudadanos.

El artículo 2, inciso 6 de la Constitución Política del Perú reconoce el derecho fundamental de toda persona *"A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar."* Es decir, a la protección de sus datos personales y a la inviolabilidad de su vida privada. Este derecho, también denominado autodeterminación informativa, impone al Estado y a los actores privados el deber de asegurar mecanismos que garanticen el uso legítimo, seguro y controlado de los datos ciudadanos. No obstante, la Constitución carece de eficacia práctica si el marco penal no sanciona a quienes, pudiendo evitar un daño masivo a este derecho, lo permiten por omisión o desidia. Al establecer responsabilidad penal, este proyecto fortalece la tutela efectiva de un derecho constitucional que, en la sociedad digital, es equivalente al derecho a la identidad y a la dignidad personal.

El estándar internacional, especialmente en el ámbito de la OCDE y la Unión Europea mediante el Reglamento General de Protección de Datos (RGPD), impone obligaciones estrictas a las empresas para adoptar medidas técnicas, organizativas y jurídicas que aseguren la protección de datos y sancionen la negligencia directiva. El Perú, aspirante a la OCDE y con creciente digitalización del sector público y privado, no puede eludir este compromiso. Modernizar el régimen de delitos informáticos y responsabilidad empresarial no solo protege a los ciudadanos, sino que posiciona al país como un entorno confiable para la inversión digital, al demostrar que el uso de tecnologías se desarrolla bajo principios de seguridad, diligencia y protección de derechos fundamentales.

La presente iniciativa legislativa no pretende criminalizar la actividad empresarial ni obstaculizar el desarrollo tecnológico, sino delimitar con claridad la responsabilidad penal cuando la inacción o desidia permite la comisión de delitos informáticos o la exposición masiva de datos personales.

Otro aspecto fundamental que justifica este proyecto es la desvinculación actual entre el régimen de responsabilidad empresarial, en las normas vigentes y el catálogo de delitos informáticos. Ley que, en su redacción original, se limita a delitos como el cohecho, el lavado

de activos o la corrupción en el ámbito internacional, dejando fuera a los delitos informáticos pese al impacto que estos tienen sobre bienes jurídicos esenciales como la intimidad, el patrimonio y la seguridad digital. La incorporación de estos delitos permitirá que las empresas que toleren o no prevengan ataques informáticos respondan no sólo en el plano civil o administrativo, sino también en el marco del proceso penal, conforme a los estándares internacionales de responsabilidad corporativa.

La finalidad de esta iniciativa es generar una cultura de prevención y cumplimiento dentro de las personas jurídicas, incentivando la adopción de protocolos de ciberseguridad y mecanismos de gestión de riesgos digitales.

Desde el punto de vista de viabilidad, la presente propuesta se enmarca dentro de las competencias para legislar en materia de transparencia, participación ciudadana y control político, sin contravenir con el artículo 79 de la Constitución Política, que prohíbe la iniciativa de gasto.

La oportunidad de esta propuesta se encuentra estrechamente vinculada al contexto nacional de creciente preocupación ciudadana frente a las filtraciones de datos personales, los ciberataques y la evidente ausencia de responsabilidad efectiva por parte de las organizaciones que administran información sensible. En los últimos años, se ha generado una notoria desconfianza social hacia entidades públicas y privadas que, pese a tener amplias capacidades tecnológicas, no adoptan medidas mínimas de seguridad digital ni informan oportunamente sobre los incidentes que afectan a millones de usuarios. En un escenario donde los derechos digitales se han convertido en un componente esencial de la dignidad humana, resulta oportuno que el Estado fortalezca los mecanismos de prevención, sanción y control. Esta iniciativa legislativa busca, en tal sentido, cerrar una brecha normativa significativa y garantizar que la omisión o negligencia en materia de protección de datos no continúe generando escenarios de impunidad.

En una sociedad progresivamente digitalizada, la protección de los datos personales y la seguridad informática constituyen pilares esenciales del Estado de Derecho. La confianza ciudadana en el entorno digital depende de la capacidad del ordenamiento jurídico para sancionar. Este proyecto de ley aporta a la consolidación de un entorno digital seguro, responsable y transparente, alineado a los principios de dignidad humana, legalidad y responsabilidad empresarial. En consecuencia, su aprobación no sólo atiende una necesidad legislativa, sino también una exigencia ética frente a los desafíos de la era tecnológica.

La implementación de la presente ley permitirá optimizar los mecanismos de protección de datos y prevención de incidentes digitales, mediante la incorporación de obligaciones claras para las personas jurídicas, sin interferir en las funciones de los organismos de control existentes. Al establecer estándares mínimos de seguridad digital y responsabilidad penal, se promueve una cultura de prevención que puede reducir exponencialmente los riesgos de filtraciones masivas, fraudes electrónicos y vulneraciones a la intimidad. Asimismo, la presente genera beneficios cuantificables en términos de reducción de daños y protección de los derechos fundamentales, sin representar costo adicional para el Estado, pues se basa en la obligación de diligencia de las propias entidades que administran información personal.

En consecuencia, la importancia de esta iniciativa legislativa radica en la construcción de un marco normativo coherente, constitucional y sostenible que articule tres pilares fundamentales, la protección efectiva de los derechos digitales, la responsabilidad empresarial en la gestión de datos personales y la coordinación interinstitucional con las autoridades encargadas de la supervisión y persecución de delitos informáticos. Estos elementos, correctamente integrados, permitirán fortalecer la seguridad digital en el país, cerrar los vacíos legales que hoy favorecen la impunidad y promover una cultura de prevención y diligencia en el manejo de información sensible, en estricto respeto del principio de legalidad y del interés público.

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

La presente iniciativa legislativa tiene por objeto garantizar la protección efectiva de los datos personales de los ciudadanos, estableciendo un mejor marco de responsabilidad que obligue a las personas jurídicas a adoptar medidas adecuadas de ciberseguridad, prevención y respuesta ante incidentes informáticos. Su finalidad es proteger la integridad de los datos personales de los ciudadanos, promoviendo una cultura de responsabilidad y prevención en las personas jurídicas frente a los riesgos derivados de los delitos informáticos y las filtraciones de información.

Esta propuesta se integra de manera coherente al ordenamiento jurídico nacional, complementando las disposiciones vigentes en materia de delitos informáticos y protección de datos. De esta forma, contribuye a garantizar el ejercicio efectivo de derechos constitucionales, asegurando que la seguridad digital y la integridad de la información sean tratadas como obligaciones indelegables de quienes administran sistemas tecnológicos y bases de datos con acceso masivo.

Por ello, la vigencia de la presente norma no contraviene el principio de legalidad ni implica una reforma estructural del sistema penal, sino que establece herramientas complementarias destinadas a reforzar los estándares de responsabilidad. En consecuencia, promueve la coherencia del sistema jurídico y fortalece el Estado democrático de derecho, al reconocer que la protección de los datos personales y la prevención de delitos informáticos constituyen elementos esenciales para la confianza social en los entornos digitales.

III. ANÁLISIS COSTO BENEFICIO

La presente propuesta considera el siguiente cuadro de actores:

ACTORES	BENEFICIOS	COSTOS
Estado	• Fortalece la capacidad sancionadora frente a filtraciones y delitos informáticos. • Refuerza la protección de derechos digitales y la confianza en el sistema judicial. • No requiere creación de nuevas entidades ni presupuesto adicional.	No Aplica
Ciudadanía	• Mayor protección frente a uso indebido de datos personales. • Incremento de la confianza en plataformas digitales y servicios en línea.	No aplica
Personas Jurídicas	• Incentiva la implementación de mejores prácticas de ciberseguridad y gestión de riesgos. • Promueve confianza en clientes e inversionistas mediante cumplimiento digital responsable.	No Aplica

Fuente: Elaboración propia

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

La presente propuesta guarda relación con la Política de Estado expresado en el acuerdo nacional: IV Estado eficiente, transparente y descentralizado, punto 28 - Plena vigencia de la Constitución y de los derechos humanos y acceso a la justicia e independencia judicial:

> "Nos comprometemos a garantizar el acceso universal a la justicia, la promoción de la justicia de paz y la autonomía, independencia y el presupuesto del Poder Judicial así como regular la complementariedad entre éste y la justicia comunal. Asimismo, nos comprometemos a adoptar políticas que garanticen el goce y la vigencia de los derechos fundamentales establecidos en la Constitución y en los tratados internacionales sobre la materia.
>
> Con este objetivo el Estado: (a) promoverá la institucionalización de un Sistema de Administración de Justicia, respetando la independencia, la autonomía y el presupuesto del Poder Judicial, el Ministerio Público, el Consejo Nacional de la Magistratura y el Tribunal Constitucional, dentro de un proceso de modernización y descentralización del Estado al servicio del ciudadano; (b) promoverá la designación transparente de las autoridades judiciales, así como su valorización y permanente capacitación; (c) promoverá entre la justicia comunal y el Poder Judicial una relación que respete la interculturalidad y regulará las competencias, atribuciones y limitaciones de aquélla; (d) consolidará la regulación de la justicia de paz y la elección popular de los jueces de paz; (e) difundirá la conciliación, la mediación, el arbitraje y en general los mecanismos alternativos de resolución de conflictos; (f) adoptará medidas legales y administrativas para garantizar la vigencia y difusión de la Constitución, afianzará el respeto irrestricto de los derechos humanos y asegurará la sanción a los responsables de su violación; (g) establecerá mecanismos de vigilancia al correcto funcionamiento de la administración de justicia, al respeto de los derechos humanos, así como para la erradicación de la corrupción judicial en coordinación con la sociedad civil; (h) garantizará la cobertura nacional y el mejor funcionamiento de la Defensoría del Pueblo; e (i) fortalecerá las instancias de control interno de los órganos jurisdiccionales."

Asimismo, guarda relación con la Agenda Legislativa del Congreso de la República, aprobada mediante Resolución Legislativa del Congreso 006-2024-2025-CR, específicamente con la política de estado 28. Plena vigencia de la Constitución y de los Derechos Humanos y acceso a la justicia e independencia judicial, tema 97 sobre "Modernización y acceso en el sistema de justicia.".