C0075-2026-GG-ASBANC

San Borja, 22 de mayo de 2026

Señor Congresista
FLAVIO CRUZ MAMANI
Presidente de la Comisión de Justicia y Derechos Humanos
Congreso de la República
Presente.-

Asunto: Opinión Institucional de la Asociación de Bancos del Perú ("ASBANC") sobre el Proyecto de Ley que amplía la responsabilidad administrativa de las personas jurídicas frente a delitos informáticos y vulneraciones de datos personales.

Referencia: Proyecto de Ley N° 14045/2025-CR.

De nuestra mayor consideración:

Nos dirigimos a usted, en representación de la Asociación de Bancos del Perú ("ASBANC"), para saludarlo cordialmente y, a la vez, alcanzar nuestros comentarios respecto del proyecto de ley de la referencia, mediante el cual se propone incorporar los delitos informáticos y determinadas vulneraciones vinculadas a datos personales dentro del régimen de responsabilidad administrativa aplicable a las personas jurídicas.

Desde ASBANC compartimos plenamente la necesidad de fortalecer las capacidades institucionales para enfrentar los crecientes riesgos asociados a la cibercriminalidad y promover estándares elevados de seguridad digital y protección de datos. En un entorno caracterizado por amenazas tecnológicas cada vez más sofisticadas, resulta fundamental contar con un marco normativo moderno, predecible y técnicamente consistente.

En tal sentido, adjuntamos como **Anexo I** nuestras observaciones técnicas, con el propósito de contribuir al análisis integral de la iniciativa legislativa.

Sin perjuicio de lo anterior, consideramos importante poner a consideración de la Comisión los siguientes aspectos:

1. Necesidad de evitar superposición de regímenes sancionadores

El sistema financiero ya se encuentra sujeto a un marco regulatorio y sancionador altamente especializado en materia de gestión de riesgos operacionales, seguridad de la información, ciberseguridad y continuidad operativa, bajo supervisión de la Superintendencia de Banca, Seguros y AFP ("SBS").

En ese contexto, la incorporación de determinadas conductas al ámbito de responsabilidad administrativa regulado por la Ley N.° 30424 podría generar escenarios de superposición entre el régimen penal corporativo y el régimen administrativo sectorial ya existente, particularmente respecto de incumplimientos vinculados a deberes de control, supervisión o vigilancia.

Por ello, estimamos importante que la propuesta delimite adecuadamente los ámbitos de competencia y responsabilidad aplicables, a fin de preservar la coherencia del sistema sancionador y evitar eventuales duplicidades regulatorias respecto de una misma conducta.

2. Necesidad de fortalecer la eficacia de los modelos de prevención

La propuesta busca incentivar la inversión en mecanismos de prevención y cumplimiento mediante la implementación de modelos de prevención corporativa. No obstante, advertimos que el marco vigente establece limitaciones para la aplicación de eximentes de responsabilidad cuando las conductas involucren a directivos o personas con capacidad de decisión o control.

En sectores altamente regulados como el financiero, las decisiones vinculadas a infraestructura tecnológica, gestión de riesgos digitales y ciberseguridad forman parte de la esfera estratégica del Directorio y de la Alta Gerencia. En consecuencia, resulta importante evaluar si el diseño actual del régimen de eximentes permite generar incentivos reales y efectivos para el fortalecimiento de los sistemas de cumplimiento y prevención corporativa.

Consideramos que una adecuada revisión de este aspecto contribuiría a alinear los incentivos regulatorios con el objetivo de promover mayores inversiones en ciberseguridad y gestión preventiva de riesgos.

3. Importancia de preservar la especialización supervisora

Asimismo, estimamos relevante que la evaluación de los modelos de prevención aplicables al sistema financiero considere las competencias técnicas y regulatorias de la SBS como autoridad especializada en supervisión bancaria, gestión de riesgos y seguridad operativa.

La participación de entidades supervisoras especializadas resulta especialmente importante en la evaluación de riesgos tecnológicos y financieros complejos, a fin de evitar posibles divergencias de criterios regulatorios y preservar la predictibilidad que requiere el funcionamiento del sistema financiero.

Por lo expuesto, solicitamos respetuosamente que la propuesta normativa continúe siendo evaluada en un espacio de análisis técnico especializado, que permita fortalecer la lucha contra la cibercriminalidad y la protección de datos personales sin generar superposición de competencias ni afectar la coherencia regulatoria aplicable a sectores altamente supervisados.

Asimismo, consideramos valioso promover espacios de coordinación técnica con participación de las autoridades competentes y de los sectores involucrados, a efectos de construir una regulación equilibrada, eficaz y técnicamente viable.

Sin otro particular, agradecemos de antemano la atención brindada a la presente y quedamos a su disposición para ampliar los argumentos técnicos expuestos.

Muy atentamente,

MARTIN NARANJO LANDERER
Presidente Consejo Directivo
ASOCIACIÓN DE BANCOS DEL PERÚ

Se adjunta:

- Anexo I: Comentarios al Proyecto de Ley N° 14045/2025-CR

Asociación de Bancos del Perú

ANEXO I

COMENTARIOS AL PROYECTO DE LEY N° 14045/2025-CR

TEMA	COMENTARIO
Duplicidad regulatoria y riesgo de vulneración del principio *non bis in ídem*	Consideramos que la propuesta omite que la protección de datos personales ya cuenta con un régimen administrativo especializado, regulado por Ley No. 29733 – Ley de Protección de Datos Personales, y su Reglamento. La supervisión y potestad sancionadora en el tratamiento de datos personales recaen exclusivamente en la Autoridad Nacional de Protección de Datos Personales ("ANPDP") por lo que la incorporación de delitos informáticos al ámbito de la Ley No. 30424 podría generar superposición de regímenes sancionadores, pudiendo derivar en: *(i)* doble persecución por los mismos hechos; y, *(ii)* vulneración del principio constitucional *non bis in ídem*.
Optimización de facultades de supervisión en el sector financiero y salvaguarda del principio *non bis in ídem*	En esa misma línea, sugerimos evaluar detenidamente el riesgo de doble persecución para las entidades del sector financiero, cuyas operaciones se ejecutan en un marco administrativo sancionador y de supervisión sumamente exhaustivo a cargo de la SBS. Habilitar que las incidencias en seguridad de la información sean procesadas penalmente bajo el esquema de responsabilidad corporativa (Ley No. 30424) podría derivar en una doble sanción por una misma conducta (el deber de vigilancia), bajo fundamentos técnicos idénticos. A fin de mantener el equilibrio del *ius puniendi* estatal y evitar conflictos con las potestades de la Ley No. 30096, consideramos recomendable delimitar las competencias punitivas resguardando la especialización sectorial ya existente.

Falta de conexión entre los delitos informáticos propuestos y la lógica de la responsabilidad corporativa	La iniciativa incorpora un catálogo amplio y heterogéneo de delitos informáticos, sin distinguir entre: *(i)* conductas con relevancia corporativa sustancial; y, *(ii)* aquellas que carecen de nexo causal con un beneficio empresarial. Esta omisión resultaría incompatible con los criterios de imputación previstos en la Ley No. 30424, que se basa exclusivamente en la obtención de beneficios empresariales o la comisión del delito en nombre o por cuenta de la persona jurídica.
Desnaturalización del modelo de prevención previsto en la Ley No. 30424	La iniciativa desvirtúa el modelo de prevención al exigir la adopción obligatoria de medidas de ciberseguridad y de seguridad de información de manera obligatoria; sin embargo, el sistema actual, establece que el modelo de prevención es: *i)* Un mecanismo voluntario, *ii)* Con efectos eximentes o atenuantes, *iii)* Basado en un enfoque de gestión de riesgos; y, *iv)* Desarrollado conforme a su Reglamento vigente. Por lo tanto, imponer un modelo obligatorio desnaturaliza el régimen y altera su diseño original. En tal sentido, consideramos oportuno analizar la articulación de la propuesta con el D.S. No. 002-2025-JUS (artículo 31-A del Reglamento de la Ley No. 30424,), a fin de no restarle eficacia al Modelo de Prevención como incentivo clave para la ciberseguridad. Dado que el proyecto extiende la responsabilidad a los delitos informáticos de la Ley No. 30096, es necesario advertir que, en el sector financiero, las decisiones sobre infraestructura digital y riesgos tecnológicos son de naturaleza estratégica y recaen formalmente sobre el Directorio y la Alta Gerencia (quienes poseen "capacidad de control"). Al establecer la normativa reglamentaria que el eximente queda sin efecto si el hecho es cometido por personas con capacidad de control, el modelo de prevención devendría en inaplicable para estos casos,

	reduciendo el beneficio a una mitigación de multa. Ante ello, proponemos revisar esta consistencia para que las empresas mantengan un incentivo real y predecible en la adopción de altos estándares corporativos.
Omisión sobre la coexistencia con las consecuencias accesorias del Código Penal	El Proyecto no considera la concurrencia entre las sanciones administrativas previstas en la Ley No. 30424; y, las consecuencias accesorias del artículo 105 del Código Penal, comprometiendo la coherencia del ordenamiento jurídico. Como resultado, se genera: *(i)* incertidumbre jurídica; *ii)* riesgos de sanciones acumulativas excesivas, *iii)* afectación del principio de proporcionalidad; y, *iv)* desnaturalización del sistema de responsabilidad penal empresarial.
Alineamiento y predictibilidad en la validación técnica de modelos	Con el propósito de asegurar la predictibilidad del sistema y la coherencia técnica, respetuosamente sugerimos que la validación de los modelos de prevención en el sector bancario se mantenga bajo la esfera de su supervisor natural, la SBS. Delegar dicha atribución a la SMV para riesgos tecnológicos complejos y específicos del entorno bancario podría generar una dispersión de criterios interpretativos. Creemos que canalizar estas evaluaciones a través de la SBS —aprovechando su alta especialización e historial técnico— robustecerá la solidez del ecosistema regulatorio sin generar duplicidades institucionales.
Plazo insuficiente para adecuar el Reglamento	El plazo de 90 días propuesto para la adecuación reglamentaria resulta insuficiente ante la complejidad del ecosistema normativo actual. Cabe precisar que durante el año 2025 se aprobaron modificaciones sustanciales a la Ley No. 30424 y entró en vigor el nuevo Reglamento de la Ley de Protección de Datos Personales. En este contexto, resulta necesario contar con un análisis de impacto regulatorio que asegure la armonización de estas reglas. Una implementación apresurada, afectaría la eficacia de los modelos de prevención y la seguridad jurídica de los sujetos obligados.