MINUTA TÉCNICA

Dirigido a: Comisión Asesora Ministerial para la Implementación de la Ley N° 21.719 que modifica la Ley N° 19.628.
De: Asociación Chilena de Ética y Compliance (ACEC)
Fecha: 23 de octubre 2025
Asunto: Interés legítimo y uso de bases de datos para fines de prevención del delito y fraude

1. Introducción.

La presente minuta ha sido elaborada por la Asociación Chilena de Ética y Compliance (ACEC), en el marco del trabajo técnico que desarrolla la Comisión Asesora Ministerial para la Implementación de la Ley Sobre Protección de Datos Personales, convocada por el Ministerio Secretaría General de la Presidencia (SEGPRES) mediante Decreto Exento N° 12, de 17 de junio de 2025.

Su objetivo es aportar elementos de análisis y propuestas regulatorias sobre la aplicación del interés legítimo como base de licitud para el tratamiento de datos personales con fines de prevención del delito y el fraude, considerando las tensiones entre seguridad, proporcionalidad y derechos fundamentales.

El reconocimiento de esta base de licitud representa una novedad sustantiva en el ordenamiento chileno y exige un desarrollo reglamentario robusto por parte de la futura Agencia de Protección de Datos Personales (APDP). En este contexto, ACEC propone en este documento un marco interpretativo, apoyado en la experiencia comparada, orientado a garantizar un uso legítimo, documentado y verificable del interés legítimo en contextos de alto impacto social.

2. Contexto normativo: evolución del fundamento y uso de fuentes de acceso público.

Históricamente, la Ley N° 19.628 fundó la licitud del tratamiento de datos personales en tres supuestos: (i) el consentimiento del titular, (ii) una autorización legal expresa, y (iii) que los datos provinieran de fuentes accesibles al público.

Sin embargo, esta tercera hipótesis, referida al uso de fuentes accesibles al público, fue configurada con una amplitud tal que en la práctica se entendió como una habilitación general para el tratamiento de datos personales disponibles públicamente. Esta interpretación permitió y legitimó, durante años, la existencia de herramientas y plataformas de indexación masiva, como los denominados *rutificadores* o sitios afines, que operaban sobre la base del acceso público a la información, sin requerir consentimiento del titular.

Ahora bien, desde una lectura más precisa, el artículo 4° debía entenderse como compuesto por hipótesis diferenciadas y autónomas de licitud, cada una con un alcance y finalidad propios: (i) la relativa a los datos provenientes de fuentes de acceso público (FAP); (ii) otra referida a los datos de carácter económico, financiero, bancario o comercial; (iii) una tercera vinculada a listados limitados de información identificadora o profesional (por ejemplo, profesión, títulos educativos o dirección); y (iv) aquella que habilitaba tratamientos con fines

de comunicación o comercialización directa. Cada una debía aplicarse de manera separada, sin que la amplitud reconocida a las FAP se extendiera automáticamente a las demás categorías.

Con el tiempo, y especialmente con la creciente exposición de bases de datos en línea, la práctica extendió este tipo de tratamientos a nuevos contextos, como verificaciones de antecedentes judiciales, laborales o reputacionales, lo que desdibujó la frontera entre el mero acceso a información pública y su tratamiento legítimo. Ello generó tratamientos masivos basados en la existencia de las fuentes públicas como bases de licitud directa, la cual se encuentra expresamente exceptuadas de los principios de finalidad, confidencialidad y de los derechos de protección de datos.

El reconocimiento del interés legítimo en la nueva Ley N° 19.628 corrige esta asimetría. El legislador abandona la noción estática de "fuente pública" y exige, en cambio, que el responsable demuestre un interés lícito, actual y ponderado, compatible con los derechos fundamentales del titular. Así, el foco ya no está en la fuente del dato como base de licitud per se, sino en la necesidad y proporcionalidad del tratamiento.

No obstante, la ley no detalla el método para realizar esa ponderación ni el estándar probatorio exigido, por lo que la futura APDP deberá desarrollar criterios interpretativos, por ejemplo, a través de una Instrucción General o Guía sobre Interés Legítimo, que doten de certeza a los responsables y garanticen la protección efectiva de los titulares.

3. Experiencia comparada y doctrina relevante.

3.1. Unión Europea.

El Dictamen 06/2014 (WP29) sobre el artículo 7(f) de la Directiva 95/46/CE[1] sentó las bases del concepto de interés legítimo. Este documento identificó tres elementos esenciales:

1. El interés debe ser real, actual y lícito (no meramente especulativo).
2. El tratamiento debe ser necesario para satisfacer ese interés.
3. Debe realizarse una prueba de ponderación entre los derechos del titular y los fines del responsable.

El WP29 reconoció expresamente la prevención del fraude, el uso indebido de servicios o el blanqueo de dinero como ejemplos de intereses legítimos admisibles, destacando que su validez depende de una evaluación caso a caso. Asimismo, propuso medidas de mitigación, como la anonimización, la reducción de datos y la información reforzada al titular, que pueden "inclinar la balanza" a favor del responsable siempre que se garanticen los derechos fundamentales.

A partir de estos lineamientos, el European Data Protection Board (EDPB) en sus Guidelines 1/2024[2] sobre el artículo 6(1)(f) del RGPD actualiza y consolida los criterios, estableciendo

[1] Disponible en línea - https://www.aepd.es/documento/wp217_es_interes_legitimo.pdf
[2] Disponible en línea - https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf

requisitos más estrictos y una metodología uniforme aplicable a todos los Estados miembros.

3.2. Fraude y delitos: reconocimiento y límites según el EDPB.

El EDPB reafirma que la prevención del fraude constituye un interés legítimo reconocido por el Considerando 47 del RGPD, pero su aplicación no es automática.
El tratamiento sólo será lícito si es:

- estrictamente necesario para prevenir el fraude;
- proporcional y limitado a los datos indispensables;
- y se basa en una finalidad específica y documentada, no en referencias genéricas como "combate al fraude" o "seguridad corporativa".

El Comité define el fraude como todo acto intencionado o engañoso para obtener una ventaja indebida o ilícita, y aclara que la detección puede incluirse dentro de la prevención cuando sea el único medio razonable para evitar su reiteración.

Asimismo, el EDPB exige aplicar los principios del artículo 5 del RGPD, es decir, minimización, limitación de conservación y transparencia. Precisa que únicamente los fraudes de entidad sustancial, es decir, aquellos que implican un perjuicio económico relevante, un riesgo operativo significativo o una afectación grave a derechos de terceros, pueden justificar una injerencia en los derechos del titular; en cambio, las verificaciones genéricas o frente a riesgos hipotéticos no superan el test de ponderación y deberán resolverse en favor del interesado.

3.3. Metodología de ponderación ("balancing test").

Tanto el WP29 como el EDPB coinciden en una estructura analítica en tres fases:

1. Identificación del interés legítimo: debe ser lícito, específico y actual.
2. Evaluación de necesidad: el tratamiento debe ser indispensable para alcanzar la finalidad, sin medios menos intrusivos disponibles.
3. Ponderación de derechos y libertades: exige valorar la naturaleza de los datos, el contexto del tratamiento, las consecuencias posibles para los titulares y sus expectativas razonables.

Las expectativas del titular, según el EDPB, dependen de su relación con el responsable, la transparencia del aviso previo, el contexto del servicio y factores personales (edad, rol, exposición pública).

El responsable puede adoptar medidas de mitigación que inclinen la balanza a su favor, como:

- anonimización o seudonimización de datos,
- separación funcional,
- transparencia reforzada,
- mecanismos de objeción accesibles,

- ejercicio ampliado de derechos incluso más allá de las obligaciones legales.

Estas medidas deben documentarse y justificar una nueva ponderación posterior a su implementación.

3.4. Relevancia para el contexto chileno.

Los criterios del WP29 y del EDPB ofrecen un marco técnico útil y adaptable al contexto nacional, pero su aplicación en Chile debe considerar las particularidades del entorno regulatorio y operativo local, caracterizado por una menor madurez institucional en materia de protección de datos, una alta exposición al fraude, y una fuerte dependencia de fuentes de información públicas y sectoriales para cumplir con obligaciones legales de prevención y control.

En este sentido, la aplicación del interés legítimo en materia de prevención del fraude y del delito debería mantener los principios sustantivos del modelo europeo, necesidad, proporcionalidad y rendición de cuentas, pero adaptarse a la realidad chilena mediante criterios graduales, coordinados con las normas sectoriales y operativamente viables.

En Chile, distintos cuerpos normativos ya imponen obligaciones de tratamiento de datos personales, vinculadas a la verificación de antecedentes, el monitoreo de operaciones y la prevención del fraude, entre ellas:

- La Ley N° 19.913, que crea la Unidad de Análisis Financiero (UAF) y establece deberes de diligencia debida, monitoreo continuo y reporte de operaciones sospechosas por parte de entidades financieras, notarios, corredores y otras instituciones obligadas.
- La Ley N° 21.180 sobre Transformación Digital del Estado, que habilita el uso de servicios de identidad digital y el intercambio de información entre organismos públicos para verificar autenticidad o prevenir suplantaciones.
- Las normas de carácter general (NCG) de la Comisión para el Mercado Financiero (CMF), que ordenan mantener sistemas de gestión de riesgo operacional y de fraude, incluyendo la recopilación y análisis de datos transaccionales.
- Los protocolos de contratación pública (ChileCompra) en el sector público.
- Las normas de Prevención de Lavado de Activos y Financiamiento del Terrorismo, que obligan a realizar verificaciones de antecedentes en registros judiciales, tributarios o comerciales.

En este contexto, el uso de fuentes de acceso público o institucional (por ejemplo, el Servicio de Impuestos Internos, el Registro Civil, la CMF, el Boletín Comercial o el Poder Judicial) no constituirán por sí mismo una base de licitud, pero puede fundamentar el interés legítimo cuando el tratamiento persigue finalidades preventivas legítimas y se aplica con proporcionalidad.

El foco, por tanto, no debe estar en el carácter público o privado de la fuente, sino en la necesidad, finalidad y garantías asociadas al tratamiento. A partir del diagnóstico y las

experiencias comparadas, se proponen las siguientes líneas de acción para orientar la implementación chilena:

- Documentar una Evaluación de Interés Legítimo (LIA) que incorpore la metodología tripartita (interés, necesidad, ponderación), pero permitiendo formatos simplificados o sectoriales para tratamientos rutinarios de bajo riesgo o bajo volumen de datos (por ejemplo, controles de identidad en plataformas digitales o validaciones en procesos de pago).

- Identificar y describir el tipo de fraude o riesgo operacional a prevenir, delimitando las categorías de datos tratadas y las fuentes utilizadas.
  En muchos casos, estas fuentes provendrán de registros públicos o de acceso institucional obligatorio, como:

  - El Servicio de Registro Civil e Identificación, para verificar identidad y estado civil.

  - El Servicio de Impuestos Internos (SII), para verificar actividad económica o situación tributaria.

  - La Comisión para el Mercado Financiero (CMF), para revisar antecedentes financieros o sanciones administrativas.

  - La Dirección del Trabajo y la Superintendencia de Pensiones, en contextos laborales o previsionales.

  - El Poder Judicial y el Diario Oficial, para antecedentes judiciales o publicaciones obligatorias.

En estos casos, el interés legítimo se sustenta en la autorización u obligación legal, y complementa y ordena la forma en que estos datos son tratados, garantizando que se usen exclusivamente para fines específicos, necesarios y proporcionales.

- Aplicar criterios de proporcionalidad y expectativas razonables, de este modo, las organizaciones podrán demostrar que el tratamiento de datos personales no responde a un interés genérico, sino a una obligación concreta de cumplimiento normativo, contractual o regulatorio, y que se limita a lo estrictamente necesario para prevenir infracciones o fraudes. Por ejemplo, los bancos, intermediarios financieros y entidades sujetas a la UAF están legalmente obligados a monitorear operaciones sospechosas, verificar identidades y prevenir el lavado de activos, conforme a la Ley N° 19.913 y a las normas de carácter general de la CMF.

  Ese marco regulatorio constituye una base objetiva y verificable de interés legítimo, en la medida en que el tratamiento se oriente a cumplir dichos deberes de control y se realice bajo principios de proporcionalidad y rendición de cuentas. Idealmente, esta lógica debería articularse con los futuros Modelos de Prevención de Infracciones (MPI) en materia de protección de datos personales, de modo que los tratamientos de datos con fines de prevención del fraude conversen normativamente con los mecanismos de compliance penal. Así, se evitaría la duplicación de evaluaciones penales, financieras y de protección de datos, y se promovería una gestión integral del

riesgo, donde el análisis de interés legítimo (LIA) se integre naturalmente al ecosistema de cumplimiento corporativo.

- Adoptar medidas de mitigación graduadas según el nivel de riesgo del tratamiento.

  Esto supone que las salvaguardas aplicadas deben ser proporcionales al tipo de tratamiento, al volumen de datos y al nivel de riesgo identificado, de manera que el cumplimiento sea exigente pero también operativamente sostenible.

  En este marco, se recomienda priorizar controles razonables y graduales, tales como:

  i. Seguridad lógica y control de accesos, para restringir el uso de la información solo al personal autorizado.
  ii. Trazabilidad y registro de actividades, que permitan auditar quién accede, modifica o comparte datos.
  iii. Seudonimización o anonimización parcial, cuando la finalidad de prevención o monitoreo no requiera identificar plenamente al titular.
  iv. Revisión o supervisión humana en decisiones automatizadas que impliquen bloqueo de operaciones, evaluación de riesgo o exclusión.
  v. Auditorías selectivas o revisiones periódicas, en lugar de fiscalizaciones continuas o sistemas tecnológicos de alto costo.

  Este enfoque permite que las grandes entidades sujetas a fiscalización apliquen medidas técnicas avanzadas, mientras que las PYMEs o instituciones con menor capacidad tecnológica puedan cumplir mediante controles organizativos equivalentes, sin incurrir en cargas desproporcionadas.

  Asimismo, estas medidas deberían integrarse de manera coherente con los Modelos de Prevención de Delitos (MPD) y los futuros Modelos de Prevención de Infracciones en materia de datos personales, garantizando una coherencia entre los diferentes controles.

  En definitiva, la proporcionalidad no debe entenderse como una flexibilización del estándar de protección, sino como un principio de adecuación que permite cumplir con eficacia y realismo, priorizando los riesgos más relevantes sin desincentivar la adopción de medidas preventivas.

- Coordinar con la futura Agencia de Protección de Datos Personales (APDP) y con las autoridades sectoriales el desarrollo de un "test nacional de interés legítimo" en estas materias, aplicable de forma proporcional y diferenciada por sectores. Este instrumento debería servir como marco común de interpretación y rendición de cuentas, armonizando las obligaciones de tratamiento de datos derivadas de la nueva Ley N° 19.628 con los deberes regulatorios ya existentes en otras materias.

  El test nacional debiera incluir orientaciones claras y verificables sobre:

- Cómo documentar la ponderación entre el interés del responsable y los derechos del titular, asegurando que las justificaciones se integren a los sistemas de gestión de cumplimiento ya exigidos por otras autoridades.
- Qué fuentes de información pueden considerarse institucionales, públicas o legítimamente accesibles, estableciendo criterios uniformes que eviten interpretaciones dispares entre sectores y otorguen certeza jurídica a los responsables.
- Qué garantías mínimas deben acompañar los tratamientos para considerarse razonables, incluyendo medidas técnicas, organizativas y de transparencia proporcionales al riesgo y al tipo de dato tratado.

La adopción de este test coordinado y sectorizado permitiría avanzar hacia un modelo de regulación convergente, donde la protección de datos personales y las exigencias de compliance dialoguen dentro de un mismo marco de responsabilidad y proporcionalidad.

4. Propuestas de líneas de trabajo para la Comisión

A partir del análisis doctrinal, la experiencia comparada y el marco regulatorio nacional, se proponen las siguientes líneas de acción para orientar la implementación del interés legítimo en Chile, con especial foco en su uso para la prevención del fraude y del delito.

4.1. Definición normativa e interpretación coordinada

- Incorporar en la reglamentación o en las Instrucciones Generales de la APDP ejemplos explícitos y graduados de cuándo la prevención del fraude o delito puede fundarse en el interés legítimo, según el tipo de entidad y el nivel de riesgo.
- Adoptar un "Test Nacional de Interés Legítimo" en estas materias coordinado entre la APDP y las autoridades sectoriales con criterios proporcionales por industria. Este test debería contemplar orientaciones prácticas sobre:
    1. Cómo documentar la ponderación entre el interés del responsable y los derechos del titular.
    2. Qué fuentes pueden considerarse institucionales, públicas o legítimamente accesibles.
    3. Qué garantías mínimas deben acompañar los tratamientos para considerarse razonables.
- Emitir guías técnicas sectoriales o interinstitucionales que armonicen la protección de datos con las obligaciones de prevención, asegurando coherencia entre los marcos normativos.

4.2. Evaluaciones de impacto y documentación de accountability

- Exigir una LIA documentada como requisito previo a todo tratamiento fundado en interés legítimo que involucre un riesgo significativo o el uso de fuentes externas.

- Requerir una Evaluación de Impacto en Protección de Datos (DPIA) en tratamientos de alto riesgo o que involucren el uso de tecnologías potencialmente intrusivas o la generación de perfiles, integrando la LIA como anexo o módulo de esa evaluación.
- Incorporar el principio de proporcionalidad documental, permitiendo plantillas y formatos sectoriales simplificados para PYMEs o entidades de bajo impacto.

4.3. Transparencia y derechos de los titulares

- Exigir transparencia reforzada, informando la finalidad, base jurídica y fuentes utilizadas en tratamientos antifraude.
- Permitir avisos simplificados o modulares adaptados al contexto operativo.
- Garantizar el derecho de oposición y revisión humana, reconociendo que, en ciertos casos, por ejemplo, investigaciones de fraude, dicho derecho puede suspenderse temporalmente para no frustrar la finalidad preventiva, siempre bajo registro y revisión posterior.

4.4. Retención, revisión y supresión

- Establecer plazos de conservación diferenciados por tipo de riesgo o sector, permitiendo retención extendida solo cuando exista un deber legal (p. ej. operaciones sujetas a investigación UAF o causas judiciales).
- Requerir revisiones periódicas de eficacia y la anonimización o supresión automática de datos cuando cesa la finalidad preventiva.
- Prohibir la creación de listas negras o perfiles permanentes no regulados, salvo que se sustenten en base legal expresa o en decisiones fundadas y revisables.

4.5. Rol de los encargados especializados en verificación y compliance

En el ecosistema de prevención del fraude y cumplimiento normativo, diversas organizaciones recurren a prestadores externos especializados en verificación de antecedentes, debida diligencia y gestión de riesgos reputacionales. Conforme al artículo 15 bis de la Ley N° 19.628 (modificada por la Ley N° 21.719), estos prestadores actúan como encargados del tratamiento, en tanto traten datos personales por cuenta y bajo instrucciones del responsable, sin determinar autónomamente los fines ni los medios esenciales del tratamiento.

Su legitimación deriva, por tanto, del fundamento jurídico que invoque el responsable del tratamiento (habitualmente el interés legítimo junto al cumplimiento de una obligación legal), mientras que el encargado debe asegurar el cumplimiento operativo, técnico y documental de dichas instrucciones.

a. Contrato de encargo y delimitación de funciones

De acuerdo con las orientaciones de la ICO sobre el interés legítimo (*Legitimate Interests – A Guide for Organisations*, 2023)[3] y con la Guía sobre las medidas de intercambio de información en la *Economic Crime and Corporate Transparency Act 2023* (UK Home Office & ICO, 2024)[4], los encargados o intermediarios que participen en procesos de intercambio de datos para la prevención de delitos económicos deben garantizar, entre otras medidas:

1. que el tratamiento se limite estrictamente a los fines instruidos por el responsable;
2. que la información se comparta únicamente entre entidades legitimadas y con fines de prevención o detección de delitos;
3. que se mantengan registros de auditoría sobre los datos compartidos y las decisiones adoptadas; y
4. que existan protocolos de seguridad y gobernanza transparentes, en cumplimiento de la norma.

En el contexto chileno, los proveedores de servicios especializados en verificación, prevención de delitos y compliance deben ser considerados, en principio, encargados del tratamiento conforme al artículo 15 bis de la nueva Ley N.º 19.628, en la medida que procesen datos personales por cuenta e instrucciones del responsable, sin definir por sí mismos la finalidad ni los medios esenciales del tratamiento.

No obstante, siguiendo la doctrina comparada, cuando estos prestadores adquieren autonomía funcional, por ejemplo, determinan sus propios criterios de análisis, conservan bases de antecedentes o elaboran perfiles reutilizables para distintos clientes, deben ser calificados como responsables del tratamiento respecto de esas operaciones, con todas las obligaciones que ello implica: base de licitud propia, deber de transparencia directa frente a los titulares, registro de actividades y cumplimiento autónomo.

En consecuencia, la futura Agencia de Protección de Datos Personales debiera promover un enfoque de "encargados reforzados", imponiendo a este tipo de proveedores obligaciones documentales, de cooperación y auditoría equivalentes a las del responsable, a fin de asegurar la trazabilidad, la proporcionalidad y la rendición de cuentas (*accountability*) en los tratamientos de datos vinculados a fines de prevención del delito o de cumplimiento normativo.

5. Conclusiones y recomendaciones a la Comisión

La incorporación del interés legítimo como base de tratamiento de datos personales ofrece una oportunidad estratégica para armonizar la prevención del fraude con la protección de los derechos fundamentales, pero su éxito dependerá de una implementación flexible, documentada y coordinada entre sectores.

Se recomienda a la Comisión Asesora Ministerial promover que la futura reglamentación y las directrices de la APDP:

[3] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/
[4] https://www.gov.uk/government/publications/information-sharing-measures-in-the-economic-crime-and-corporate-transparency-act/guidance-on-the-information-sharing-measures-in-the-economic-crime-and-corporate-transparency-act-2023

1. Reconocimiento expreso del interés legítimo en la prevención del delito.

Establecer de forma explícita que la prevención, detección e investigación del fraude, lavado de activos o infracciones normativas puede constituir un interés legítimo del responsable, siempre que se acredite su necesidad, proporcionalidad y ponderación adecuada frente a los derechos de los titulares.

2. Creación de un Test Nacional de Interés Legítimo (LIA) para prevención del delito y fraude.

Desarrollar un marco metodológico uniforme para este tipo de tratamientos que permita documentar la evaluación del interés legítimo. El test debería incluir criterios sectoriales definidos junto a autoridades especializadas en estas materias.

3. Integración de la DPIA en los tratamientos de mayor riesgo o impacto.

Promover que los tratamientos de datos personales realizados con fines de prevención del fraude, detección de ilícitos o verificación de cumplimiento normativo, cuando impliquen alto riesgo para los derechos de los titulares, por su volumen, sensibilidad, uso de fuentes externas o decisiones automatizadas, sean objeto de una Evaluación de Impacto en Protección de Datos (DPIA).

4. Transparencia graduada y salvaguardas proporcionales.

Implementar mecanismos de transparencia adaptados al riesgo y contexto operativo (por ejemplo, avisos simplificados en verificaciones antifraude), acompañados de medidas de mitigación razonables y vías efectivas para el ejercicio de derechos, especialmente en tratamientos automatizados.

5. Supervisión basada en riesgo y mejora continua.

Adoptar un enfoque de fiscalización centrado en el nivel de riesgo y la madurez de los sistemas de cumplimiento, evitando cargas desproporcionadas para PYMEs y promoviendo la mejora progresiva de los estándares de protección.

6. Determinación clara del rol de los proveedores especializados.

Reconocer que los proveedores de servicios de verificación, due diligence y compliance actúan como encargados del tratamiento cuando procesan datos bajo las instrucciones del responsable. Solo se considerarán responsables independientes cuando reutilicen datos, definan sus propios fines o mantengan bases de antecedentes aplicables a múltiples clientes. Frente a estos reconocer el interés legitimo de un tercero como suficiente base de licitud.

7. Contratos de encargo con cláusulas mínimas obligatorias.

Establecer requisitos contractuales mínimos para los encargados, por ejemplo, finalidad específica, medidas de seguridad, trazabilidad, confidencialidad, auditoría y supervisión por parte del responsable. Se recomienda incorporar cláusulas de no reutilización de datos y cooperación ante fiscalizaciones.

8. Rendición de cuentas y cooperación permanente.

Imponer a los encargados especializados la obligación de mantener registros de accesos y operaciones, documentar las medidas de seguridad aplicadas, notificar incidentes, y colaborar en auditorías o requerimientos de la APDP, de forma análoga a los mecanismos de accountability del responsable.

9. Fomento de certificaciones y estándares sectoriales.

Promover mecanismos voluntarios de certificación y acreditación sectorial para prestadores de servicios de compliance y prevención, basados en las buenas prácticas internacionales, con el fin de fortalecer la confianza, transparencia y supervisión transversal del ecosistema.