Datos y Ciberseguridad: Desafíos Regulatorios

InsurteChile®

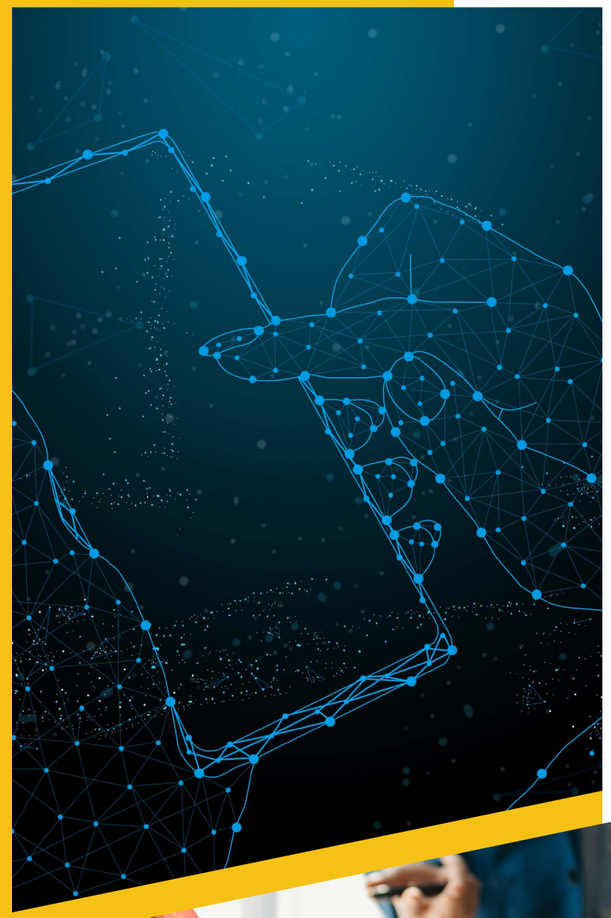
Co-Creando la Protección del Futuro

ANINAT ABOGADOS Kennedys Atipicus

Trabajo colaborativo entre miembros del squad técnico y el valoso aporte del equipo

2025

Indice



Introducción

En abril de 2025, InsurteChile organizó un workshop entre sus asociados, a fin de abordar cuatro grandes ejes temáticos en torno a las preocupaciones y desafíos actuales de la industria en el contexto de implementación de la Ley N° 21.719, que modificó sustancialmente la ley N° 19.628 sobre datos personales (“Nueva LPDP”), y su relación con otros marcos normativos recientes. El encuentro convocó a representantes de compañías de seguros, corredores e insurtechs, generando un valioso espacio de intercambio y reflexión técnica sobre las condiciones habilitantes para una gobernanza normativa eficaz.

Se organizaron cuatro grandes mesas de trabajo, que abordaron diversas temáticas, cuyas conclusiones se desarrollan en este documento:
En la primera mesa de trabajo se destacó la urgente necesidad de contar con parámetros claros por parte de la autoridad, en coordinación con los actores de la industria, de manera que se logre concordar la reciente reforma en materia de protección de datos con otras normativas que inciden en la industria, como la Ley N° 21.521 (“Ley Fintech”), la Ley Marco de Ciberseguridad (N° 21.663), las

disposiciones de protección al consumidor y los cuerpos normativos relativos a salud. En particular, se identificó como prioridad la clarificación de qué obligaciones resultan prevalentes ante posibles superposiciones regulatorias, así como la delimitación de competencias entre las distintas autoridades fiscalizadoras.
Se coincidió además en que el diseño de tales criterios debiera priorizar un enfoque práctico que anticipe criterios interpretativos y reduzca la carga administrativa asociada a exigencias duplicadas. Asimismo, se propuso institucionalizar mesas de trabajo preventivas que permitan resolver controversias regulatorias en forma anticipada y promover una implementación progresiva y armónica de las nuevas normas.

La segunda mesa se centró en los desafíos prácticos derivados de distribución de seguros en un modelo intermediado, sea tradicional o masivo, derivados de la asignación bajo los criterios de la ley de roles para los distintos intervinientes respecto del tratamiento de datos, roles que derivan de distintos instrumentos y posiciones y que pueden variar en una misma relación, debiendo además distinguirse la asignación estos roles según la ley con la asignación que hacen las partes en los distintos contratos. Todo lo anterior representa un desafío fundamental en la industria pues obliga a redefinir las actuales responsabilidades y estructuras de negocio.

Asimismo, se debatió sobre los criterios aplicables a la utilización de bases de datos como el Sistema de Información de Siniestros de Seguros Generales (“SISGEN”), considerando los principios de interés legítimo y minimización. Se subrayó la importancia de actualizar los contratos de distribución para reflejar correctamente estos roles, así como la necesidad de reforzar las políticas internas de acceso y uso de información, especialmente en lo relativo a la movilidad de los equipos comerciales y la responsabilidad empresarial en el marco de la Ley de Delitos Económicos. La tercera mesa giró en torno a los retos y La tercera mesa giró en torno a los retos y oportunidades que representa el derecho a la portabilidad de datos personales para el sector asegurador. Se abordó el impacto que podría tener esta figura en la competencia y la innovación, especialmente si se logra implementar un protocolo técnico común que defina formatos interoperables, canales seguros de transmisión y salvaguardas tanto contractuales como tecnológicas.
Se revisaron experiencias previas como la portabilidad financiera y el Sistema de Consultas de Seguros (“SICS”), y se identificaron limitaciones en su adopción por parte de los usuarios. A partir de ello, se sugirió la necesidad de desarrollar interfaces sencillas, mecanismos de consentimiento eficaces y una gobernanza sectorial que permita dar sustentabilidad al modelo, tomando como base el conocimiento acumulado en otros sectores como el bancario y sanitario.

Finalmente, la cuarta mesa de trabajo se enfocó en las implicancias de la automatización de decisiones y el uso de herramientas de inteligencia artificial (IA) en la operación aseguradora. Con la entrada en vigencia de la nueva ley, se reconoció que las compañías deberán revisar aquellos procesos que puedan generar efectos jurídicos relevantes sobre los titulares de datos, tales como el cálculo automatizado de primas, el rechazo de siniestros o el perfilamiento de clientes.

Los participantes relevaron la importancia de garantizar transparencia algorítmica y mecanismos efectivos para la intervención humana en decisiones relevantes. Se discutió la validez del consentimiento como base legal en contextos sensibles, la aplicabilidad del criterio de necesidad contractual y la necesidad de preparar explicaciones comprensibles sobre el funcionamiento de los modelos utilizados. Todo ello, con el objetivo de construir guías sectoriales que permitan alinear la innovación tecnológica con las exigencias de protección de derechos.

El presente trabajo recoge de manera sistemática los desafíos gremiales levantados, evidenciando el alto grado de conciencia que el sector asegurador posee respecto de la magnitud de los cambios normativos en curso y la importancia de enfrentar este nuevo escenario incorporando el cumplimiento normativo dentro de la cultura de cada empresa y promoviendo procesos de diálogo con las autoridades regulatorias, siempre en observancia de las normas que promueven y defienden la libre competencia en Chile.

Capítulo I : Gobernanza y Coordinación Normativa

En un contexto normativo que evoluciona con rapidez y en el que convergen múltiples regulaciones -como la protección de datos, la ciberseguridad, los servicios financieros digitales y los derechos del consumidor-, la gobernanza y la coordinación normativa se han transformado en pilares fundamentales para la estabilidad, la legitimidad y la operatividad del ecosistema asegurador chileno.

La entrada en vigencia de la Nueva LPDP trajo consigo una serie de desafíos que no solo afectan la relación entre los aseguradores y sus clientes, sino también la interacción entre estos actores y las autoridades competentes. Esta transformación no puede abordarse con una simple reacción a la ley, sino que exige construir marcos de gobernanza que permitan implementar de manera coherente las nuevas exigencias legales, armonizando criterios, previniendo conflictos y asegurando una aplicación progresiva y eficiente de la normativa.

En este escenario, el diálogo entre el sector asegurador -incluidas las compañías tradicionales, los corredores y las insurtechs- y las distintas entidades regulatorias debe pasar de ser esporádico o reactivo a convertirse en una práctica permanente, colaborativa y técnicamente fundada. Solo mediante ese diálogo continuo será posible diseñar reglas prácticas, generar certeza jurídica y evitar que los desafíos regulatorios se transformen en barreras para la innovación o la competencia.

Uno de los primeros obstáculos que enfrenta la industria es la superposición de normas. Hoy confluyen regulaciones provenientes de distintas leyes sectoriales: la Ley de Protección de Datos, la Ley Marco de Ciberseguridad, la Ley Fintech, la normativa sobre derechos del consumidor, y marcos legales específicos del ámbito de la salud, todos con aplicación potencial sobre los mismos hechos. Esta pluralidad, sin una coordinación efectiva, produce incertidumbre sobre qué norma prevalece en caso de conflicto y qué autoridad es competente para fiscalizar cada situación. Para las entidades del sector, esto implica cargas duplicadas, riesgos regulatorios y una complejidad que sólo puede abordarse con una gobernanza proactiva.

La fragmentación institucional agrava el problema. La Comisión para el Mercado Financiero (“CMF”), el Servicio Nacional del Consumidor (“SERNAC”), la Agencia de Protección de Datos (“APDP”) y la Agencia Nacional de Ciberseguridad (“ANCI”) actúan muchas veces con mandatos convergentes pero sin instancias formales de articulación. La ausencia de espacios institucionalizados de coordinación entre estas agencias ha llevado a que algunas normas se apliquen sin considerar sus efectos en otras áreas, y que los regulados deban asumir costos y esfuerzos que no necesariamente mejoran la protección de los usuarios ni la eficiencia de los servicios. Frente a este diagnóstico, se aprecian diversas alternativas orientadas a fortalecer la gobernanza sectorial. Una de ellas es la elaboración de guías específicas para el sector seguros, consensuadas entre reguladores y gremios, que definan con claridad cuáles son las obligaciones que prevalecen cuando existen normas en conflicto, qué criterios deben aplicar las autoridades fiscalizadoras, y cómo debe coordinarse la regulación en aspectos comunes. Estas guías no solo permitirían armonizar los distintos cuerpos normativos, sino que además ofrecerían seguridad jurídica tanto para los reguladores como para las entidades fiscalizadas.

Otro mecanismo de coordinación clave podría ser el establecimiento de mesas de trabajo permanentes entre el sector y la autoridad. Estas instancias no deben limitarse a diálogos informativos, sino constituirse como espacios de colaboración técnica, donde se discutan borradores de reglamentos, se anticipen criterios interpretativos, y se evalúe de manera conjunta la viabilidad de las nuevas exigencias. Un ejemplo concreto sería someter a consulta pública los instrumentos técnicos vinculados a la aplicación de la Nueva LPDP antes de su entrada en vigor, permitiendo así su adecuación a la realidad operativa del sector asegurador.

Asimismo, podría evaluarse junto con las autoridades un mecanismo de certificación centralizado, denominado -por ejemplo- “Sello APDP” o “Sello ANCI”, según cuál fuese el organismo al que se le otorgue dicha decisión. Este sello funcionaría como una validación oficial del cumplimiento de estándares mínimos en el tratamiento de datos personales, ciberseguridad, derecho del consumidor y otras regulaciones que afecten a la industria aseguradora. Su existencia

permitiría delimitar las competencias fiscalizadoras de otras agencias, evitando requerimientos contradictorios o redundantes. También ofrecería una señal de confianza hacia los usuarios y permitiría a las empresas demostrar su compromiso con la protección de la privacidad.

En paralelo, uno de los temas más sensibles es la gestión de datos en el sector, particularmente en lo relativo al uso de bases como SISGEN. La existencia de estas bases ha sido clave para prevenir fraudes, facilitar la tarificación y mejorar la eficiencia en la atención de siniestros. Sin embargo, su operatividad exige ser analizada y acondicionada bajo la nueva normativa, especialmente a la luz del principio de minimización de datos y del interés legítimo como base de licitud. Aquí, la gobernanza es esencial para definir claramente los usos permitidos, limitar la información compartida y establecer salvaguardas contractuales y técnicas para su administración.

En cuanto a las relaciones contractuales entre los distintos actores del sector, se ha observado una creciente necesidad de clarificar jurídicamente los roles de responsable y mandatario en el tratamiento de datos. Esto es particularmente relevante en esquemas de comercialización indirecta, donde intervienen corredores, sponsors y compañías. Las nuevas exigencias normativas obligan a que estos roles estén debidamente consignados en los contratos respectivos, y a que existan acuerdos específicos -como los Data Transfer Agreements (“DTA”) o Data Processing Agreements (“DPA”)- que respalden jurídicamente las funciones delegadas.

El cambio regulatorio no se agota en los instrumentos jurídicos. También requiere ajustes al interior de las organizaciones. Las compañías deben revisar sus modelos de gobernanza, capacitar a sus equipos en nuevas obligaciones y redefinir los niveles de acceso a la información personal, de modo que cada perfil funcional tenga acceso sólo a los datos que necesita. Esta tarea no solo responde a una exigencia legal, sino que contribuye a fortalecer la confianza de los usuarios y a reducir los riesgos reputacionales y legales asociados al mal uso de la información.Un aspecto adicional que se ha puesto en discusión es el derecho a la portabilidad de los datos personales, que plantea enormes oportunidades pero también desafíos prácticos. Para que la portabilidad sea útil y segura, es necesario establecer formatos comunes, canales de transmisión estandarizados y salvaguardas técnicas adecuadas. Esto requiere un trabajo conjunto, donde gremios, aseguradoras, insurtechs y autoridades definan reglas claras que faciliten el ejercicio de este derecho sin afectar la viabilidad de los modelos de negocio.

Finalmente, la irrupción de la inteligencia artificial y de sistemas automatizados en procesos como la suscripción, la tarificación o la gestión de siniestros ha llevado la discusión normativa a terrenos aún más complejos. La nueva ley reconoce el derecho de los titulares a no ser objeto de decisiones automatizadas que los afecten significativamente, salvo que concurran bases legales específicas. Esto implica que las compañías deberán revisar sus sistemas, incorporar mecanismos de intervención humana y preparar formatos para explicar, de manera comprensible, cómo funcionan sus algoritmos. Aquí también la coordinación con el regulador será esencial para evitar interpretaciones divergentes y asegurar una implementación razonable.

Capítulo II :
Educación normativa: un imperativo para la industria

Como se anticipó, la Nueva LPDP marca un antes y un después en la forma en que las compañías de seguros, corredores e insurtechs deben gestionar la información de sus clientes en Chile. Se trata de una legislación moderna, inspirada en estándares internacionales como el Reglamento General de Protección de Datos de la Unión Europea (“GDPR”), que impone obligaciones sustantivas y formales a todo aquel que actúe como responsable o encargado del tratamiento de datos personales.

En este nuevo contexto normativo, la implementación de políticas de cumplimiento al interior de las empresas no puede limitarse a la adopción formal de manuales o protocolos. Por el contrario, se requiere una transformación profunda de la cultura interna de las organizaciones, que reconozca la protección de datos no como una carga administrativa, sino como un componente corporativo esencial. Esta transformación solo será posible si existe un compromiso transversal desde el directorio hasta los niveles operativos de las empresas.

Un nuevo estándar de responsabilidad

La Nueva LPDP establece principios que redefinen la forma en que las organizaciones deben concebir sus procesos internos: minimización de datos, proporcionalidad, finalidad específica, consentimiento inequívoco, deber de información y derecho a la portabilidad, entre otros. A estos se suman obligaciones concretas como el deber de registro de actividades de tratamiento, la realización de evaluaciones de impacto en privacidad, la notificación de incidentes de seguridad y la designación de un delegado de protección de datos (“DPO”) en ciertos casos.

La consecuencia práctica de estas disposiciones es clara: todo miembro de la organización que tenga acceso, manipule o gestione información personal debe estar debidamente formado e informado para hacerlo conforme al nuevo estándar. En este sentido, la educación normativa es una necesidad estratégica.

Las aseguradoras manejan datos altamente sensibles -desde condiciones médicas hasta patrones de comportamiento financiero-, lo que las convierte en actores especialmente expuestos. El desconocimiento o mal manejo de estos datos puede derivar no solo en sanciones administrativas significativas, sino también en litigios civiles, pérdida de reputación y daño irreversible en la confianza del cliente. Es más, podría afectar no sólo la responsabilidad de las empresas, sino de las personas naturales involucradas en una eventual infracción.

Por otro lado, si bien la Ley de Protección de Datos es la piedra angular de esta transformación, no puede analizarse de manera aislada. Existen otros cuerpos normativos que imponen estándares y deberes adicionales para las compañías de seguros y sus intermediarios, como la Ley Marco de Ciberseguridad, la Ley Fintech y la Ley N° 19.496 (“Ley del Consumidor”).

Y, como si fuera poco, la Ley N° 21.595 sobre Delitos Económicos tipifica diversas conductas relacionadas con el uso indebido de datos personales y dispositivos informáticos, las que podrían ser imputadas no solo la empresa misma, en caso de no contar con modelos de prevención adecuados, sino también las personas naturales.

Necesidad de un cambio cultural

Ante este entramado normativo, la respuesta razonable por parte de la industria debiera ser la adopción de programas integrales de cumplimiento que incluya, al menos, los siguientes elementos:

Capacitación periódica y obligatoria para todos los niveles de la organización en materia de protección de datos y ciberseguridad.

Diagnósticos de riesgo normativo y técnico, que identifique los procesos más sensibles en el ciclo de vida del dato.

Controles internos preventivos, con auditorías regulares y canales de denuncia seguros.

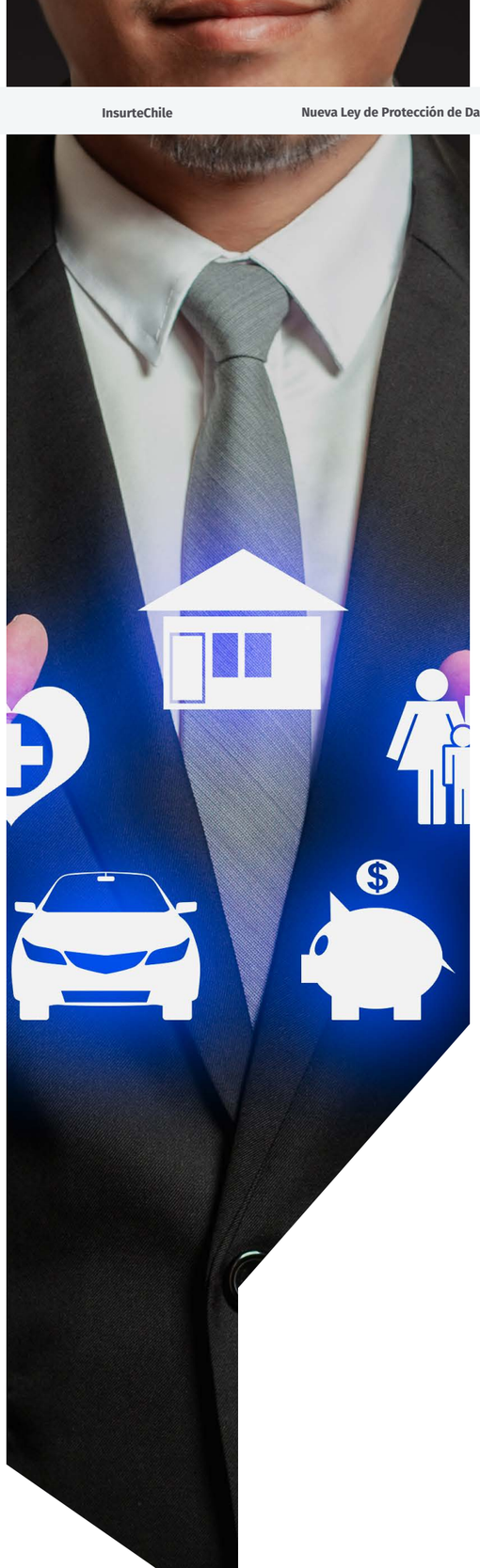
Revisión y rediseño de contratos con terceros, especialmente aquellos que impliquen subencargados de tratamiento o transferencia de datos.

Asesoría externa especializada, en caso de ser necesaria, capaz de ordenar procesos, proponer reformas y acompañar la implementación efectiva de medidas.

Revisión de políticas de privacidad, avisos legales y flujos de consentimiento, ajustados a la nueva legislación y a las buenas prácticas.

Este esfuerzo debe liderarse desde el más alto nivel. El directorio y la alta administración deben comprender que su responsabilidad no es solo reputacional o estratégica, sino que también puede traducirse en responsabilidad legal directa. La protección de datos ya no es solo un asunto del área legal o de tecnología: es un imperativo ético y organizacional.

La metodología, por tanto, debe ser colaborativa en todas sus etapas (desde el diagnóstico hasta la implementación de controles), a fin de evitar vacíos que impidan hacer una debida evaluación de riesgos al interior de las empresas y aplicar mecanismos que sean adecuados a su realidad concreta.



Capítulo III : Principios relevantes para la industria bajo la Nueva LPDP

A partir de lo indicado, es claro que la aplicación de la Nueva LPDP reviste especial relevancia en la industria aseguradora, dado que es probable que en torno a ella se alinee la mayoría de los otros estatutos aplicables. El cumplimiento efectivo de esta ley, por tanto, exige una revisión profunda de los procesos internos y externos asociados a la gestión de información personal, especialmente considerando el rol del corredor como intermediario clave.

Ya sea que se trate de un modelo de venta masivo o tradicional, se puede justificar el tratamiento de datos que realizan los intervinientes en una o varias causales, pero una de sus características más relevantes es el hecho de que los roles varían según la finalidad y utilidad que se le está dando al respectivo dato personal. Por ejemplo, es probable que una empresa pase desde basar su tratamiento de datos en un consentimiento dado en una etapa precontractual, a basarlo en la ejecución del contrato una vez celebrado el seguro, o en la ley misma en materia de liquidación.

Además, la Nueva LPDP despeja cualquier discusión sobre quién es el dueño del dato, es siempre el cliente. De la misma forma, los roles de las partes en relación con el dato viene dados por la propia ley, con independencia de lo que se establezca en los contratos entre estas.

1. Consentimiento y Licitud del Tratamiento de Datos en la Relación Aseguradora-Corredor-Cliente

1.1 Obtención Válida de Consentimiento

En el sector asegurador, el consentimiento constituye la base general para el tratamiento lícito de datos personales (artículo 12). Tanto las compañías como los corredores deben obtener un consentimiento libre, informado, específico respecto a cada finalidad (por ejemplo: cotización, emisión de póliza, gestión de siniestros), previo e inequívoco por parte del cliente titular.

Veamos un ejemplo práctico:

Cuando un corredor recopila antecedentes personales y sensibles (salud, patrimonio) para cotizar seguros en distintas compañías, debe presentar al cliente un formulario claro donde se especifique cada finalidad del tratamiento y obtener su aceptación expresa (por escrito o medio electrónico). La revocación del consentimiento debe ser tan sencilla como su otorgamiento.

La ley prohíbe prácticas como consentimientos tácitos o "por defecto", así como condicionar la prestación del servicio a consentimientos no estrictamente necesarios para su ejecución.

1.2 Interés Legítimo vs Consentimiento: Casos en la Intermediación

El artículo 13 permite que tanto aseguradoras como corredores traten datos sin consentimiento cuando exista un interés legítimo que no menoscabe los derechos del titular.

En la práctica aseguradora, ello podría ocurrir en hipótesis como las siguientes:

Prevención del fraude: El corredor puede compartir información relevante con la aseguradora para detectar operaciones sospechosas.

Gestión administrativa interna: El procesamiento mínimo necesario para cumplir obligaciones legales o contractuales puede fundarse en interés legítimo.

No obstante, siempre debe informarse al titular sobre esta base jurídica y ofrecerle mecanismos efectivos para ejercer su derecho de oposición.

1.3 Marketing, Evaluación de Riesgos y Procesos Precontractuales

Marketing directo: El envío de ofertas personalizadas por parte del corredor o la aseguradora debe -por supuesto- realizarse bajo consentimiento expreso; por otra parte, si se invoca interés legítimo (por ejemplo, clientes vigentes), debe garantizarse siempre el derecho a oposición.

Evaluación precontractual: El análisis previo a la suscripción (evaluación del riesgo asegurable) nace de un consentimiento expreso manifestado en la solicitud o propuesta.

Evaluaciones de impacto: Cuando el corredor o aseguradora realiza tratamientos masivos, de menores o perfiles automatizados (por ejemplo, scoring para segmentar clientes), debe efectuar una evaluación previa de impacto conforme al artículo 15 ter.

2. Acceso, Minimización y Protección de Datos en la Cadena Comercial Aseguradora

2.1 Principio de Minimización aplicado a Corredores y Aseguradoras

El principio de proporcionalidad (artículo 3.c) exige que tanto corredores como aseguradoras recolecten y procesen únicamente los datos estrictamente necesarios para cada finalidad informada al cliente. Por ejemplo:

No solicitar antecedentes médicos si sólo se cotiza un seguro patrimonial.

Limitar el almacenamiento a lo indispensable durante la vigencia contractual o legalmente exigido.

Ambos actores deben establecer procedimientos periódicos para depurar bases de datos y anonimizar/suprimir información una vez cumplidos los plazos legales o contractuales.

2.2 Restricciones Internas y Responsabilidad Compartida

La ley impone obligaciones estrictas sobre seguridad (artículo 3.f) y confidencialidad (artículo 14 bis):

Los corredores deben restringir el acceso interno a los datos personales sólo al personal autorizado que intervenga directamente en la gestión comercial o administrativa.

Las aseguradoras deben exigir contractualmente a los corredores que implementen medidas técnicas y organizativas equivalentes.

Se recomienda establecer acuerdos internos claros sobre roles, responsabilidades y auditorías periódicas entre aseguradoras y corredores respecto al acceso y uso compartido de información.

El deber de confidencialidad subsiste incluso después del término laboral o contractual tanto para empleados directos como para intermediarios.

2.3 Designación y Rol del Delegado de Protección de Datos (DPO) en Entornos con Intermediarios

La Nueva LPDP exige que cada responsable identifique un encargado interno ("encargado de prevención", artículo 14 ter.b) responsable del cumplimiento normativo en materia de protección de datos personales.

En el contexto asegurador:

Tanto las compañías como los corredores con operaciones relevantes deben designar formalmente un encargado con autonomía suficiente para supervisar políticas internas,

coordinar respuestas ante incidentes e interactuar con titulares y con la Agencia.

Este encargado debe tener acceso directo a la alta dirección e independencia funcional respecto a las áreas comerciales.

En relaciones comerciales complejas (por ejemplo, brokers internacionales), se recomienda formalizar acuerdos sobre coordinación entre DPOs/encargados internos para asegurar coherencia en respuestas ante incidentes o solicitudes regulatorias.

Como se ha descrito, no cabe duda de que la Nueva LPDP redefine las obligaciones operativas en materia de protección y tratamiento de datos personales dentro del ecosistema comercial asegurador chileno. La existencia del corredor como intermediario introduce desafíos adicionales: desde asegurar una obtención válida del consentimiento hasta implementar controles efectivos sobre minimización, acceso restringido y designación clara del responsable interno. La colaboración transparente entre aseguradoras y corredores será esencial para cumplir con los estándares regulatorios, mitigar riesgos legales/reputacionales y fortalecer la confianza del cliente titular en todo el ciclo comercial del seguro bajo el nuevo marco legal chileno.

En relaciones comerciales complejas (por ejemplo, brokers internacionales), se recomienda formalizar acuerdos sobre coordinación entre DPOs/encargados internos para asegurar coherencia en respuestas ante incidentes o solicitudes regulatorias.

Como se ha descrito, no cabe duda de que la Nueva LPDP redefine las obligaciones operativas en materia de protección y tratamiento de datos personales dentro del ecosistema comercial asegurador chileno. La existencia del corredor como intermediario introduce desafíos adicionales: desde asegurar una obtención válida del consentimiento hasta implementar controles efectivos sobre minimización, acceso restringido y designación clara del responsable interno. La colaboración transparente entre aseguradoras y corredores será esencial para cumplir con los estándares regulatorios, mitigar riesgos legales/reputacionales y fortalecer la confianza del cliente titular en todo el ciclo comercial del seguro bajo el nuevo marco legal chileno.

Capítulo IV :
Herramientas y Plataformas

Bases de Datos Comunes en la Industria

Uno de los temas más relevantes para la industria aseguradora, considerando sus diversos participantes, dice relación con el acceso, utilización y contribución a sistemas de información comunes, entendiendo por tales a las plataformas tecnológicas, repositorios de información o infraestructura de datos de acceso compartido, operada y administrada de manera centralizada o distribuida, a la cual múltiples personas jurídicas independientes tienen derecho de acceso, consulta, ingreso o modificación de información, conforme con las condiciones, protocolos y niveles de autorización previamente establecidos, con el propósito de facilitar la prestación de servicios en este mercado.

Este tipo de infraestructuras ha cumplido un rol sustantivo en el desarrollo de actividades comerciales en el mercado asegurador, dotando a las compañías de activos de información que permiten su ejercicio competitivo, de conformidad con el marco normativo vigente.

Análisis Legal y práctico del SISGEN

El SISGEN es una plataforma de información común administrada por la Asociación de Aseguradores de Chile S.A., que permite a las aseguradoras asociadas acceder a información de siniestros dentro de los ramos de seguros generales, exceptuando ciertos seguros como el SOAP, con el fin de apoyar la labor competitiva e independiente de suscripción de riesgos, a través del acceso de información de siniestralidad de los asegurados, mitigando así los riesgos inherentes al riesgo moral o al fraude o entrega de información insuficiente por parte de los actuales y potenciales asegurados.

Desde una perspectiva práctica, SISGEN, como plataforma, comparte ciertos atributos similares a los que se encuentran y manifiestan en las centrales de riesgos o burós de créditos, en el sentido de dotar a los agentes, dentro del marco jurídico vigente, los elementos de información esenciales para el adecuado desenvolvimiento competitivo, (siniestralidad por un lado y morosidades o nivel de deuda por el otro).

Respecto del alcance legal, bajo las disposiciones de la Nueva LPDP, toda base de datos común debe cumplir estrictamente con los principios aplicables al tratamiento de datos personales dispuestos en su artículo 3°, esto es, licitud y lealtad, finalidad, proporcionalidad, calidad, responsabilidad, seguridad, transparencia e información, y confidencialidad.

Sobre este particular, nos enfocaremos particularmente en dos aspectos: la base de licitud aplicable y los responsables de datos concernidos.

Respecto de la base de licitud aplicable, conviene tener presente que bases de datos como el SISGEN no operan a la fecha a través del consentimiento del tratamiento de datos por parte de los usuarios. Contrario a lo anterior, se ha justificado a la fecha el tratamiento de datos concernido en SISGEN considerando la excepción a la autorización del titular de datos considerada en el inciso final del artículo 4° de la LPDP vigente.

"(…) Tampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos".

Teniendo presente que aquella excepción no se encuentra recogida en la Nueva LPDP, debe en consecuencia examinarse nuevas bases de licitud, bajo los términos de los artículos 12 y 13 del nuevo texto legal. Para estos efectos, debe tenerse presente que a diferencia de otras bases de datos comunes cuya existencia se encuentra mandatada por una obligación legal (como, por ejemplo, el nuevo Registro de Deuda Consolidada), no existe normativa legal explícita que requiera el establecimiento de un repositorio común sobre siniestralidad.

En otro orden de cosas, en lo que respecta al responsable de tratamiento de datos, debemos considerar que podrían cumplir este rol tanto la Asociación de Aseguradoras de Chile ("AACH") como gestor del sistema, como las compañías de seguros aportantes y consultantes, previo análisis de libre competencia del diseño que se proyecte. Conforme los términos de la Nueva Ley LPDP, debe determinarse quién o quiénes deciden los fines y medios del tratamiento concernido en SISGEN. Bajo este supuesto, pueden surgir diversas alternativas, como por ejemplo:

Las aseguradoras son todas corresponsables de tratamiento y la AACH es la encargada del tratamiento.

AACH es responsable de tratamiento de forma exclusiva.

AACH es responsable de tratamiento y las aseguradoras son otros responsables independientes respecto de las operaciones que realizan (aportar y consultar).

En nuestro caso, nos decantamos por la tercera opción, siendo de todas formas recomendable que se actualice la normativa interna de funcionamiento del SISGEN y que se suscriba un Data Sharing Agreement ("DSA") para regular las transferencias e intercambios mutuos. Asimismo, debe establecerse un procedimiento común de notificación de Derechos ARCOP (Acceso, Rectificación, Cancelación, Oposición y Portabilidad), toda vez que -de acuerdo con el artículo 10 de la Nueva LPDP- "si los datos personales del titular son tratados por diversos responsables, el titular puede ejercer sus derechos ante cualquiera de ellos".

En esta misma línea, recomendamos que el SISGEN como cualquier otra plataforma común cuente con las siguientes prestaciones:

Registrar quién accede a qué datos y para qué finalidad.

Permitir auditorías internas y externas.

Garantizar que sólo corredores, aseguradoras o liquidadores autorizados puedan solicitar o tratar información personal relevante para su función

Evaluación del Interés Legítimo en el Uso de Datos Compartidos

El artículo 13 (d) de la Nueva LPDP permite el tratamiento sin consentimiento cuando exista un interés legítimo del responsable o un tercero, siempre que no se vulneren los derechos y libertades del titular, practicándose el examen por fases que se conoce como "evaluación de interés legítimo". En bases como SISGEN:

El interés legítimo puede fundarse en la prevención del fraude, cumplimiento normativo o gestión eficiente del riesgo necesario para el cumplimiento de los deberes legales y normativos que pesan sobre las compañías de seguros para el aseguramiento de riesgos. Es obligatorio documentar una evaluación previa que

justifique el uso compartido frente a los derechos del titular.
El titular debe ser informado sobre este fundamento jurídico y tener mecanismos efectivos para ejercer su derecho a oposición cuando corresponda.

En ningún caso el canal comercializador (multitienda) puede acceder directamente a datos personales incorporados en esta plataforma; su rol se limita a facilitar la oferta comercial.

Propuestas de Limitación y Anonimización

La Nueva LPDP exige aplicar el principio de proporcionalidad del tratamiento: sólo deben tratarse los datos estrictamente necesarios para cada finalidad informada (artículo 3(c). Para bases comunes:

Se recomienda anonimizar o seudonimizar los datos cuando sea posible, especialmente para análisis estadísticos o estudios internos. Asimismo, se debe analizar inspectivamente si todas las variables a la fecha consideradas en la base son necesarias para los fines de tarificación.

El acceso debe estar segmentado según roles: por ejemplo, el liquidador sólo accede a información relevante para la liquidación del siniestro.

Los datos deben ser suprimidos o anonimizados una vez cumplida las finalidades concernidas. En bases como SISGEN, al igual que las limitaciones existentes en bases de centrales de riesgo, se debe evaluar la existencia de un plazo máximo de retención de datos, basado estrictamente en lo relevante para la evaluación de riesgo de suscripción.

Contratos y Gobernanza de Datos

2.1. Estándares Contractuales para Mandatos y Responsabilidad

La relación de intercambio y tratamiento de datos entre corredor, aseguradora y liquidador debe estar respaldada por contratos que reflejen las exigencias legales en materia de protección de datos personales. A diferencia de otros mercados, no resulta por sí evidente los roles o posiciones jurídicas que cada uno cumple considerando (i) las particularidades de la cadena de valor y comercialización de seguros, y (ii) que cada entidad tiene deberes con otros participantes a la par de tener que cumplir exigencias legales específicas y propias de su calidad regulatoria para con el asegurado, el contratante, y el beneficiario.

Consideraciones particulares cuando existe tratamiento por encargo

Mandato expreso: Todo tratamiento delegado (por ejemplo, procesamiento por parte del liquidador) debe estar regulado por contrato escrito o medio electrónico idóneo (artículo 15 bis).

Cláusulas obligatorias: El contrato debe especificar objeto, duración, finalidades del tratamiento, tipo de datos tratados, categorías de titulares y obligaciones recíprocas.

Responsabilidad solidaria: Si un encargado trata los datos fuera del mandato o los cede sin autorización expresa, asume responsabilidad solidaria junto al responsable principal.
Deberes post-servicio: Al término del encargo, el encargado debe devolver o suprimir todos los datos tratados.

En modelos masivos e individuales, estos estándares contractuales son esenciales para delimitar responsabilidades entre las partes e incorporar mecanismos claros para reportar incidentes o vulneraciones.

Recomendaciones en relaciones entre agentes, corredores, aseguradoras, canales, y liquidadores

Implementar una evaluación dinámica de funciones: Las entidades aseguradoras deben adoptar una metodología de evaluación continua y detallada de los roles que define la Nueva LPDP, analizando cada actividad de tratamiento de datos para determinar quién controla realmente los fines y medios. Esto va más allá de las etiquetas organizativas generales y permite comprender con precisión las responsabilidades.

Reforzar la gobernanza integral de los datos: Establecer y perfeccionar continuamente marcos de gobernanza de datos integrados que incorporen la privacidad desde el diseño en todos los procesos y sistemas empresariales desde su creación. Esto incluye un mapeo riguroso de los datos, evaluaciones periódicas del impacto de la protección de datos (“EIPD”) y mecanismos adecuados de rendición de cuentas para demostrar el cumplimiento continuo.
Desarrollar acuerdos contractuales a medida: Utilizar Data Processing Agreements a medida para las relaciones entre el responsable y el encargado del tratamiento, y acuerdos de responsabilidad conjunta legalmente vinculantes para las actividades de procesamiento compartidas. De ser el caso de múltiples responsables, considerar los DSA. Todos estos contratos deben definir claramente las responsabilidades respectivas, especificar las medidas de seguridad, esbozar los procedimientos relativos a los derechos de los interesados y abordar con precisión el subprocesamiento y las transferencias internacionales. Las plantillas genéricas suelen ser insuficientes para las realidades matizadas del intercambio de datos de seguros.

Priorizar la transparencia proactiva, especialmente para la IA: Mejorar la comunicación transparente con los titulares de datos en relación con todas las actividades de tratamiento de datos, en particular las que implican la toma de decisiones automatizada en la suscripción y la tramitación de siniestros. A la luz de las sentencias del Tribunal de Justicia de la Unión Europea (“TJUE”), las compañías deben estar preparadas para proporcionar información significativa sobre la lógica, la importancia y las consecuencias previstas de dichos procesos automatizados.

Establecer bases legales funcionales para los tratamientos y conjuntos de datos: Desarrollar estrategias claras para justificar la recopilación exhaustiva de datos sobre bases legales adecuadas, como intereses legítimos o necesidad contractual, garantizando el estricto cumplimiento del principio de proporcionalidad, todo lo que deberá ser debidamente documento en

caso de revisión posterior por parte de la autoridad.
2.2. Programas de Concientización Interna y Sanciones

En materia de protección de datos, la concientización se inserta dentro de las exigencias de gobernanza efectiva, que requiere contar con programas internos robustos. Se sugiere considerar, entre otros, los siguientes elementos.

Capacitaciones periódicas sobre principios legales aplicables.

Difusión interna sobre políticas corporativas y canales para reportar incidentes.

Simulacros regulares ante incidentes de seguridad, considerando las exigencias de gestión de riesgo operacional y de seguridad dispuestas por la CMF, la ANCI, y la APDP.

Sanciones

La Ley establece un régimen estricto de infracciones leves, graves y gravísimas (artículos 34 bis–34 quáter), con multas que pueden alcanzar hasta 20.000 UTM o incluso, en hipótesis de reincidencia ante infracciones gravísimas hasta el 4% de los ingresos anuales del giro en el último año calendario, e incluso suspensión temporal parcial o total del tratamiento (artículo 38).

Las empresas deben definir procedimientos disciplinarios internos claros ante incumplimientos.

Las sanciones deben ser proporcionales al daño causado e incluir medidas correctivas inmediatas.

Capítulo V : Portabilidad de datos y estandarización

Derecho a la Portabilidad de Datos

La Nueva LPDP reconoce expresamente en el artículo 9 el derecho a la portabilidad de los datos personales, permitiendo al titular solicitar y recibir una copia de sus datos personales en un formato electrónico estructurado, genérico y de uso común, que permita ser operado por distintos sistemas, así como transferirlos directamente a otro responsable cuando sea técnicamente posible.

Este derecho, de nueva generación en materia de protección de datos, nace como un refinamiento particular del derecho de acceso, dotando al titular de poder no solo conocer la información que de él concierne, sino incidir en su tratamiento digital, sea a través de su almacenamiento y copia local o bien la transferencia a terceros responsables a través de interfaces dedicadas. En este sentido, se ha establecido que el derecho a portabilidad considera dos prestaciones identificables entre sí:

(a) Recibir copia de datos en un formato electrónico estructurado, genérico y de uso común (p.ej. XML o JSON).

(b) Comunicar o transferir los datos directamente a otro responsable de datos, cuando sea técnicamente posible, a través de, por ejemplo, APIs, servicios de transferencia segura de datos, webservices, etc.

El derecho a la portabilidad, con todo, tiene limitaciones importantes:

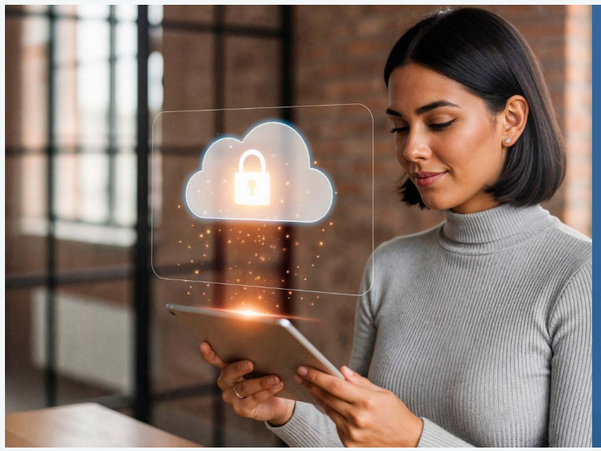
En cuanto a su alcance objetivo, se trata de los datos que el titular haya facilitado al responsable de datos, y que el tratamiento se realice automatizadamente considerando como base de licitud el consentimiento del titular.

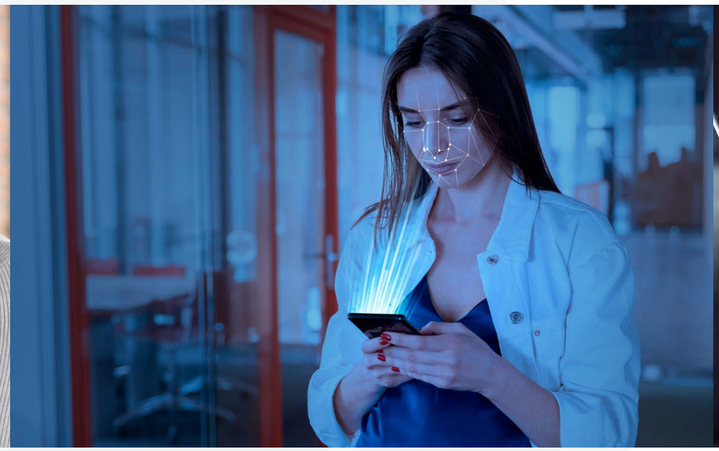
En cuanto a su aplicación práctica, no se exige directamente al responsable cumplir elementos de interoperabilidad más allá de un formato estructurado y uso común y usar interfaces, cuando estas existan. Así, elementos tales como la interoperabilidad sintáctica y semántica (que se estandarice la forma de incorporar los datos y el significado de los mismos) o elementos tales como interfaces de uso continuo y rendimiento eficiente quedan fuera de lo requerido por la ley. Asimismo, no se establece que sea un derecho de uso continuo, pudiendo darse el caso que se desarrolle a través de transferencias por evento (on-off).

Teniendo en consideración lo anterior, es dable señalar que regímenes como la portabilidad financiera (cuando se suscribe el uso de un formato JSON común entre proveedor actual y nuevo proveedor), el SICS, y próximamente el Sistema de Finanzas Abiertas (“SFA”) regulado por la Ley Fintech, consideran definiciones más exigentes en materia de integración e interoperabilidad, aunque limitadas al alcance de datos y partes de transferencia específicamente indicados en la ley. En contraste, el derecho a la portabilidad de la Nueva LPDP no descansa en requisitos técnicos concretos, pero facilita el intercambio entre cualquier tipo de responsable, respecto a todos los datos personales permitidos en el alcance objetivo. Esto último posibilita que se avance en mecanismos de autorregulación o estandarización que promuevan el uso e implementación de estándares comunes acordes a la necesidad de cada mercado y producto en particular.

Definición y Aplicación en el Sector Asegurador

En modelos donde un canal (por ejemplo, una multitienda) ofrece seguros intermediados por un corredor y asegurados por una compañía, el cliente puede ejercer su derecho ante cualquiera de estos responsables (corredor o aseguradora) para obtener sus datos -por ejemplo, historial de pólizas, siniestros, información declarada- y transferirlos a otra compañía o corredor si así lo desea.





En modelos tradicionales, el cliente puede solicitar al corredor o aseguradora que le entregue sus datos para cotizar con otro intermediario o cambiarse de compañía sin perder su historial relevante.

Beneficios y Riesgos de la Portabilidad Intra e Intersectorial

Entre los beneficios que se pueden prever en esta materia, destacan a priori los siguientes:

Empoderamiento del cliente: Facilita el cambio entre compañías o corredores sin barreras artificiales, promoviendo la competencia y mejores condiciones comerciales.

Eficiencia operativa: Reduce duplicidad en recolección de antecedentes y agiliza procesos precontractuales.

Transparencia: Permite al titular conocer qué información posee cada actor del ecosistema asegurador, en una forma estructurada, más allá de lo que pueda recibir como parte del derecho de acceso.

Integración e innovación: En la medida que existan las interfaces, permite la interconexión de diversos tipos de responsables de datos, tanto dentro como fuera del mercado asegurador, permitiendo la creación de modelos de seguros embebidos y oferta personalizada.

Por su parte, entre los riesgos que podrían visualizarse respecto de tal escenario de portabilidad, cabe destacar los siguientes:

Falta de entrega de valor: Entrega de archivos no estructurados de forma adecuada, clara y transparente, impide la utilización posterior por usuarios y otros responsables de datos.

Seguridad y confidencialidad: La transferencia masiva o frecuente puede exponer datos sensibles (salud, patrimonio) a riesgos sustantivos si no existen salvaguardas técnicas adecuadas.

Interoperabilidad limitada: Diferencias en formatos o sistemas pueden dificultar la efectiva portabilidad entre actores del sector o hacia otros sectores (por ejemplo, banca). Uso indebido: El acceso por parte de terceros no autorizados o la utilización para fines distintos a los consentidos puede generar infracciones graves según lo dispuesto en los artículos 34 ter y quáter.

Protocolo Sectorial de Portabilidad: Formatos, Interfaces y Salvaguardas

Estandarización sectorial

Definir formatos interoperables (por ejemplo, XML, JSON) que incluyan campos relevantes con extensión y tipo de datos previamente definidos (datos numéricos, alfanuméricos, variables binarias, etc.): identificación del titular, historial de pólizas, siniestros reportados/liquidados, beneficiarios designados.

Establecer interfaces seguras (APIs) para transmisión directa entre responsables cuando sea técnicamente viable, considerando mejores prácticas de identidad digital, autenticación y autorización (ID, ARC, Oauth2, OIDC).

Levantar propuestas de estandarización de información públicamente disponible y relevante para seguros: Incorporación de métricas estándar para determinación de variables y campos en aspectos tales como registros de propiedad, vehículos motorizados, información tributaria, etc.

Salvaguardas técnicas y organizativas

Autenticación robusta del titular antes de proceder con la portabilidad.
Registro detallado de las transferencias realizadas.
Encriptación durante la transmisión y almacenamiento temporal.
Registros trazables de autorización de acceso y consentimiento.

Limitaciones contractuales claras

Los contratos entre corredores, compañías y liquidadores deben establecer procedimientos específicos para atender solicitudes de portabilidad conforme a ley.

Debe informarse al titular sobre las consecuencias prácticas (por ejemplo, posibles demoras si existen siniestros pendientes).

Desafíos adicionales

En modelos masivos donde intervienen múltiples actores (canal comercializador, corredor, aseguradora), debe quedar claro quién es responsable primario ante solicitudes de portabilidad.
El canal comercializador no debe acceder ni almacenar datos personales en la medida que no se ejerza una portabilidad que los beneficie como receptores; sólo pueden responder solicitudes quienes tengan calidad legal de responsable o encargado según la Nueva LPDP

Como es posible apreciar, la portabilidad de datos personales bajo la Nueva LPDP representa un avance significativo hacia mercados más competitivos y transparentes en el sector asegurador chileno. El cumplimiento cabal no sólo mitiga riesgos regulatorios, sino que fortalece la confianza del cliente/asegurado bajo este nuevo marco legal integral.

Capítulo VI :
Automatización e Inteligencia Artificial

Decisiones Automatizadas bajo la Ley N° 21.719

1.1. Derecho a No Ser Evaluado Exclusivamente por IA

Como se ha indicado, la promulgación de la Nueva LPDP representa un hito normativo en Chile en materia de protección de datos personales y tiene importantes implicancias para el uso de tecnologías emergentes, especialmente la inteligencia artificial (“IA”) y la automatización robótica de procesos (“RPA”). En el contexto asegurador, estas herramientas tecnológicas han ganado un protagonismo creciente en procesos clave como la tarificación de riesgos, suscripción de pólizas, liquidación de siniestros y perfilamiento comercial de clientes. No obstante, la nueva regulación establece un marco de derechos y obligaciones que obligan a revisar y reestructurar muchos de estos usos.

Uno de los aspectos centrales de la ley es la consagración del derecho del titular a no ser objeto de decisiones automatizadas que produzcan efectos jurídicos o lo afecten significativamente, salvo que se cumpla alguna de las siguientes condiciones: (i) que exista consentimiento explícito del titular, (ii) que la decisión sea necesaria para la celebración o ejecución de un contrato, o (iii) que esté expresamente autorizada por una norma legal.

1.2. Consentimiento Explícito y Transparencia Algorítmica

Este derecho impone un deber a las aseguradoras de garantizar la transparencia, explicabilidad y revisabilidad de los sistemas automatizados, y también de informar claramente a los titulares sobre el funcionamiento y consecuencias de dichas decisiones. Las entidades deberán implementar mecanismos que permitan:

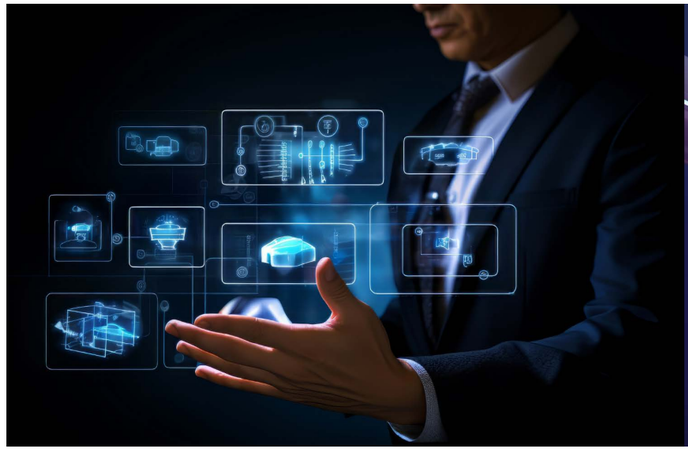
Informar de manera comprensible la existencia y lógica de los procesos automatizados.

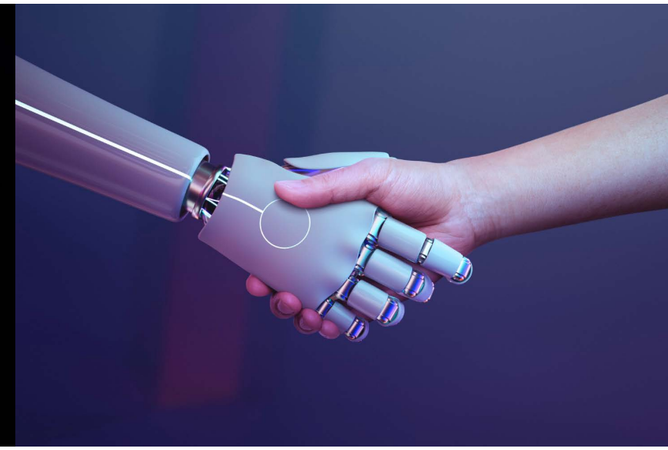
Garantizar la posibilidad de intervención humana, en caso de que el titular desee impugnar una decisión o presentar observaciones.

Establecer canales operativos y trazables para la recepción y respuesta a estos requerimientos.

1.3. Ejemplos y Casos de Uso: Tarificación, Suscripción, Siniestros

Durante el workshop de abril de 2025, se identificó que muchos de los procesos actualmente utilizados en la industria requieren una reconfiguración sustantiva para cumplir con estas exigencias. Si bien se reconoce el potencial de la excepción de “necesidad contractual” como base de licitud para decisiones automatizadas, existe un consenso sobre la falta de claridad operativa de esta figura. Se propuso que la futura Agencia de





Protección de Datos Personales desarrolle guías sectoriales que establezcan criterios comunes. Casos paradigmáticos como el uso de SISGEN, esencial para prevenir el fraude, requieren definiciones claras que aseguren su continuidad bajo una base jurídica válida.

Finalmente, se destacó la necesidad de avanzar hacia una explicabilidad algorítmica estandarizada mediante plantillas comunes que permitan entregar información relevante a los titulares sin afectar la propiedad intelectual de los modelos.

2. Desafíos Prácticos de la IA/RPA

2.1. Revisión de Procesos Automatizados y Mapeo de Riesgos

Durante la sesión correspondiente a esta temática, representantes de diversas entidades del sector compartieron experiencias y preocupaciones en torno a la aplicación práctica de la Nueva LPDP en contextos de automatización e inteligencia artificial. Un primer punto crítico fue la necesidad de mapear los flujos de negocio que involucran IA o RPA y auditar su cumplimiento normativo, particularmente en lo relativo a la licitud del tratamiento, proporcionalidad, y riesgos para los derechos del titular.

2.2. Retos de Implementación y Explicabilidad

Las organizaciones manifestaron que el plazo de 24 meses resulta limitado frente a los ajustes necesarios. Asimismo, se identificó una carencia de herramientas internas para ofrecer explicaciones comprensibles sobre el funcionamiento de los modelos automatizados. Se propone colaborar con el regulador en la creación de plantillas de explicabilidad, conciliando transparencia, viabilidad y protección de la propiedad intelectual.

2.3. Compatibilidad entre Interoperabilidad y Protección de Datos

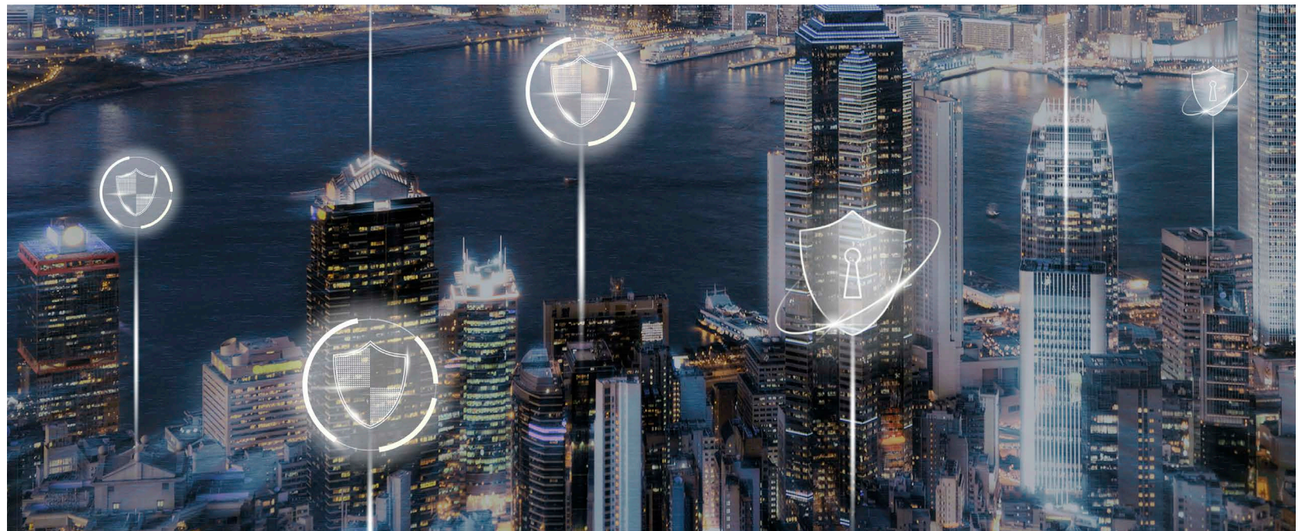
Se expresó preocupación por el posible impacto negativo sobre mecanismos compartidos como SISGEN. Si no se clarifica su estatus legal, podría producirse una fragmentación del ecosistema de datos del sector. Las aseguradoras también manifestaron dudas sobre el uso de fuentes externas como Equifax o TransUnion, y la necesidad de redefinir los límites del interés legítimo y el principio de minimización.

Capítulo VII :
Oportunidades y desafíos para la industria aseguradora

Chile está experimentando un profundo proceso de transformación en su arquitectura legal y regulatoria en materia financiera, tecnológica y de protección a los derechos de las personas. Este proceso, lejos de circunscribirse a un fenómeno meramente normativo, representa una oportunidad histórica para redefinir la cultura interna de las empresas y la relación entre los servicios financieros y la ciudadanía, particularmente en el ámbito de los seguros.

Este nuevo ecosistema regulatorio está llamado a transformar la manera en que las compañías de seguros, los corredores tradicionales y las insurtechs diseñan sus productos, interactúan con sus clientes y desarrollan sus modelos de negocio. Sin embargo, la velocidad del cambio normativo, sumada a los elevados estándares regulatorios en materia de transparencia, seguridad y protección de datos, plantean desafíos relevantes respecto de la capacidad adaptativa del sector y su disposición para asumir un rol protagónico en la economía digital.

La Ley Fintech no solo crea un marco normativo para regular nuevas formas de prestación de servicios financieros, tales como el financiamiento colectivo, la asesoría automatizada o la custodia de instrumentos financieros, sino que además introduce el SFA (“Open Finance”),



lo que permitirá que diversas entidades financieras tengan pleno acceso a ciertos datos de sus clientes a terceros autorizados, previa autorización expresa del titular de la información. Esta misma Ley consagra los seguros paramétricos, oportunidad para la industria aseguradora que enriquecerá el análisis del modelo de negocios de las empresas a futuro.

En el ámbito asegurador, este avance normativo podría abrir la puerta a una nueva etapa de competencia e innovación. En particular, las compañías de seguros y corredores podrían utilizar datos provenientes del sistema bancario, previsional y crediticio para perfeccionar su evaluación de riesgos, personalizar sus pólizas y desarrollar productos altamente segmentados. Asimismo, las insurtechs tendrían la posibilidad de acceder a información valiosa para diseñar productos a medida y ofrecerlos directamente al consumidor y a otras empresas mediante plataformas digitales.

La Nueva LPDP representa un cambio de paradigma en la forma en que las empresas -incluidas las aseguradoras y sus intermediarios- gestionan la información de sus clientes. Inspirada en el GDPR europeo, la ley chilena introduce principios que derivan en que, para la industria de seguros, el tratamiento de datos personales sensibles, tales como antecedentes médicos, información genética o historial de enfermedades, requerirá ahora una justificación jurídica más robusta y medidas de resguardo mucho más estrictas. Ello se traduce no solo en mayores exigencias en materia de compliance, sino también en la necesidad de rediseñar los sistemas internos, capacitar a los equipos, establecer nuevos procesos de gobernanza de datos y, eventualmente, crear oficinas de protección de datos dentro de cada institución.

Este nuevo marco representa una oportunidad para que las aseguradoras apliquen políticas transparentes, consentimientos explícitos y estrategias de protección robustas. También se abre la posibilidad de alianzas con insurtechs especializadas en tecnologías de privacidad diferencial, anonimización o gestión del consentimiento.

La Ley Marco de Ciberseguridad, por su parte, impone a las entidades reguladas por la CMF un estándar de seguridad superior, particularmente en lo relativo a la gestión de incidentes, la protección de infraestructuras críticas y la obligación de reportar brechas de seguridad a la autoridad. En el caso de las compañías de seguros, esto adquiere una importancia capital, considerando el carácter masivo y sensible de los datos que manejan.

La ley establece además la presencia de entes prestadores de servicios esenciales que deben cumplir con obligaciones reforzadas en materia de gestión de riesgos, monitoreo continuo, auditorías internas y externas, y cumplimiento de estándares técnicos que serán definidos por la Agencia Nacional de Ciberseguridad. Las com-

pañías de seguros que operen a gran escala y manejen datos críticos probablemente serán catalogadas bajo esta figura, lo cual requerirá inversiones significativas en ciberdefensa, resiliencia operacional y coordinación con otros actores del sistema financiero.

Asimismo, la proliferación de insurtechs que operan bajo modelos 100% digitales hace necesario repensar los mecanismos de certificación de seguridad para proveedores tecnológicos, la interoperabilidad segura entre sistemas, y la creación de ambientes de pruebas reguladas (sandboxes) que permitan testear innovaciones sin poner en riesgo la estabilidad del ecosistema.

El marco legal en materia de consumo ha avanzado significativamente en principios como la información veraz, la no discriminación arbitraria, la reparación efectiva del daño y el derecho a la retractación en compras a distancia. En el sector asegurador, estas garantías son particularmente relevantes en el contexto de la contratación de seguros a través de plataformas digitales, donde la asimetría informativa es mayor y la comprensión del producto puede ser limitada.

La Ley del Consumidor exige hoy mayor transparencia en las condiciones contractuales, claridad en las exclusiones y tiempos de respuesta definidos en caso de siniestros. A su vez, la jurisprudencia del SERNAC y los tribunales de justicia ha establecido que las cláusulas ambiguas deben interpretarse en favor del consumidor, lo que obliga a rediseñar muchos contratos de seguros bajo un lenguaje más comprensible y accesible.

Esto representa una oportunidad para aquellas insurtechs que construyan sus propuestas de valor en torno a la experiencia del usuario, la usabilidad y la claridad de la oferta. Asimismo, los corredores y aseguradoras tradicionales pueden reposicionarse como aliados del consumidor si incorporan tecnología para mejorar los canales de atención, trazabilidad de reclamos y seguimiento de pólizas.

Capítulo VIII : Conclusiones

Frente a este nuevo escenario normativo, es probable que la industria aseguradora chilena se reconfigure en torno a modelos colaborativos entre incumbentes y nuevos entrantes. Las compañías de seguros tradicionales cuentan con capital, experiencia y redes de distribución consolidadas, mientras que las insurtechs aportan agilidad, capacidad de desarrollo tecnológico y conocimiento del consumidor digital. Los corredores, por su parte, tienen un rol clave en traducir la complejidad técnica del producto a un lenguaje comprensible para el cliente final.

El desafío es construir alianzas estratégicas que permitan aprovechar las fortalezas de cada actor, respetando los marcos regulatorios y promoviendo la inclusión financiera y digital. No se trata simplemente de adoptar tecnología, sino de repensar los modelos de negocio en función de los valores que las nuevas generaciones demandan: transparencia, eficiencia, seguridad y propósito.

Quienes sean capaces de integrar la protección de datos como un valor central, invertir en ciberseguridad como condición de continuidad operativa, y rediseñar sus productos bajo una lógica centrada en el usuario, no solo sobrevivirán en esta nueva etapa, sino que liderarán el cambio.

El desafío es de envergadura, pero también lo es el potencial de crecimiento. En la medida que compañías de seguros, corredores e insurtechs comprendan que el cumplimiento normativo es inseparable de la confianza del cliente, y con mayor razón en un contexto de coordinación regulatoria entre autoridades, se podrá construir una industria más sólida, competitiva y alineada con los principios que inspiran el nuevo escenario digital. En el mismo sentido, la colaboración público-privada para el diseño de normas racionales y justas -incluyendo evaluar un mecanismo de certificación centralizado- será indispensable para que la administración del Estado sea capaz de establecer reglas y criterios acordes a la dinámica de este mercado.

InsurteChile, la AACH y otras asociaciones gremiales desempeñarán un rol clave en este nuevo escenario para coordinar los esfuerzos de manera eficiente y realista, siempre respetando los lineamientos que establece la normativa y jurisprudencia de libre competencia en Chile.

www.insurtechile.org

hola@insurtechile.org

insurtechile

InsurteChile®

Co-Creando la Protección del Futuro

2025