UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA

DEPARTAMENTO DE INGENIERÍA COMERCIAL

VALPARAÍSO – CHILE

IMPACTO DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES N° 21.719 EN LAS INSTITUCIONES FINANCIERAS Y PROPUESTA DE UN PLAN DE ACCIÓN PARA SU CUMPLIMIENTO

MEMORIA PARA OPTAR AL TÍTULO DE INGENIERO COMERCIAL

PROFESOR GUÍA : MACARENA GATICA SILVA

PROFESOR CORREFERENTE : SERGIO MUÑOZ ARRIAGADA

DICIEMBRE 2025

CONSTANCIA DE VALIDACIÓN Y CONFIDENCIALIDAD DE MONOGRAFÍA A REPOSITORIO ACADÉMICO

1.- IDENTIFICACIÓN DEL TRABAJO ACADÉMICO

Tipo de monografía (marcar una opción): ☒ Memoria o trabajo de título; ☐ Tesis de Postgrado;

Título del trabajo: Impacto de la Ley de Protección de Datos Personales N°21.719 en las instituciones financieras y propuesta de un plan de acción para su cumplimiento.

Nombre del candidato(a): Valeria Patricia Vargas Leiva

Carrera / Grado: Ingeniería Comercial

Campus: Casa Central Valparaiso **;** **Departamento**: Ingeniería Comercial

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, Macarena Gatica Silva, en mi calidad de profesor(a) guía/director(a) del trabajo académico mencionado anteriormente **DEJO CONSTANCIA** que:

- He revisado esta versión del documento y corresponde a la versión final aprobada del trabajo.
- El trabajo cumple con los requisitos académicos y de formato establecidos por la institución

3.- EVALUACIÓN DE CONFIDENCIALIDAD POR PROPIEDAD INDUSTRIAL

☒ El trabajo **NO contiene información que amerite confidencialidad** y puede ser publicado de inmediato en repositorio con acceso abierto.

☐ El trabajo **CONTIENE** información con potenciales implicancias de propiedad industrial o intelectual y requiere un periodo de confidencialidad (embargo) por:

☐ 6 meses; ☐ 12 meses; ☐ 2 años; ☐ 3 años; ☐ 5 años; ☐ 10 años

Fundamentación de la necesidad de confidencialidad (obligatorio si se solicita embargo):

4.- FIRMAS

Profesor(a) guía o director(a) de memoria o tesis:

Fecha: 20/03/2026 ; **Firma:** _____

Estudiante o Candidato(a):

Fecha: 20/03/2026 ; **Firma:** _____

Este formulario debe ser insertado como página 2 de la memoria o tesis, completado y firmado por estudiante y profesor(a) antes de la entrega en portal PRISMA de Biblioteca USM.

AGRADECIMIENTOS

En esta etapa final, quiero agradecer a todas las personas que fueron parte de este proceso y que me acompañaron durante este importante camino académico.

A mi mamá, por su amor incondicional, su apoyo constante y por creer siempre en mí. Gracias por estar presente en cada etapa y por impulsarme a seguir adelante.

A mi papá, por ser mi ejemplo de esfuerzo, responsabilidad y perseverancia. Gracias por siempre tener los mejores consejos en los momentos más difíciles.

A mi hermano, por estar siempre presente a lo largo de este proceso y por acompañarme siempre con su cariño.

A mis compañeros, con quienes tuve la suerte de compartir este camino y hoy se han convertido en mis grandes amigos. Gracias por su apoyo y por hacer que esta etapa fuera aún más significativa.

A mis gatos, Rodolfo y Rocco, por su compañía silenciosa y cariño a su manera, que siempre lograron traerme calma en los momentos que más lo necesitaba.

Finalmente, agradezco a mi universidad por haber sido el espacio de aprendizaje y crecimiento que me permitió llegar hasta este momento y cerrar una etapa tan importante de mi vida.

RESUMEN EJECUTIVO

La presente investigación examina el impacto de la Ley N°21.719 sobre Protección de Datos Personales en las instituciones financieras chilenas y desarrolla una propuesta de plan de acción orientada a garantizar su cumplimiento efectivo. Esta normativa, promulgada en 2024 y cuya entrada en vigor está prevista para diciembre de 2026, representa una modernización sustantiva del marco regulatorio nacional, alineándolo con estándares internacionales como el Reglamento General de Protección de Datos (GDPR) europeo, en respuesta a la creciente digitalización y a los riesgos asociados a la gestión de información sensible.

El sector financiero chileno, por su naturaleza intensiva en datos personales, se configura como uno de los ámbitos más impactados por la nueva ley. La normativa introduce principios rectores tales como licitud, transparencia, seguridad y responsabilidad proactiva, amplía los derechos de los titulares e impone obligaciones específicas, entre ellas la designación de un Delegado de Protección de Datos (DPO), la realización de Evaluaciones de Impacto en la Privacidad (DPIA), la notificación de brechas de seguridad y la implementación de medidas técnicas y organizativas robustas. Asimismo, establece un régimen sancionatorio severo, con multas que pueden alcanzar hasta 20.000 UTM, lo que genera riesgos económicos y reputacionales significativos para las instituciones.

La metodología empleada combina análisis cualitativo, benchmarking normativo respecto del GDPR y evaluación costo–beneficio, evidenciando que la adopción proactiva de medidas de cumplimiento resulta más eficiente que asumir sanciones o daños reputacionales. El estudio concluye que la protección de datos debe integrarse como un eje estratégico dentro de la gobernanza corporativa, superando enfoques reactivos y consolidando una cultura organizacional orientada a la privacidad.

La propuesta de plan de acción contempla medidas en materia de gobernanza, procesos internos, infraestructura tecnológica, capacitación y gestión de incidentes, asegurando un enfoque integral y sostenible. El análisis económico demuestra que el costo estimado de implementación (CLP $185–297 millones) es entre cuatro y siete veces inferior al valor de una sanción gravísima, lo que refuerza la conveniencia de invertir en cumplimiento preventivo. Más allá del aspecto financiero, la protección de datos se erige como un factor estratégico para fortalecer la confianza del cliente, preservar la reputación institucional y garantizar la competitividad en un entorno digital cada vez más regulado.

En síntesis, la Ley N°21.719 no debe ser concebida únicamente como una exigencia normativa, sino como una oportunidad para que las instituciones financieras chilenas consoliden su resiliencia digital, adopten estándares internacionales y fortalezcan la confianza en la economía digital.

ABSTRACT

This research examines the impact of Chilean Law N°21.719 on Personal Data Protection within financial institutions and proposes a strategic action plan to ensure effective compliance. Enacted in 2024 and scheduled to take effect in December 2026, this regulation modernizes the national legal framework, aligning it with international standards such as the European General Data Protection Regulation (GDPR), in response to growing digitalization and cybersecurity risks.

The financial sector, due to its intensive use of sensitive data, is among the most affected by this law. The regulation introduces key principles such as lawfulness, transparency, security, and proactive accountability, expands data subject rights, and imposes obligations including the appointment of a Data Protection Officer (DPO), Privacy Impact Assessments (DPIA), breach notifications, and robust technical and organizational measures. It also establishes a strict sanctioning regime, with fines up to 20,000 UTM, creating significant economic and reputational risks.

The methodology combines qualitative analysis, regulatory benchmarking against GDPR, and cost–benefit evaluation, demonstrating that proactive compliance is more efficient than facing penalties or reputational damage. The proposed action plan addresses governance, internal processes, technological infrastructure, training, and incident management, ensuring a comprehensive and sustainable approach. Economic analysis shows that implementation costs (CLP $185–297 million) are four to seven times lower than the maximum fines, reinforcing the strategic value of compliance.

In conclusion, Law N°21.719 should not be viewed merely as a regulatory burden but as an opportunity for Chilean financial institutions to strengthen digital resilience, adopt international standards, and enhance trust in the digital economy.

INDICE

INDICE DE TABLAS

1) INTRODUCCIÓN

En los últimos años, la protección de datos personales ha adquirido una relevancia creciente a nivel global debido al acelerado avance de la digitalización, la masificación de los servicios financiero en línea y la interconexión de sistemas, que han generado un aumento exponencial en la generación y manejo de información sensible. Esto ha provocado la necesidad de garantizar la seguridad y privacidad de los datos frente a riesgos asociados a la vulnerabilidad, uso indebido , filtraciones o accesos no autorizados; riesgos que no sólo afecta a los individuos, sino también a las confianza en las instituciones y al buen funcionamiento de la economía digital.

En este contexto, la regulación en Chile no había sido tan estricta frente a estándares internacionales, como el Reglamento General de Protección de Datos (GDPR) en Europa o la Ley General de Protección de Datos (LGPD) en Brasil. La legislación vigente, la Ley 19.719 de protección de vida privada promulgada en 1999, es considerada insuficiente frente a los desafíos que plantea el mundo digital actual.

Ante esta situación, el 13 de diciembre de 2024 se promulgó la Ley N°21.719 de Protección de Datos Personales, que busca reemplazar la normativa anterior y cuya entrada en vigencia está programada para diciembre de 2026. Esta nueva ley tiene como objetivo actualizar y modernizar la normativa sobre protección de datos, adecuándola a los estándares internacionales y establecer un marco más riguroso y claro para las organizaciones que procesan la información de sus usuarios.

Esto implica un desafío significativo para las instituciones del sector financiero, dado que este tipo de instituciones gestionan grandes volúmenes de datos altamente sensibles, como historiales crediticios, transacciones, información patrimonial y, en algunos casos, datos biométricos. La correcta gestión de estos datos son fundamentales para mantener la confianza de los clientes y mantener la estabilidad del sistema económico.

Sin embargo, la falta de claridad y experiencia en la implementación de esta nueva normativa ha generado incertidumbre y desafíos técnicos respecto a los cambios estructurales, tecnológicos y culturales que deberán adoptar las instituciones financieras en un plazo relativamente corto. Este proceso implica una reestructuración de procesos, implementación de tecnologías avanzadas de protección y seguridad, así como la capacitación continua del personal en las nuevas obligaciones legales.

En este escenario, se busca analizar el impacto de la Ley N°21.719 de Protección de Datos Personales en las instituciones financieras chilenas y, partir de dicho análisis, proponer un plan de acción práctico

y viable que facilite su cumplimiento normativo. Con ello, se pretende entender los desafíos que plantea la ley y ofrecer una propuesta aplicada que contribuya a mejorar la gestión de datos, reforzar la confianza de los clientes y asegurar la competitividad del sector en un entorno cada vez más regulado y digitalizado.

2) ORIGEN Y PRÓPOSITO DEL ESTUDIO

El estudio del impacto de la Ley de Protección de Datos Personales N°21.719 en las instituciones financieras surge de la necesidad de analizar cómo los avances regulatorios y tecnológicos están transformando el ecosistema económico y social. En los últimos años, la digitalización ha intensificado la generación y circulación de datos, provocando que la información personal sea un activo estratégico de alto valor de las instituciones financieras, cuyo modelo de negocio depende de la confianza de sus clientes y de la seguridad del manejo de sus datos.

Esto ha provocado un incremento de los riesgos vinculados a vulneraciones de seguridad, fraudes, fuga y uso indebidos de los datos sensibles, lo que ha puesto en evidencia la importancia de la existencia de marcos normativos sólidos y mecanismos de cumplimientos efectivos. Lo anterior no solo representa un desafío técnico, sino también, uno ético y social respecto a la protección de los derechos fundamentales de las personas.

La elección de esta problemática para su estudio, responde al carácter crítico del sector financiero en Chile, debido a que el sistema económico depende de que las instituciones financieras manejen con responsabilidad los datos de los clientes, inversionistas y empresas. La exposición que conlleva el manejo de grandes volúmenes de información sensible, convierte a las instituciones en uno de los sectores más impactado por esta ley, debido a que los riesgos que esta quiere mitigar.

Además, este estudio se justifica por el contexto histórico en el que se encuentra Chile. La promulgación de la nueva Ley N°21.719 en diciembre de 2024, con entrada en vigor para 2026, marca un antes y después en la regulación chilena sobre datos personales, que por años fue considerada insuficiente frente a estándares internacionales como el Reglamento General de Protección de Datos (GDPR) en Europa o la Ley General de Protección de Daros (LGPD) en Brasil. Esta brecha normativa generaba una situación de desventaja en términos de competitividad y confianza internacional, que ahora demanda a las instituciones financieras procesos de adaptación acelerado para cumplir con las nuevas exigencias.

3) OBJETIVOS

3.1 Objetivo general

Analizar el impacto de la Ley de Protección de Datos Personales N°21.719 en las instituciones financieras en Chile y diseñar un plan de acción que permita su cumplimiento normativo efectivo.

3.2 Objetivos específicos

1) Evaluar el estado actual de las políticas y prácticas de protección de datos personales en las instituciones financieras.
2) Identificar las principales obligaciones y cambios que introduce la Ley 21.719 en el tratamiento de datos personales en las instituciones financieras.
3) Identificar los desafíos y brechas que enfrentan actualmente que instituciones financieras para adaptarse a los nuevos requisitos.
4) Proponer un plan de acción concreto y viables que facilite el cumplimiento normativo de la Ley 21.719, considerando estrategias, recursos y procesos.

4) ALCANCE GENERAL

En el presente estudio tiene como objetivo analizar el impacto de la Ley de Protección de Datos Personales en las instituciones financieras en Chile, específicamente en aquellas del sector bancario, ya que son estas entidades son actores claves en la economía nacional debido a que manejan información sensible sobre las finanzas de las personas, y si esa información no es protegida adecuadamente, se pone el riesgo la confianza de los clientes y estabilidad financiera del sistema económico del país.

La investigación se focaliza al territorio chileno, considerando el proceso de transición normativa que abraca el periodo 2024-2026, correspondiente a la promulgación y próxima entrada en vigor de la nueva normativa el año 2026, el cual es un periodo clave porque las instituciones deben preparase para la entrada en vigencia de la ley, mediante la implementación de ajustes en las estrategias organizacionales, tecnológicos y culturales

En cuanto a los límites del estudio se consideran las obligaciones específicas que la nueva ley impone a las instituciones financieras, incluyendo tanto los desafíos como las brechas que deben enfrentar para poder lograr cumplir con las nuevas disposiciones y la propuesta plan de acción que sirva como guía práctica para que se adapten de manera eficiente.

Por el contrario, se excluyen de la investigación otros sectores que también se encuentran sujetos a la ley, como el comercio, salud, educación u organismos públicos, dado que cada uno tiene sus propias características y desafíos que necesitan estudios propios. Así mismo, no se abordaran aspectos técnicos más avanzados de ciberseguridad, como protocolos de encriptación o desarrollo de software, ya que exceden los objetivos de la investigación.

5) ESTADO DEL ARTE

5.1 Conceptos claves

El análisis del impacto de la Ley N°21.719 en el sector financiero requiere aclarar previamente ciertos conceptos fundamentales., los cuales constituyen la base teórica que permite comprender el alcance de la normativa y las implicancias que tendrá en la gestión de datos de las instituciones financieras.

- **Datos de carácter personal o datos personales**: Cualquier información vinculada o referida a una persona natural identificada o identificable a través de medios que puedan ser razonablemente utilizados.

- **Datos personales sensibles**: Aquellos datos personales que conciernen o se refieren a las características físicas o morales de una persona, tales como el origen racial, ideología, afiliación política, creencias o convicciones religiosas o filosóficas, estado de salud físico o psíquico, orientación sexual, identidad de género e identidad genética y biomédica.

    - **Dato Biométrico**: Datos obtenidos a partir de un tratamiento técnico específico, capturando características físicas, fisiológicas o conductuales de una persona que permitan o confirmen su identificación única, tales como: huella, iris, rasgos de la mano o faciales y la voz.

      Para su tratamiento se requiere información:

        - Previa del sistema biométrico, fin del tratamiento y plazo.

        - Consentimiento expreso de su titular.

    - **Datos Personales de niños, niñas (<14) y adolescentes (>14 y <18)**:

        - Para niños/niñas: Se requiere autorización por los padres o representantes legales.

        - Para adolescentes: Se requiere la autorización del adolescente, salvo datos sensibles de menor de 16 años (>14 <16), donde aplica norma de niños/niñas.

- **Responsable del tratamiento**: Persona natural o jurídica, pública o privada, a quien compete decidir acerca del tratamiento de datos personales, sus medios y fines, con independencia de si los datos son tratados directamente por él o a través de un tercero o encargado del tratamiento o procesador de datos.

- **Titular de los datos**: Persona natural, identificada o identificable, a quien conciernen o se refieren los datos personales.

- **Tratamiento de datos**: Cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado, o no, que permitan recolectar, procesar, almacenar, comunicar, transmitir o utilizar de cualquier forma los datos personales.

- **Consentimiento**: Toda manifestación de voluntad libre e informada mediante la cual el titular de datos, su representante legal o mandatario, según corresponda, autoriza en forma expresa y por escrito el tratamiento de los datos personales que le conciernen.

  Este consentimiento debe ser: |

  - Libre: El titular no debe ser presionado o forzado a dar su consentimiento.

  - Especifico: El consentimiento debe ser para un propósito concreto, se debe detallar exactamente para qué utilizaran los datos.

  - Inequívoco: Debe haber una acción clara y positiva por parte del titular.

  - Informado: El titular debe recibir toda la información necesaria para tomar una decisión consciente. Esta información debe ser clara, sencilla y comprensible.

- **Fuente accesible al público**: Todas aquellas bases de datos personales, públicas cuyo acceso o consulta puede ser efectuado en forma lícita por cualquier persona, sin existir restricciones o impedimentos legales para su acceso o utilización.

- **Protección de datos personales**: conjunto de principios, normas y medidas orientadas a garantizar un tratamiento lícito, transparente y seguro de la información, vinculado al derecho fundamental a la privacidad y a la autodeterminación informativa.

- **Fishing**: método de engaño donde un atacante se hace pasar por una entidad legitima para obtener datos personales o financiero de la víctima mediante correos, mensajes o sitios web falsos.

- **Malware**: es un software malicioso que infecta dispositivos para robar información, dañar sistemas o interrumpir operaciones, siendo una de las principales amenazas para la seguridad bancaria.

- **Big Data**: conjuntos de datos extremadamente grandes, rápidos y variados que los métodos tradicionales no pueden manejar. Su objetivo es extraer valor y conocimiento oculto de estas grandes fuentes de información.

Estos conceptos no solo delimitan el marco técnico y jurídico de la Ley N°21.719, sino que además orientan la manera en que las instituciones financieras deberán integrar la privacidad en su gestión diaria. En este sentido, más que un conjunto de definiciones abstractas, representan herramientas prácticas que permiten transformar la protección de datos en un elemento central de la confianza y la sostenibilidad del sistema financiero chileno.

5.2 Antecedentes del Estado del Arte

5.2.1 Evolución de la protección de datos a nivel global

La protección de datos personales ha pasado de ser sólo una preocupación a convertirse en un pilar fundamental del derecho y la tecnología a nivel mundial. Su origen se remonta a finales del siglo XIX, donde los abogados estadounidenses Samuel Warren y Louis Brandeis publicaron el articulo llamado “El derecho de la privacidad” en la Harvard Review, marcando un hito al enfatizar en la necesidad de la privacidad de datos a medida que los avances tecnológicos empezaban a afectar la privacidad de las personas. Sin embargo, a nivel internacional esta materia tomó fuerza con la Declaración Universal de los Derechos Humanos de 1948, que estableció explícitamente los derechos de privacidad, señalando en el artículo 12: “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra injerencias o ataques”. Esto significó un gran avance en este tema, pero no fue hasta la era digital que este derecho requirió una regulación específica.

Según estimaciones de IDC, en 2010 se generaban cerca de 2 zettabytes de datos al año, mientras que en 2020 esa cifra superó 59 zettabytes, con proyecciones que apuntan a duplicarse en 2025. Este crecimiento acelerado ha convertido a los datos en un recurso estratégico equiparable al petróleo, base para el desarrollo de la inteligencia artificial, la analítica predictiva y la personalización de servicios. En consecuencia, el valor económico de la información se ha multiplicado, incentivando su recolección y tratamiento a gran escala por parte de empresas privadas y organismos públicos, trayendo consigo riesgos significativos.

La verdadera transformación global llegó con el Reglamento General de Protección de Datos (GDRP) de la Unión Europea en 2018, lo que no sólo provocó una revolución europea, si no impuso una nueva vara para la protección de la privacidad e impulsó cambios en todos los continentes, llevando a que las leyes y mecanismos se reforzaran en diversos países, como un aumento en las multas por violaciones de esta legislación. De esta forma, en las otras jurisdicciones se crearon creación de leyes similares para mantener el estándar internacional, como la Ley de Protección de Datos en Brasil (LGPD), la Ley de Privacidad del Consumidor en California (CCPA) y la nueva ley chilena de Protección de Datos Personales N°21.719, demostrando que la protección de datos ya no es una opción, sino una exigencia global.

5.2.2 Contexto internacional de la Protección de Datos

La evolución normativa en la protección de datos personales no ha sido un fenómeno aislado, sino parte de una tendencia internacional marcada por la digitalización de la economía y el creciente valor de la información en los mercados globales. Desde fines del siglo XX, distintos países y organismos han impulsado marcos regulatorios destinados a equilibrar la innovación tecnológica con la defensa de los derechos fundamentales de las personas.

El **Reglamento General de Protección de Datos (GDPR)** de la Unión Europea, aprobada en 2016 y vigente desde mayo del 2018 ha marcado un precedente en la protección de datos personales, convirtiéndose en el marco normativo más influyente y sentando las bases para la regulación de protección de datos en Europa y en todos los continentes. Su principal objetivo es proporcionar a los ciudadanos y residentes más control sobre cómo se utilizan sus datos personales y simplificar el entorno regulador unificando la legislación en los estados miembros de la Unión Europea, esta normativa no solo sistematiza principios universales como licitud, finalidad, minimización y responsabilidad proactiva, sino que también impone obligaciones estrictas a las organizaciones, incluyendo la designación de un Delegado de Protección de Datos, la realización de evaluaciones de

impacto y la notificación de brechas de seguridad. Su alcance extraterritorial lo convierte en un estándar para cualquier organización que trate datos de ciudadanos europeos, influyendo así en legislaciones de otros países.

Brasil fue pionero en América Latina en tener una ley de protección de datos fuerte, con la promulgación de la **Lei Geral de Proteção de Dados Pessoais (LGPD)** en 2018, se inspira en los principales lineamientos del GDPR y abarca tanto el sector público como el privado, reconociendo derechos amplios a los titulares y crea la **Autoridade Nacional de Proteção de Dados (ANPD)** como organismo de supervisión. De este modo, Brasil se posicionó como pionero regional en la adopción de estándares de privacidad (ANPD, 2020).

En Estados Unidos, el marco regulatorio ha sido más fragmentado, esto significa que no existe una ley nacional única y centralizada que cubra de manera uniforme todos los datos personales y sectores de la economía, a diferencia de marcos como el GDPR europeo o la LGPD brasileña. El ejemplo más influyente es la **California Consumer Privacy Act (CCPA)**, vigente desde 2020, la cual refuerza los derechos de los consumidores en cuanto al acceso, eliminación y limitación en la venta de sus datos personales. Aunque es de alcance estatal, la CCPA ha marcado un precedente relevante, especialmente por su impacto en empresas tecnológicas de alcance global (State of California, 2018).

Además de estas legislaciones específicas en algunos países, la discusión internacional sobre la privacidad de datos ha estado marcada por la labor de organismos multilaterales que buscan establecer estándares globales. Desde 1980, la **Organización para la Cooperación y el Desarrollo Económicos (OCDE)** ha promovido activamente directrices sobre privacidad y flujos transfronterizos de datos, las cuales fueron actualizadas en 2013 para enfatizar la responsabilidad proactiva y la seguridad integral en el ciclo de vida de la información (OCDE, 2013). Estas directrices sirven como modelo fundamental para países que buscan un marco equilibrado entre competitividad económica y protección de los derechos ciudadanos. Por su parte, el **Convenio 108 del Consejo de Europa**, abierto a la firma en 1981 y actualizado en 2018 bajo el nombre de **"Convenio 108+"**, constituye a el único tratado internacional vinculante en la materia, teniendo un rol clave en la difusión global de principios comunes de protección de datos y ha sido adoptado también por países fuera de Europa, lo que refleja su valor como plataforma universal (Consejo de Europa, 2018).

El contexto internacional evidencia un movimiento unificado hacia la consolidación de estándares más exigentes en la protección de datos personales y que lo reconoce como un derecho fundamental. En este escenario, Chile al promulgar la Ley N°21.719 El contexto internacional evidencia un

movimiento convergente hacia la consolidación de estándares más exigentes en la protección de datos personales.

5.2.3 Situación previa en Chile: Ley N°19.628 y sus limitaciones

La primera normativa chilena en materia de protección de datos fue la **Ley N°19.628** sobre **Protección de la Vida Privada**, promulgada en 1999. Para su época, esta ley representó un avance significativo al reconocer la importancia de regular el manejo de datos personales, pero con el paso del tiempo, el auge de las tecnologías digitales y la globalización de la economía de datos la hicieron insuficiente para responder a los desafíos contemporáneos, como la acelerada digitalización, la internacionalización de los servicios financieros y el aumento de la exposición de las personas a riesgos de vulneración de la información (Consejo para la Transparencia, 2011).

Su diseño y alcance respondían a un contexto sustancialmente distinto al actual, caracterizado por riesgos digitales limitados y el uso masivo de Internet recién comenzaba a expandirse, encontrándose en sus primeras etapas. Esta situación dejó a Chile rezagado en comparación con otros países de la región, considerando que Argentina y Uruguay son reconocidos como los únicos países de América Latina que ofrecen un adecuado nivel de protección de datos, conforme a los estándares de la Directiva 95/46 del Parlamento Europeo y del Consejo.

En la práctica, la aplicación se ha limitado a la judicialización de casos puntuales de vulneración, sin abordar la complejidad del tratamiento de datos a gran escala ni de definir las responsabilidades adecuadas de las empresas en la gestión de la información de sus clientes.

5.2.3.1 Brechas y desafíos detectados en la antigua normativa

El diseño de la Ley N°19.628 presentaba limitaciones estructurales que fueron objeto de críticas por parte de organismos internacionales, estas deficiencias pusieron en evidencia la urgente necesidad de una nueva legislación que fuese más moderna y acorde con la nueva era digital. La normativa presentaba importantes brechas y desafíos que, en la práctica, impedían una protección efectiva de los derechos de las personas en el manejo de su información personal.

Una de las limitaciones más relevantes radica en que el enfoque central de la ley es el tratamiento lícito del dato por parte de las empresas, dejando en segundo plano el control efectivo y el derecho del titular. Su diseño establece las condiciones mínimas para que una entidad puede recopilar y usar la información, priorizando la circulación del dato necesaria para la economía de 1999. Este enfoque genera un desequilibrio de poder a favor de las empresas que son responsables del tratamiento, ya

que se concentra más en las obligaciones de quien usa el dato que en la capacidad de la persona de decidir sobre su destino.

A esta debilidad se le suma la **excepción de fuente de acceso público**, cuya formulación resulta ser excesivamente amplia y ambigua. La normativa, específicamente en su artículo 2 letra G, define a estas fuentes como *"registros o recopilaciones de datos personales públicos o privados de acceso no restringido o reservado a los solicitantes"*, lo que implica una presunción permisiva, debido a que determina que salvo el titular de los datos permita su divulgación, o a menos que la ley prohíba su divulgación, cualquier tercero puede acceder y dar tratamiento a la información que se encuentra en estas fuentes accesibles al público. Al ser formulada antes de la masificación del internet y las redes sociales, esta Ley no pudo anticipar la exposición masiva de datos que estas plataformas generarían, lo que significa que esta información es considerada una información accesible al público, el cual puede ser tratado por terceros sin el consentimiento del titular. Por lo tanto, este defecto de formulación crea una excepción que permite que un gran universo de datos personales sea tratado y recopilado por terceros sin requerir el consentimiento explícito del titular, dejando a una cantidad enorme de información sin protección real.

Un defecto adicional y de gran envergadura en la Ley N°19.628 fue la ausencia de un organismo o autoridad encargada de controlar y fiscalizar el cumplimiento normativo sobre tratamiento de datos personales, lo que generaba una aplicación limitada, ineficaz y poco uniforme, dejando la fiscalización diluida y dependía de la iniciativa de los propios titulares de la información velar por el resguardo de sus derechos. Esto obligaba a los ciudadanos a recurrir directamente a tribunales de justicias, un proceso excesivamente engorroso, lento y complejo, resultando en la imposibilidad de hacer sus derechos efectivos de manera oportuna, excepto en casos excepcionales y graves. Además, esta ausencia de supervisión provocó una débil o nula cultura de cumplimiento normativo en las organizaciones, que no veían un riesgo real a eventuales incumplimientos en la normativa.

Adicionalmente, los derechos reconocidos de los titulares de datos eran limitados y de difícil ejercicio en la práctica, ya que la Ley sí contemplaba la posibilidad de solicitar el acceso, rectificación, cancelación o eliminación (derechos ARCO) de información personal, eran procedimientos que carecían de claridad, accesibilidad y rapidez necesaria, esto quiere decir, que si bien la Ley otorga al ciudadano derechos teóricos, no provee las garantías procesales ni los mecanismos para obtener una respuesta satisfactoria y oportuna por parte del responsable del tratamiento.

Otro aspecto crítico, es la debilidad de su régimen sancionatorio, debido a que las multas establecidas en la Ley N°19.628 eran notablemente bajas y carecían del efecto disuasorio necesario para generar

un incentivo real para su cumplimiento. En especial en sectores de gran relevancia económica y volúmenes de información sensible como el sector el financiero, debido a que establecen sanciones que oscilaban entre 1 y 50 UTM (Unidades Tributarias Mensuales), lo que provocó un escenario en que los costos de incumplir la normativa fuesen significativamente menores que las inversiones necesarias para implementar medidas robustas de seguridad, gobernanza y compliance. En consecuencia, de manera indirecta esta Ley incentivó un cálculo de riesgo/beneficio que favorecía el incumplimiento y la exposición de los datos, consolidando una cultura de ausencia de riesgo real en el tratamiento de la información personal.

En consecuencia, la Ley N°19.628 se consolidó como una normativa obsoleta e insuficiente, completamente incapaz de garantizar una adecuada protección de la vida privada y seguridad digital en un país cada vez más interconectado. Las debilidades estructurales de esta ley representaban una amenaza significativa para la confianza de los clientes y la resiliencia institucional, especialmente en el sector financiero, cuyas operaciones y estabilidad dependen fundamentalmente del manejo de grandes volúmenes de datos sensibles.

Estas limitaciones en la antigua normativa se transformaron en uno de los principales motores para la promulgación de la Ley N°21.719 para impulsar la modernización legal, que busca corregir estas deficiencias históricas y establecer un marco teórico robusto y acorde a los estándares de la era digital.

5.2.4 Contexto del sector financiero en Chile y su exposición al riesgo

5.2.4.1 Volumen y sensibilidad de los datos personales en la banca chilena

El sector financiero chileno maneja una enorme cantidad de datos personales de sus clientes muchos de los cuales incluyen son considerados altamente sensible. Este escenario es crucial dado que una porción significativa de la población adulta forma parte del sistema financiero formal, ya sea a través de la banca tradicional o servicios Fintech.

Según la Comisión para el Mercado Financiero (CMF), hacia mayo de 2025 se registraban más de 21,2 millones de clientes bancarios digitales en Chile (incluyendo tanto a personas naturales como a empresas), lo que representa un crecimiento de 92% desde 2019, una cifra equivalente a casi la población total del país. Cada uno de estos clientes entrega a las instituciones financieras datos de identificación (nombre y RUT), detalles de contacto, información laboral e ingresos, y sus datos financieros propiamente tales, como los saldos de cuentas, movimientos bancarios, historiales crediticios, entre otros. La confidencialidad de estos datos financieros es crítica, debido a que revelan información y patrones sensibles sobre los hábitos de gastos, niveles de endeudamiento y patrimonio

de las personas, lo que provoca que si caen en manos equivocadas o tienen un indebido manejo, podría afectar gravemente la privacidad y seguridad de los individuos.

Ante este contexto, el sector financiero chileno se caracteriza por manejar una de las bases de datos más voluminosas y delicadas del país, donde bancos y entidades financieras centralizan la información de millones de personas, desde datos personales básicos hasta datos financieros. Esta situación impone a estas instituciones una gran responsabilidad respecto a la seguridad de la información y protección de la privacidad, no solo para los clientes afectados, sino también para la confianza en la financiera involucrada. Las autoridades chilenas reconocen la importancia de mantener estándares estrictos de protección de datos en el sistema financiero, lo cual se ve reflejado en que la CMF ha enfatizado que todos los actores financieros deben cumplir con criterios estrictos y consistentes, dado que si un actor falla, esto puede tener efectos sobre todo el resto del sistema.

5.2.4.2 Digitalización financiera y exposición a riesgos

El acelerado avance de la digitalización de la banca y los servicios financieros en Chile ha multiplicado los canales de acceso y, con ello, los riesgos asociados. En la actualidad, la banca en línea y móvil se ha convertido en el estándar para la mayoría de los usuarios, cerca de un 75% de los consumidores declara acceder a la banca digital varias veces por semana, y alrededor del 40% abrió cuentas bancarias completamente en línea (Fintechile, 2025). Esta tendencia se ve reforzada por la demanda, un estudio realizado por PwC en 2025 revela que el 72% de los usuarios prefiere bancos 100% digitales, lo que refleja un crecimiento del 20% respecto a años anteriores. Si bien esta masificación de los canales electrónicos, como portales web, aplicaciones móviles y pagos digitales, ofrecen ventajas en torno en comodidad y el alcance para los usuarios, también amplía significativamente la superficie de ataque disponible para ciberdelincuentes si no se cuenta con las protecciones adecuadas.

Los ciberataques contra el sector financiero no son un fenómeno nuevo, pero su frecuencia, sofisticación y costo han incrementado sostenidamente en la era digital, esto se debe a que los bancos son blancos altamente atractivos debido a la riqueza de sus activos y la sensibilidad de los datos que custodian. Se estima que a nivel global, un 40% de los incidentes son intencionales (Aldasoro, 2022), siendo phishing y malware las modalidades más comunes. Chile no se encuentra ajeno a esta tendencia, el rápido crecimiento de la banca digital ha traído consigo una sofisticación paralela de los delitos en línea, incluyendo correos falsos diseñados para robar datos, virus informáticos infiltrados en sistemas bancarios, y ataques a plataformas financieras. El Banco Central de Chile (BCCh) ha advertido que la materialización de un riesgo cibernético en una entidad financiera podría poner en

peligro la confidencialidad, integridad o disponibilidad de sus sistemas, perjudicar su imagen e incluso afectar la confianza del público, provocando replicas en todo el sistema financiero. En casos extremos, una reacción inadecuada podría desencadenar situaciones de inestabilidad financiera sistémica, lo que subraya la importancia de fortalecer la ciber-resiliencia del sector, es decir, la capacidad del sistema para anticipar, resistir y adaptarse a incidentes y ciberataques.

En cuanto a los riesgos tecnológicos, estos crecen de la mano con la digitalización. Por un lado, las empresas deben adoptar tecnologías nuevas que exigen protocolos de seguridad para la protección de los datos que se almacenan y comparten. Paralelamente, los usuarios hoy en día realizan la mayoría de sus transacciones sin interacción humana, confiando en las plataformas digitales bancarias sean seguras. De acuerdo al estudio de PwC, indicó que 45% de los chilenos está preocupado por la protección de sus datos al usar servicios bancarios digitales, evidenciando a la ciberseguridad como un factor clave en la confianza del cliente Por lo tanto, si la percepción de la seguridad es débil o inexistente, muchos optaran por cambiar de banco o reducir su uso de canales en línea. Ignacio Munizaga, Gerente General de Magnet Chile, complementa al señalar que *"el desafío está en ofrecer una experiencia rápida y sencilla sin comprometer la seguridad, ya que si los clientes no sienten que sus datos están seguros, cambiaran de banco"*.

La digitalización ha transformado la seguridad de ser solo un costo operacional a ser un pilar de la estrategia comercial y la estabilidad sistémica. La exposición al riesgo cibernético no solo amenaza la integridad del sistema financiero, sino que también pone en juego la fidelidad del cliente, haciendo de la ciber-resiliencia un imperativo de mercado y una condición sine qua non para la competencia en la banca moderna.

5.2.4.3 Casos recientes de ciberataques y filtraciones

Desde el año 2018, Chile ha experimentado diversos incidentes de ciberseguridad que han afectado directamente a bancos y empresas financieras, comprometiendo tanto la continuidad operativa de los servicios como la integridad de los datos financieros de los clientes, evidenciando los múltiples riesgos digitales que enfrenta el sector financiero chileno.

1) **Ataque al Banco de Chile (mayo 2018)**:

Este incidente representó un punto de inflexión en la ciberseguridad bancaria chilena. El ataque sin precedente afectó al Banco de Chile, obligando inicialmente a cerrar sus sucursales y suspender sus servicios digítales, se trató de una operación altamente sofisticada, en la que los atacantes instalaron un malware destructivo como distracción para dañar 9.000 estaciones de

trabajo y 500 servidores. Sin embargo, el real objetivo era utilizar la red internacional SWIFT para realizar transferencias fraudulentas, logrando sustraer alrededor de US$ 10 millones desde cuentas del propio banco en el extranjero fue el primer ataque de carácter internacional atribuido a un grupo de hackers profesionales (presuntamente el grupo Lazarus de Corea del Norte), demostrando que incluso las instituciones financieras de mayor envergadura podían ser vulnerables al cibercrimen global. El impacto fue tanto financiero (pérdida directa de capital) como reputacional, pues generó una profunda preocupación ciudadana respecto a la capacidad de la banca para custodiar tantos los fondos como los datos de sus clientes.

2) Filtraciones masivas de tarjetas de crédito (julio 2018):

Apenas dos meses después del incidente del Banco de Chile, el sector fue sacudido por dos de las filtraciones más graves de datos financieros ocurridas en Chile. La primera filtración fue por un grupo de cibercriminales autodenominados ShadowBrokers publicó en redes sociales los datos de más de 14.000 tarjetas de crédito de clientes chilenos y extranjeros, la información incluía el número completo del plástico, la fecha de vencimiento y los códigos de verificación (CVV). Se estimó que al menos el 10% de estas tarjetas estaban activas y en uso, perteneciendo a múltiples entidades como Santander, Banco de Chile, Scotiabank, Bci, Itaú y BancoEstado. Este hecho obligó a los bancos emisores a bloquear preventivamente cientos de tarjetas, causando molestias a miles de clientes

Semanas después, se volvieron a filtrar datos de casi mil tarjetas de crédito a través de Twitter, de las cuales 208 estaban activas, siendo el fraude proveniente desde un comercio internacional. Más tarde, se produjo una nuevamente una filtración que expuso datos de unas 55.000 tarjetas adicionales en su mayoría extranjeras, pero también de más de 500 emitidas en Chile, de las cuales 188 eran bancarias.

El propio SERNAC calificó estas filtraciones como “una de las mayores vulneraciones de datos en la historia del país”, alertando sobre el daño irreparable de la confianza en los sistemas de pago digitales. Estos incidentes revelaron dos deficiencias cruciales en el sistema, la falta de estándares robustos de ciberseguridad que previnieran la captura masiva de datos y la ausencia de un protocolo eficiente de notificación oportuna que protegiera rápidamente a los titulares.

3) Vulneración de datos de clientes de BancoEstado (agosto 2018):

En agosto del mismo año, se descubrió la difusión no autorizada de información personal orquestada por un ingeniero informático de 23 años, con acceso a bases de datos públicas del SERVEL (Servicio Electoral), el cual había recolectado y difundido información personal de alrededor de 250.000 clientes de BancoEstado, publicando parte de estos datos en su cuenta de Twitter denominada “La Balsa Pirata”, e incluso intentó vender bases de datos en línea .

Aunque no se trató de un hackeo directo a los sistemas del banco, el caso demostró que la falta de regulación y control sobre bases de datos públicas podía derivar en graves filtraciones que afectaban directamente a la seguridad de las instituciones financieras y sus clientes. BancoEstado interpuso una querella criminal y el caso fue investigado como delito de uso indebido de datos personales. La exposición mediática fue considerable, y generó un fuerte cuestionamiento mediático sobre las falencias en la protección de información pública reutilizada en el ámbito privado, lo que puso en evidencia un vacío legal que la Ley N°19.628 no había previsto ni regulado.

4) Robo vía transferencias en Banco Consorcio (noviembre 2018):

Banco Consorcio fue víctima de un ataque informático que resultó en pérdidas económicas significativas. Mediante el acceso indebido a los sistemas de pagos internacionales, los atacantes realizaron transferencias fraudulentas por cerca de US$ 2 millones hacia cuentas en el extranjero. El banco reconoció el incidente, aunque aclaró que las pérdidas afectaban solo a recursos propios y no comprometían los fondos de los clientes.

Este hecho demostró que la exposición a ataques internacionales y el riesgo asociado a las interconexiones con redes financieras globales no era exclusivo de las grandes corporaciones, sino también instituciones medianas con operaciones globales. Además, el incidente en Banco Consorcio reveló la necesidad de reforzar los controles los sistemas de pagos transfronterizos, un punto débil que ya había sido explotado meses antes en el caso del Banco de Chile.

Los incidentes de 2018 reflejan la diversidad y gravedad de los riesgos cibernéticos que enfrenta el sector financiero, abarcando desde fraudes millonarios y filtraciones de datos personales de clientes hasta la interrupción de servicios al cliente. La urgencia de la situación se ve amplificada por la escalada actual de amenazas, debido a que en el año 2025, solo de febrero a abril, se detectaron 813.191 amenazas, lo que representa un crecimiento del 53% respecto al mismo periodo del año anterior.

Las lecciones extraídas de estos episodios han impulsado importantes cambios regulatorios y de inversión en seguridad. Además, cada incidente público sensibiliza más a las personas sobre la fragilidad digital, generando presión continua para mejorar los estándares y prácticas de seguridad, tanto en la banca tradicional como para plataformas Fintech. La recurrencia de estos ataques demostró de forma empírica que el marco legal preexistente era inefectivo para proteger la estabilidad financiera y la privacidad de los ciudadanos.

5.2.4.4 Alertas regulatorias y percepción social de la ciberseguridad en el sistema financiero chileno

Ante el sostenido incremento de las amenazas digitales, los organismos reguladores y supervisores en Chile han reaccionado activamente para reforzar las medidas de ciberseguridad del sistema financiero, consientes de los riesgos sistémicos.

La Comisión para el Mercado Financiero, que supervisa tanto bancos como entidades Fintech desde 2022, ha actualizado su normativa para exigir mayores estándares de seguridad, incorporando la gestión de ciberseguridad dentro de los requerimientos regulatorios para bancos en 2018 por la entonces Superintendencia de Bancos (SBIF, hoy integrada a CMF) En los años posteriores, la CMF introdujo instrucciones sobre gestión de riesgo operacional, seguridad de la información, continuidad de negocio y reporte de incidentes, un ejemplo clave es el capítulo 20-10 de la Recopilación Actualizada de Normas (RAN) para bancos, que cubre la gestión de s ciberseguridad y estableció las bases de datos de incidentes de seguridad obligatorias para entidades financieras. El objetivo principal detrás de estas regulaciones es aplicar estándares consistentes a todos los actores del mercado, pues una brecha en una institución financiera puede propagarse por la interconexión del sistema financiero, esto refleja la preocupación la solidez del sistema se determina por su componente menos resistente, especialmente en materia de protección de datos y ciber-resiliencia.

Por su parte, el Banco Central de Chile ha incorporado activamente las consideraciones de ciberseguridad en su rol responsable de la estabilidad financiera. En los recientes Informes de Estabilidad Financiera, el Banco Central ha señalado que los ciber-riesgos figuran entre las principales amenazas globales para la estabilidad, a la par de riesgos macroeconómicos tradicionales. Tras los incidentes del 2018, participó activamente en el Consejo de Estabilidad Financiera (CEF), el cual reactivó un grupo de trabajo especial sobre Continuidad Operacional, este grupo coordina a la CMF, Superintendencia de Pensiones, Ministerio de Hacienda y el propio Banco Central para compartir información de incidentes en tiempo real, acordar protocolos conjuntos de contingencia y asegurar que la regulación en ciberseguridad sea coherente en todo el sistema financiero. Fruto de

esta coordinación, en julio de 2018 las autoridades financieras chilenas firmaron un Memorándum de Entendimiento en que se comprometieron a unificar estándares y esfuerzos contra riesgos cibernéticos, y a realizar evaluaciones internacionales para detectar brechas respecto a las mejores prácticas globales.

En respuesta a las filtraciones de datos financieros que han afectado a los clientes, el Servicio Nacional del Consumidor (SERNAC) ha intervenido reiteradamente, recalcando a las empresas su deber de garantizar la seguridad de los consumidores. Luego de las filtraciones de tarjetas entre 2018 y 2019, el SERNAC exigió mejoras de seguridad y compensaciones, enfatizando que los consumidores tienen derecho a servicios seguros y que las empresas son responsables de proteger sus datos personales, asumiendo su responsabilidad en caso de fallos.

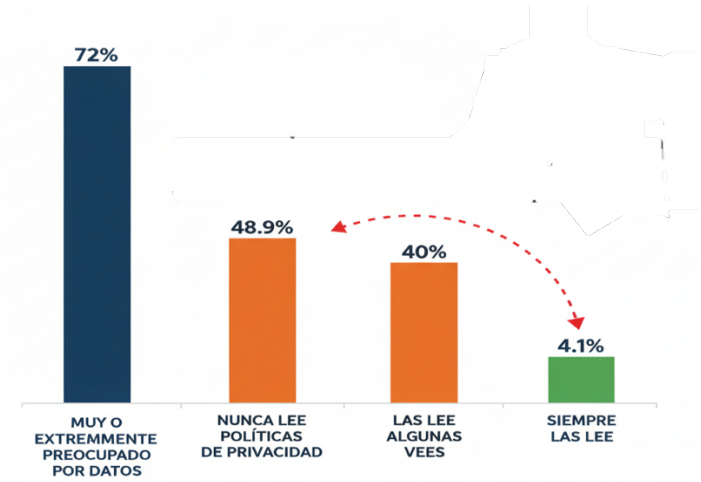
A nivel institucional y legal, Chile ha lanzado importantes iniciativas; en 2017 adoptó una Política Nacional de Ciberseguridad, creando en 2018 un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) gubernamental, y actualmente, el país discute una Ley Marco de Ciberseguridad, ya aprobada en el Senado (pendiente en 2025), que busca crear una Agencia Nacional de Ciberseguridad y fortalecer las capacidades para prevenir y responder a incidentes a nivel nacional, estas acciones demuestran que los organismos públicos están conscientes de las amenazas y decididos a robustecer el marco institucional.

En el intertanto, la CMF ha seguido actualizando normas específicas y del mismo modo, la Ley 21.719 de Protección de Datos Personales, promulgada a fines de 2024, implicará nuevas obligaciones para bancos y entidades financieras en cuanto al tratamiento lícito, seguro y transparente de la información personal de sus clientes, elevando el estándar de protección acorde a buenas prácticas internacionales.

Los incidentes constantes y el aumento de la dependencia digital han motivado fuertes advertencias regulatorias en Chile, así como también un alto grado de sensibilización ciudadana respecto a los riesgos en el ámbito financiero. El Banco Central, ha señalado que el riesgo de ciberataques o fallas en el sistema tiene efectos reputacionales y económicos que pueden llegar a romper la confianza del público e incluso derivar en problemas de estabilidad financiera si la respuesta es deficiente.

En cuanto a la percepción ciudadana sobre la seguridad de sus datos financieros y personales, este ha evolucionado hacia una mezcla de preocupación y demanda de mayores garantías. Una encuesta realizada en 2022 por el Servicio Nacional del Consumidor (SERNAC) para lograr identificar el conocimiento, los cuidados y el interés que tienen los consumidores respecto al tratamiento de sus

datos personales en los sitios web, mostró que un 72% de los chilenos se declara muy o extremadamente preocupado por la posibilidad de que sus datos personales sean recopilados o utilizados sin autorización en internet, el 48,90% nunca leen la política de privacidad de los sitios web que visitan, 40% de las personas declara leerla algunas veces y sólo el 4,1% señala siempre leer la política de privacidad del sitio web que navega.



Fuente: SERNAC

La autoridad destaca que estos resultados confirman la "Paradoja de la Privacidad" que se observa a nivel internacional, un fenómeno donde los consumidores expresan su preocupación por sus datos, pero sus acciones no reflejan ese mismo nivel de cuidado, debido a la tendencia de revelar información personal a cambio de recompensas relativamente pequeñas o a un bajo compromisos por proteger sus datos personales. Esta inquietud general por la privacidad se vincula directamente con el ámbito financiero, donde los usuarios comparten información sensible con bancos y esperan altos estándares de protección. Asimismo, en el contexto de creciente delincuencia informática, más de la mitad de las personas percibe un riesgo elevado de ser víctima de fraudes o delitos online, lo que ha hecho de la seguridad digital una prioridad en la opinión pública. Cada incidente de alto perfil en un banco refuerza dichas percepciones, como el caso de Banco Estado en 2020, se evidenció temor entre algunos clientes respecto a la disponibilidad de su dinero y la integridad de sus datos, al punto que hubo un pico de consultas y reclamos ante organismos como el SERNAC y asociaciones de consumidores.

Hoy existe un consenso claro entre reguladores y ciudadanía acerca de la importancia de proteger los datos y operaciones financieras frente a riesgos tecnológicos. Las advertencias de las autoridades

buscan prevenir que nuevos incidentes afecten la confianza en el sistema bancario, recordando que la confianza es un activo frágil que puede verse debilitada rápidamente tras una brecha de seguridad. A su vez, los clientes exigen cada vez con más fuerza transparencia y diligencia, esperando que los bancos actúen con máxima responsabilidad. Esta presión dual ha impulsado mejoras continuas en los estándares de ciberseguridad, así como un entorno normativo más robusto que aspira a elevar significativamente la protección de los datos personales en Chile. En última instancia, la fluida colaboración entre industria financiera, entes reguladores y usuarios informados será clave para fortalecer la ciber-resiliencia del sector y mantener la estabilidad y credibilidad en la era de la banca digital.

5.2.4.5 Evidencia cualitativa: percepciones de confianza y reputación

La percepción de los usuarios del sistema bancario chileno frente a la protección de sus datos ha estado marcada por altos niveles de preocupación debido a episodios de vulneración de datos y que organizaciones priorizan sus beneficios por sobre la seguridad de sus clientes.

Con el objetivo de tener una visión general sobre la percepción del uso de datos personales, el Observatorio de Sociedad Digital de la Facultad de Economía y Negocios (FEN) de la Universidad de Chile y la consultora CustomTrigger realizaron el estudio El Ciudadano y su Privacidad, revelando que el 93% de los encuestados se sienten "muy preocupados" por qué organizaciones públicas o privadas utilicen sus datos personales con fines distintos a los autorizados y sólo una cuarta parte de las personas confía en que el sector privado cuide adecuadamente sus datos personales, esto refleja la desconfianza hacia el manejo de la privacidad por parte de las empresas e instituciones. Además, casi 9 de cada 10 chilenos perciben que las organizaciones son las principales beneficiarias del intercambio de datos personales, incrementando esta visión negativa sobre cómo se tratan estos datos. Consecuentemente, muchos usuarios se muestran poco dispuestos a compartir información sensible, donde un 78% se siente "*incómodo*" o "*muy incómodo*" al entregar sus datos a organizaciones, especialmente a través de canales digitales, lo que evidencia una brecha importante de confianza y transparencia entre el público y las entidades que gestionan sus datos privados.

En cuanto a las instituciones financieras, la confianza del público históricamente también ha sido limitada, aunque recientemente con señales de mejora. Según el Ipsos Trustworthiness Monitor 2021, en Chile se presentaba uno de los niveles más bajos de confianza en la banca a nivel global, donde apenas un 18% de los consumidores chilenos consideraba confiables a las empresas bancarias frente a un 28% de promedio mundial, mientras que un 39% las calificaba como poco confiables. Esta desconfianza tiene consecuencias prácticas en la inclusión financiera, donde la principal razón de

quienes no usan productos bancarios en Chile es justamente la falta de confianza en las instituciones financieras (mencionada por un 49% de los encuestados). No obstante, el Índice de Inclusión Financiera 2024 de Credicorp (encuesta regional realizada por Ipsos), se evidencia la recuperación en la reputación del sistema financiero chileno, donde un 46% de los chilenos afirma confiar en las instituciones financieras del país, ocho puntos porcentuales por encima de la medición anterior. Este aumento coincide con avances en inclusión financiera y podría reflejar esfuerzos de la industria por mejorar sus estándares de seguridad y transparencia.

La importancia de la percepción de seguridad para la confianza pública es ampliamente reconocida por autoridades y especialistas, advirtiendo que la confianza depende directamente de esta percepción. La Comisión para el Mercado Financiero ha señalado que "*la confianza de los clientes en las entidades que participan en el mercado financiero es una condición necesaria*" para las personas que están dispuestas a usar productos financieros, también enfatiza que al implementar medidas efectivas de seguridad la confianza en el sistema financiero se fortalece, evidenciando la conexión directa entre gestión de riesgo y confianza pública. Del mismo modo, el Banco Central de Chile advierte que los incidentes de ciberseguridad en bancos o infraestructuras de pago pueden dañar la reputación e incluso romper la confianza de los usuarios en esas instituciones, tras la filtración de datos de Banco Santander en 2024, el SERNAC enfatizó que los consumidores "*tienen derecho a servicios seguros*" y que las empresas deben garantizar la protección de la información personal. Estas declaraciones muestran que la confianza no solo se construye desde la experiencia de los clientes, sino también desde la capacidad regulatoria de generar un entorno seguro y transparente.

5.2.4.6 Evidencia cuantitativa: entorno digital bancario y la necesidad de actualización de la normativa

Cómo se mencionó anteriormente, el sector financiero en Chile ha experimentado una transformación digital acelerada en los últimos años, lo que ha multiplicado tanto las oportunidades como los riesgos. El número de clientes bancarios con acceso en línea se ha incrementado 4,6 veces en diez años, y las transferencias electrónicas de fondos se han multiplicado por 9 en el caso de personas naturales y por 5 en empresas, estos indicadores reflejan la masificación de canales digitales en la banca chilena y un volumen de datos personales sin precedentes circulando por las plataformas financieras. Tal expansión digital amplía la superficie de exposición al riesgo, pues cada nuevo usuario y transacción en línea representan potenciales puntos de ataque o filtración de información.

De forma paralela, la evolución de las amenazas cibernéticas ha tenido una evolución considerable tanto a nivel global como nacional, ya que en los últimos años ha incrementado la sofisticación y

frecuencia de los delitos en línea dirigidos a instituciones financieras. En este sentido, en el informe Global Risks Report 2024 del Foro Económico Mundial ubica a la ciberseguridad entre los principales diez riesgos globales, quedando octavo en 2023 y primero dentro de los riesgos tecnológicos, reflejando la alta probabilidad e impacto de estas amenazas. De igual modo, estudios internacionales reportan miles de intentos de ataque semanales por entidad: en el sector financiero se registraron en 2024 un promedio de 1.510 ataques por empresa a la semana, un 30% más que el año anterior.

En cuanto a el continente local, América Latina tampoco se encuentra ajena a esta tendencia, informes del BID (Banco Interamericano de Desarrollo) y la OEA (Organización de los Estados Americanos) ya advertían en 2020 que la región "*aún no está suficientemente preparada*" para enfrentar los ciberataques, señalando que solo 7 de 32 países contaban por aquel entonces con planes de protección de infraestructura crítica. Asimismo, estos estudios resaltan que los ciberataques en la región han ido en aumento, apuntando principalmente a instituciones financieras. La experiencia que generó la pandemia aceleró la digitalización y dejó aún más evidentes estas vulnerabilidades digitales.

En Chile, las estadísticas de incidentes y fraudes demuestran la urgencia del problema. La CMF reportó 237 incidentes operacionales de alto impacto en la banca solo entre 2015 y 2018, si bien la mayoría de ellos correspondían a fallas tecnológicas o errores operativos, también se registraron eventos de seguridad de la información en los que se puso en riesgo la continuidad de los servicios, los datos de los clientes o la confianza en ciertas entidades bancarias. Más recientemente, el número de fraudes digitales ha aumentado de forma exponencial, un ejemplo son los reclamos de consumidores por fraudes en medios de pago bancarios se duplicaron en un solo año, pasando de 311.000 casos anuales en 2022 a 684.000 en 2023, mientras los montos reclamados escalaron de 108 mil millones a 243 mil millones de pesos chilenos (SERNAC, 2024). Este fenómeno ha tensionado al sistema, cierto aumento puede atribuirse a la mayor conciencia y nuevas normas de protección al usuario, pero también revela que nos encontramos en un entorno plagado de intentos de estafa, phishing y brechas de seguridad que afectan a miles de clientes. De hecho, autoridades chilenas han iniciado acciones colectivas frente a ataques masivos de phishing y han evidenciado que la mayoría de los fraudes bancarios terminan con reclamos no resueltos favorablemente para los usuarios, lo que evidencia desafíos tanto en prevención como en respuesta.

Frente a estas tendencias cuantitativas (creciente digitalización, amenazas al alza, pérdidas económicas por fraudes y eventos de ciberseguridad en el sector) surge la pregunta sobre si las instituciones financieras chilenas tienen el nivel de preparación para enfrentar los posibles riesgos. Si bien el regulador ha tomado medidas importantes, como exigir a los bancos mantener una base de

incidentes de ciberseguridad y reportarlos bajo un estándar común en 2018, las brechas continúan persistiendo. En la Evaluación Internacional de Ciberseguridad de 2020, tanto Chile como buena parte de Latinoamérica quedó rezagado en aspectos claves como la protección de infraestructura crítica y la coordinación frente a incidentes. Hasta hace poco, Chile carecía de una autoridad especializada en protección de datos y operaba bajo un marco legal obsoleto de 1999 (Ley 19.628) que, si bien sentó las bases iniciales, no contemplaba las exigencias del entorno digital actual, esta ley antigua basada en un modelo europeo ya superado, no imponía obligaciones sólidas en seguridad de la información ni otorgaba suficientes derechos a los titulares de datos frente a las nuevas amenazas. En este contexto, la Ley 21.719 de Protección de Datos Personales se presenta como una respuesta necesaria y tardía para modernizar el marco regulatorio, alineando al país con estándares internacionales como el GDPR europeo, creando por primera vez una Agencia Nacional de Protección de Datos y estableciendo obligaciones estrictas de seguridad, reporte de incidentes y responsabilidad proactiva para las organizaciones, debido a que los sectores intensivos en datos personales, en especial el bancario y financiero, venían demandando una actualización normativa de este tipo, necesaria para garantizar los derechos de los titulares y fomentar la confianza en la economía digital.

En definitiva, los datos respaldan de forma contundente la necesidad de una regulación moderna en el entorno bancario digital de Chile. El gran aumento de usuarios y operaciones en línea, junto con el crecimiento de ciberamenazas y fraudes de alto costo, han acabado por situar un panorama de riesgo que no podía seguir siendo abordado con herramientas legales del siglo pasado. Por esto, la Ley 21.719 llega para subsanar las brechas de gobernanza de datos y exigir estándares más elevados de ciberseguridad y protección de la información en las instituciones financieras, algo indispensable para fortalecer la resiliencia del sistema financiero y la confianza de sus millones de usuarios en la era digital.

5.3 Marco teórico del Estado del Arte

5.3.1 Fundamentos de la Protección de Datos

La Ley N°21.719, promulgada en Chile en agosto de 2024, constituye un antes y después en materia de protección de datos personales, ya que reemplaza y actualiza profundamente la antigua Ley N°19.628 de 1999. Su dictación responde a la necesidad de alinear la regulación chilena con los estándares internacionales, particularmente con la normativa europea (Reglamento General de Protección de Datos) y con las exigencias derivadas de la creciente digitalización de los servicios, la masificación de las tecnologías de la información y la expansión del comercio electrónico y de los servicios financieros digitales.

El reconocimiento de los datos personales como un derecho fundamental es uno de los principales avances de la nueva normativa, esto quiere decir mientras la Ley N°19.628 se centraba en regular aspectos operativos del tratamiento de datos, la nueva ley establece explícitamente que la protección de los datos personales forma parte del derecho a la vida privada y a la autodeterminación informativa, otorgando así a las personas una posición reforzada frente a quienes tratan su información. Este cambio de paradigma impone una condición legal obligatoria que debe ser acatada por la totalidad de las entidades incluyendo empresas privadas, organismos públicos y cualquier tipo de organización, afectando directamente la legalidad y legitimidad de sus operaciones.

5.3.1.1 Principios fundamentales de la Ley

Los principios fundamentales del tratamiento de datos personales de la Ley 21.719 constituyen la columna vertebral de la protección de la información y actúan como directrices que deben guiar a los responsables como a encargados de las operaciones del tratamiento en sí. Su cumplimiento se basa en que los datos sean usados de forma ética, segura y transparente, protegiendo con ello la dignidad y los derechos de los individuos.

Además, la Ley incorpora principios que refuerzan la responsabilidad activa de las organizaciones, este cambio de criterio implica que se pase de una fiscalización reactiva (actuación solo tras una denuncia) a una exigencia proactiva que obliga a los responsabas a documentar, gestionar y demostrar formalmente a la Agencia de Protección de Datos Personales que han adoptado y mantienen todas las medidas preventivas de seguridad necesarias para el cumplimiento de la Ley.

La nueva normativa se basa en los siguientes principios esenciales:

1. **Principio de Licitud y Lealtad**: todo tratamiento de datos debe ejecutarse sobre la base de una legitimación previa, es decir, como el consentimiento previo o una obligación contractual o legal. Se exige que al proceder sea de manera transparente, recayendo en el responsable la carga de la prueba para acreditar la validez de la base de licitud utilizada.

2. **Principio de Finalidad**: los datos personales solo pueden ser recopilados para fines específicos, explícitos y claramente definidos. Esto impide que las organizaciones acumulen información sin un objetivo claro o la utilicen para fines distintos a los informados.

3. **Principio de Proporcionalidad**: este principio busca que solo se recopile la cantidad de información personal estrictamente necesaria para cumplir la necesidad declarada.

4. **Principio de Calidad**: obliga al responsable a mantener los datos personales exactos, completos y actualizados, implementando mecanismos eficientes para atender las solicitudes rectificación o supresión por parte del titular.

5. **Principio de Seguridad**: se exige la implementación de medidas técnicas y organizativas rigurosas para proteger los datos contra accesos no autorizados, perdidas o alteración. Este principio se relaciona directamente con la obligación de notificar vulneraciones de seguridad.

6. **Principio de Responsabilidad**: las empresas que manejan datos personales deben asegurarse poder demostrar el cumplimiento de la ley cuando sea necesario. Esto significa que no basta con decir que protegen la información, sino que deben implementar medidas concretas para verificar el cumplimiento de las normas.

7. **Principio de Confidencialidad**: impone que toda la información personal debe manejarse con el máximo nivel de privacidad y protección, esto significa que quienes tienen acceso a los datos están obligados a evitar filtraciones, usos indebidos o divulgaciones no autorizadas.

8. **Principio de Seguridad**: las organizaciones deben adoptar medidas técnicas y organizativas para proteger los datos contra accesos no autorizados, pérdidas o filtraciones.

9. **Principio de Transparencia e Información**: los titulares tienen derecho a saber qué datos suyos están siendo utilizados, con qué propósito y quién los maneja. Por eso, las empresas deben informar de manera clara, gratuita y accesible cómo tratan la información personal.

Esto permite que los usuarios tomen decisiones informadas sobre si quieren o no compartir sus datos.

5.3.1.2 Derecho de los titulares (ARSOP)

Otro pilar fundamental es el derecho de los titulares a controlar sus datos personales, la Ley N°21.719 amplía y fortalece los derechos ya existentes bajo la legislación anterior, integrando tanto los derechos tradicionales ARCO (acceso, rectificación, cancelación y oposición) como derechos emergentes que responden a los desafíos del entorno digital:

- **Derecho de Acceso**: es el derecho del titular a solicitar y obtener confirmación acerca de si los datos personales que le conciernen están siendo tratados por una organización.

- **Derecho de Rectificación**: es el derecho a solicitar la modificación de los datos objeto de tratamiento por parte de una organización, que sean inexactos, incompletos o que estén desactualizados.

- **Derecho de Supresión**: es el derecho a la eliminación de los datos personales que en cada caso corresponda, en las circunstancias siguientes:

    - Cuando los datos no resulten necesarios en relación con los fines del tratamiento para el cual fueron recogidos.
    - Cuando el titular haya revocado su consentimiento para el tratamiento y éste no tenga otro fundamento regulatorio.
    - Cuando los datos hayan sido obtenidos o tratados ilícitamente por el responsable.
    - Cuando se trate de datos caducos.
    - Cuando los datos deban suprimirse para el cumplimiento de una sentencia judicial, o de una obligación legal.
    - Cuando el titular haya ejercido su derecho de oposición de conformidad a la ley y no existan otro fundamento legal para su tratamiento.

- **Derecho de Oposición**: es el derecho que permite negarse al uso de los datos en determinadas circunstancias, los principios de proporcionalidad y finalidad respaldan este derecho, evitando que la información se use para fines distintos a los informados o que causen daños.

- **Derecho de Portabilidad**: derecho que concede recibir en un formato estructurado, de uso común y de lectura mecánica, una copia de los datos personales que haya sido facilitado a un responsable del tratamiento, con el finde transmitirlos a otro responsable del tratamiento.

5.3.2 Obligaciones de las instituciones financieras

Las instituciones financieras son uno de los sectores que manejan mayor cantidad de datos personales de relevancia estratégica, debido a su volumen y la sensibilidad de la información que gestionan, por lo que la Ley N°21.719 introduce un conjunto de obligaciones específicas para los responsables y encargados del tratamiento de datos personales. Estas obligaciones no solo buscan garantizar la legalidad del tratamiento de datos, sino también fortalecer la confianza pública en un sector cuya estabilidad depende en gran medida de la reputación y de la seguridad de sus operaciones.

En primer lugar, la ley establece que cada institución tiene la obligación de designar un **Delegado de Protección de Datos (DPO)** o responsable de cumplimiento en protección de datos, esta figura debe contar con independencia funcional y conocimientos especializados, y su tarea principal es supervisar la aplicación de la normativa dentro de la institución, asesorar en políticas y procedimientos de protección de datos, y actuar como punto de contacto con la autoridad de control y con los titulares de los datos. La incorporación del DPO representa un cambio cultural significativo para las instituciones financieras, ya que implica profesionalizar la gestión de la privacidad y elevarla al nivel de la gobernanza corporativa.

También, la normativa exige la implementación de medidas técnicas y organizativas adecuadas de seguridad, orientadas a prevenir accesos no autorizados, pérdidas o alteraciones de datos. En el pasado este deber se trataba de forma general en la Ley N°19.628, ahora se especifica con mayor detalle, incorporando principios como la seguridad desde el diseño y por defecto, que obliga a entregar la protección de datos en todas las fases de desarrollo de productos y servicios financieros. Para la banca, esto significa incorporar estándares de seguridad en aplicaciones móviles, sistemas de inteligencia artificial, Big Data y plataformas digitales, de esta manera se asegura la confidencialidad e integridad de la información.

Otra obligación es la de realizar **Evaluaciones de Impacto en la Privacidad (DPIA)** en los casos en que el tratamiento pueda implicar un alto riesgo para los derechos de los titulares. Este requisito resulta especialmente relevante en instituciones financieras, donde el uso de tecnologías como biometría, analítica predictiva o sistemas automatizados de decisión crediticia puede generar afectaciones significativas a la privacidad. Las DPIA actúan como un instrumento preventivo que

obliga a identificar riesgos, proponer medidas de mitigación y documentar el proceso de toma de decisiones.

La ley también impone el deber de notificar las brechas de seguridad tanto a la autoridad de control como a los titulares de los datos afectados, este punto responde a una de las carencias más criticadas de la Ley N°19.628, que no obligaba a informar filtraciones ni ciberataques. En la práctica, esta obligación refuerza la transparencia y permite a los clientes financieros tomar medidas de resguardo frente a potenciales fraudes, a la vez que eleva la presión reputacional sobre las instituciones para invertir en sistemas de prevención eficaces.

Así mismo, las instituciones deben mantener un registro actualizado de sus actividades de tratamiento, lo que implica llevar inventarios detallados de los datos que administran, las finalidades de su uso, los destinatarios y los plazos de conservación. Esta obligación de trazabilidad permite a la autoridad fiscalizar de manera más efectiva y asegura que las instituciones tengan un control interno sobre sus prácticas de gestión de datos.

Además de estas disposiciones centrales, la Ley N°21.719 introduce obligaciones adicionales que refuerzan el marco de cumplimiento:

- Elaborar y difundir una política interna de protección de datos, aplicable a todos los trabajadores y procesos de la institución.
- Realizar evaluaciones periódicas de cumplimiento, incluyendo auditorías internas y externas, con el fin de detectar brechas y proponer mejoras continuas.
- Implementar programas de capacitación y concientización para los trabajadores que traten datos personales, dado que una parte importante de los incidentes se origina en errores humanos.
- Responder bajo un esquema de responsabilidad solidaria cuando intervienen terceros en el tratamiento, lo que obliga a la banca a ejercer control estricto sobre sus proveedores y socios estratégicos.

De forma conjunta, estas obligaciones redefinen el marco de actuación de las instituciones financieras, trasladando el cumplimiento normativo desde un enfoque reactivo hacia uno proactivo y demostrable (accountability). El cumplimiento ya no se limita a evitar sanciones, sino que constituye un requisito indispensable para sostener la confianza de los clientes y asegurar la resiliencia institucional en un entorno marcado por la digitalización y las amenazas cibernéticas.

5.3.3 Autoridad de control y régimen sancionatorio

En esta nueva Ley, la protección de datos ya no depende únicamente de las buenas prácticas de las instituciones, una de las creaciones más relevantes es la de la **Agencia de Protección de Datos Personales**, el cual es un organismo autónomo de derecho público, de carácter técnico y descentralizado. Su objetivo principal es velar por le efectiva protección de los derecho de la vida privada de las personas y sus datos personales, fiscalizando el cumplimiento efectivo de la ley. Hasta antes de su promulgación, Chile carecía de una autoridad independiente con competencias específicas en esta materia, lo que constituía una de las principales debilidades del antiguo marco legal. Esta carencia había dejado en manos de los propios titulares de datos la tarea de iniciar acciones judiciales frente a infracciones, lo que en la práctica reducía drásticamente el nivel de protección y fiscalización.

La Agencia tiene un diseño institucional que le otorga facultades de supervisión, fiscalización y sanción. Entre sus competencias principales se encuentran:

- Monitorear y fiscalizar el cumplimiento de la Ley N°21.719 por parte de responsables y encargados de tratamiento.
- Dictar directrices, guías y recomendaciones técnicas sobre buenas prácticas en materia de protección de datos.
- Exigir información y documentación a las instituciones que traten datos personales, incluidas las financieras, con el fin de verificar su adecuación normativa.
- Investigar denuncias presentadas por titulares y actuar de oficio frente a incidentes de gran relevancia.
- Aplicar sanciones administrativas proporcionales a la gravedad de las faltas.

En relación con el régimen sancionatorio, la ley establece un sistema escalonado que clasifica las infracciones en leves, graves y gravísimas, con multas que pueden alcanzar hasta 20.000 UTM**.** Este rango representa un salto significativo en comparación con las sanciones de la antigua Ley N°19.628, que eran bajas y carecían de efecto disuasorio real. Para las instituciones financieras, este endurecimiento implica que los incumplimientos ya no se perciben como un costo marginal asumible, sino como un riesgo económico y reputacional de gran envergadura.

Tabla 1. Clasificación de Sanciones

Tipo	Descripción	Multas aplicables
Leves	Corresponden a incumplimientos de carácter administrativo o formal, que no afectan de manera directa y significativa los derechos de los titulares de datos. Incluyen faltas menores de registro, información o plazos, donde el daño potencial es acotado.	**Hasta 5.000 UTM (MM$343)**
Graves	Comprenden incumplimientos que suponen una amenaza directa a la seguridad y legalidad del tratamiento de datos. Incluyen la ausencia de medidas de resguardo, la falta de un responsable de protección de datos o el tratamiento sin base legal válida, cuando no existe afectación masiva.	**500 a 10.000 UTM (MM$686)**
Gravísimas	Constituyen vulneraciones de máxima severidad, en las que los derechos de los titulares son comprometidos de forma masiva o deliberada. Se incluyen prácticas de comercialización ilícita de datos, el ocultamiento de brechas de seguridad con gran impacto y la reincidencia en infracciones graves.	**1.000 a 20.000 UTM (MM$1.373)**

Elaboración propia

En caso de reincidencia de infracciones graves o gravísimas, las multan pueden triplicarse o incluso alcanzar hasta el 2% o 4% de las ventas netas anuales, y ordenar la suspensión del tratamiento por 30 días (renovable).

Están sanciones introducen multas de magnitudes inéditas en el ordenamiento chileno, en el sector financiero las instituciones manejan millones de datos sensibles, por lo tanto, una infracción gravísima puede equivaler a sanciones millonarios que no solo impactan en lo económico, sino también pueden generar un efecto reputacional devastador. Añadir que las sanciones no sólo se limitan a multas, la Agencia puede ordenar la suspensión temporal de operaciones del tratamiento correspondiente, la eliminación de bases de datos obtenidas de forma ilícita e incluso la publicidad de la sanción, lo que añade un componente reputacional de alto impacto. En el caso del sector bancario, donde la confianza del cliente es un activo crítico, la exposición pública de una sanción podría tener consecuencias en la fidelización, en el acceso a mercados y en la competitividad frente a actores más cumplidores.

Por lo tanto, la creación de la Agencia de Protección de Datos y el establecimiento de un régimen sancionatorio robusto marcan un punto de inflexión en la cultura de cumplimiento del sistema financiero chileno, donde el cumplimiento normativo deja de ser voluntario y pasa a convertirse en una obligación supervisada por una autoridad con competencias efectivas, lo que eleva las exigencias regulatorias y consolida la protección de los derechos de los titulares en un sector altamente expuesto a riesgos tecnológicos.

5.3.4 Comparación con el GDRP y otras referencias internacionales

La Ley N°21.719 se inserta dentro de una tendencia internacional de fortalecimiento de la protección de datos personales, inspirada principalmente en el **Reglamento General de Protección de Datos (GDPR)** de la Unión Europea, aunque también considera elementos de marcos latinoamericanos como la Ley General de Protección de Datos de Brasil (LGPD) y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México. Esta comparación permite identificar fortalezas, diferencias y lecciones aplicables al contexto chileno.

Respecto a los derechos de los titulares de los datos, tanto la Ley 21.719 como el GDPR coinciden en la mayoría de los aspectos fundamentales, como acceso, rectificación, cancelación y oposición, pero también se incorporan facultades modernas como la portabilidad de los datos, la posibilidad de solicitar la eliminación de información en ciertos contextos y el derecho a ser informado oportunamente en caso de brechas de seguridad. Ambos marcos normativos exigen la designación de un Delegado de Protección de Datos (DPO), la realización de Evaluaciones de Impacto en la Privacidad (DPIA) en casos de alto riesgo y la implementación de políticas internas de protección de datos. Asimismo, se establece la obligación de notificar a la autoridad y a los titulares en caso de incidentes que comprometan la información personal, una obligación que en Chile constituye un cambio fundamental respecto del marco anterior. Este enfoque preventivo y de transparencia se inspira directamente en el modelo europeo, pero también encuentra paralelos en experiencias regionales como la Ley General de Protección de Datos Personales de Brasil (LGPD), que desde 2018 introdujo principios y obligaciones similares.

En cuanto a la autoridad de control, ambos marcos contemplan organismos independientes encargados de supervisar y fiscalizar el cumplimiento de la normativa. En Europa, cada Estado miembro cuenta con una autoridad nacional de protección de datos, mientras que en Chile se ha creado la Agencia de Protección de Datos Personales, con facultades para realizar inspecciones,

auditorías y sancionar incumplimientos, garantizando que la protección de los datos sea efectiva y verificable.

En lo relativo al régimen sancionatorio, las similitudes con el GDPR son notorias aunque con diferencias en magnitud, debido a que mientras la normativa europea prevé multas que alcanzan hasta 20 millones de euros o el 4% de la facturación global de la empresa, la Ley N°21.719 establece sanciones que van desde infracciones leves con multas de hasta 500 UTM, hasta infracciones gravísimas con sanciones que pueden llegar a 20.000 UTM. Aunque en términos absolutos las sanciones chilenas son menores, en el contexto local representan un cambio sustancial al elevar los costos del incumplimiento a niveles nunca antes vistos en materia de privacidad.

Desde la perspectiva del sector financiero, la experiencia europea demuestra que el cumplimiento del Reglamento General de Protección de Datos ha obligado a los bancos a implementar medidas avanzadas de ciberseguridad, políticas internas de privacidad y programas integrales de cumplimiento normativo. La Ley 21.719 permite que las instituciones financieras chilenas adopten buenas prácticas internacionales, fortaleciendo la confianza de clientes e inversionistas y asegurando la interoperabilidad con estándares globales.

Además, la creación de la Agencia de Protección de Datos Personales en Chile responde al mismo esquema institucional del GDPR y de la LGPD en Brasil, al dotar al país de una autoridad independiente con facultades de fiscalización, supervisión y sanción. Este avance corrige una de las principales debilidades del régimen anterior, donde no existía una entidad dedicada exclusivamente a la protección de datos.

En conclusión, la Ley N°21.719 se posiciona como un marco normativo alineado con los estándares internacionales más avanzados en la materia. Si bien existen diferencias de escala y de capacidades institucionales, la estructura general de principios, derechos, obligaciones y sanciones sigue de cerca el modelo europeo, a la vez que incorpora lecciones de otras jurisdicciones regionales como Brasil y México. Esta convergencia normativa permitirá a Chile no solo reforzar la protección de los datos personales a nivel interno, sino también favorecer la interoperabilidad internacional en el intercambio de información y servicios financieros digitales, un aspecto crucial en un mercado globalizado.

5.3.5 Retos del cumplimiento de la Ley 21.719

La implementación de la Ley N°21.719 representa un desafío significativo y con retos multidimensionales para las instituciones financieras, que van más allá del cumplimiento legal y exigen cambios estructurales en su gobernanza, procesos y cultura organizacional.

Uno de los principales retos es la adaptación institucional y cultural, ya que la Ley exige que la gestión de datos personales se integre dentro de la gobernanza corporativa y que todas las áreas, desde desarrollo tecnológico hasta atención al cliente, internalicen la importancia de la privacidad y la seguridad. Esto implica modificar procesos internos, establecer protocolos claros, capacitar al personal y garantizar que la cultura de cumplimiento no sea solo formal, sino operativa y permanente. La creación de la figura del Delegado de Protección de Datos supone no solo un cargo técnico, sino la instauración de una cultura de privacidad en toda la organización. En este sentido, los bancos y compañías financieras deberán superar la visión de que la protección de datos es un requisito "formal" y pasar a considerarla un eje estratégico de confianza y reputación, tal como ocurre en mercados más avanzados.

Continuando con el desafío cultural, se tiene en cuenta que al introducirse un enfoque proactivo y de responsabilidad demostrable (accountabilitty), el cual obliga a las instituciones a documentar todas sus actividades de tratamiento, realizar evaluaciones de riesgos y notificar brechas de seguridad de manera inmediata, representa un tanto cambio cultural como operativo frente a la normativa anterior, donde el cumplimiento era en gran medida reactivo y poco verificable. La necesidad de mantener registros actualizados y de responder a posibles auditorías de la autoridad de control requiere recursos humanos y tecnológicos adicionales, así como una coordinación interdepartamental constante.

Otro desafío clave es de carácter tecnológico y operativo, debido a que la banca maneja sistemas complejos e interconectados, como plataformas de pago, aplicaciones móviles, analítica de datos y servicios en la nube, donde la minimización de datos, la seguridad por diseño y las evaluaciones de impacto deben integrarse desde el inicio. Sin embargo, gran parte de la infraestructura existente fue concebida bajo lógicas de negocio anteriores, con acumulación de grandes volúmenes de datos y sin criterios de depuración o segmentación estricta. La transición hacia esquemas que privilegien la retención limitada y la trazabilidad representa un reto técnico que demandará inversiones significativas en infraestructura, auditorías de sistemas, evaluaciones de impacto en la privacidad, mecanismos de trazabilidad y coordinación con proveedores externos. Para muchas instituciones, equilibrar eficiencia operativa y cumplimiento normativo puede ser complejo y costoso.

También, otro desafío es el regulatorio y de supervisión, ante la creación de la Agencia de Protección de Datos Personales introduce un nuevo actor fiscalizador que se suma a los ya existentes, como la CMF, SERNAC y Banco Central, esto implica que las instituciones financieras deberán aprender a coordinar el cumplimiento de múltiples autoridades, con marcos normativos que a veces se superponen o incluso pueden entrar en tensión. Por lo tanto, esta situación exige un esfuerzo adicional de armonización regulatoria interna y de generación de reportes que respondan a distintos requerimientos.

En cuento a la gestión de incidentes y comunicación con clientes, es un nuevo reto debido a la obligación de notificar brechas de seguridad a la Agencia y a los titulares cambia radicalmente la manera en que se manejan los incidentes de ciberseguridad. Ya no basta con contener el ataque o la filtración; ahora las instituciones deberán comunicar de forma clara, rápida y transparente lo ocurrido, sus consecuencias y las medidas de mitigación. En un sector donde la confianza del cliente es el principal activo, una mala gestión comunicacional puede resultar más costosa que la propia multa, configurando un reto reputacional de primera magnitud.

Finalmente, el reto más transversal es garantizar la sostenibilidad del cumplimiento, teniendo como referencia la experiencia internacional, especialmente en Europa tras la entrada en vigor del GDPR, demuestra que la adaptación inicial es solo el primer paso y el verdadero desafío consiste en mantener el cumplimiento en el tiempo, con capacitación continua del personal, auditorías periódicas, métricas de desempeño y actualización tecnológica. En este contexto, las instituciones financieras chilenas deben construir capacidades internas que les permitan responder no solo a la Ley N°21.719, sino también a futuras exigencias regulatorias que puedan surgir en un entorno de innovación digital acelerada.

En síntesis, los retos del cumplimiento de la Ley N°21.719 no se limitan a la incorporación de nuevas políticas o tecnologías, sino que requieren una transformación organizacional integral que abarque cultura, procesos, tecnología, regulación y comunicación, configurando un desafío estratégico para todo el sistema financiero chileno.

6) METODOLOGÍA DE LA INVESTIGACIÓN

6.1.1 Tipo de investigación

Para este estudio se utilizó un enfoque cualitativo, ya que se busca analizar y comprender el impacto de la Ley N°21.719 sobre Protección de Datos Personales genera en las instituciones financieras chilenas y proponer un plan de acción estratégico que facilite su cumplimiento efectivo.

El estudio se enfoca en comprender cómo los cambios normativos inciden en la gestión de datos personales dentro del sistema financiero, evaluando su efecto en materia de gobernanza, transparencia, seguridad de la información y responsabilidad corporativa. Asimismo, se pretende desarrollar lineamientos estratégicos que fortalezcan la cultura de cumplimiento y la confianza pública en el sector financiero.

6.1.2 Enfoque metodológico

El estudio se sustenta en una metodología de **benchmarking estratégico comparativo**, enfocado en contrastar el marco legal chileno con modelos internacionales consolidados, particularmente el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, el cual es considerado el estándar internacional más avanzado en materia de protección de datos personales. Este enfoque permite identificar semejanzas, diferencias y buenas prácticas aplicables al contexto nacional, con el fin de orientar la formulación del plan de acción.

El análisis se centra en documentos normativos, más que en datos cuantitativos, lo que permite evaluar el grado de alineamiento normativo de Chile frente al estándar internacional y los desafíos que enfrentan las instituciones financieras en gobernanza de datos, ciberseguridad y transparencia.

Además, se incorpora una **evaluación de viabilidad económica**, orientada a determinar si la implementación del plan de acción propuesto resulta financieramente sostenible para las instituciones. Para ello, se comparan los costos de adopción de medidas de cumplimiento (creación de cargos especializados, la inversión en softwares, capacitaciones o auditorías externas, etc.) con

los costos del incumplimiento (sanciones de hasta 20.000 UTM, impactos reputacionales y pérdida de confianza).

A continuación, se presentan las etapas:

1. Diagnóstico inicial: revisión del estado actual de las políticas y prácticas de las políticas y prácticas de protección de datos.
2. Identificación de obligaciones y brechas: análisis de la Ley 21.719 y comparación con la normativa anterior.
3. Benchmarking normativo: contraste con GDRP para definir buenas prácticas.
4. Evaluación económica: análisis costo beneficio entre cumplimiento e incumplimiento.
5. Diseño del plan de acción: propuesta estructurada con ejes estratégicos.

En síntesis, la metodología aplicada integra análisis cualitativo, benchmarking normativo y evaluación económica para garantizar la coherencia y viabilidad del plan propuesto. La combinación de estas herramientas permite fundamentar recomendaciones alineadas con estándares internacionales, aplicables al contexto chileno y sostenibles en el tiempo, asegurando que el cumplimiento de la Ley N°21.719 se aborde como una estrategia integral y no solo como una obligación legal.

7) APLICACIÓN METODOLÓGICA

La entrada en vigencia de la Ley N°21.719 moderniza el marco de protección de datos en Chile y tiene un impacto especialmente relevante en las instituciones financieras, ya que su operación depende del uso intensivo de datos personales. La normativa introduce nuevos derechos, obligaciones y sanciones que obligan al sector a ajustar procesos internos, fortalecer la gobernanza de datos y elevar los estándares de ciberseguridad.

Debido a lo anterior, se vuelve imprescindible analizar cómo otros marcos normativos internacionales han abordado desafíos similares en la protección de datos de sus ciudadanos. En particular, el del Reglamento General de Protección de Datos (GDPR) de la Unión Europea, debido a que este es el estándar global más consolidado y exigente en materia de protección de datos personales.

El análisis comparativo entre ambas normativas constituye una parte central de este trabajo, ya que permite identificar las principales buenas prácticas, coincidencias, divergencias y oportunidades de aprendizaje que pueden guiar la implementación efectiva de la nueva Ley N°21.719 en el sistema

financiero. A través de esta metodología de benchmarking, se busca no solo contrastar los marcos regulatorios, sino también detectar prácticas consolidadas en materia de gobernanza, gestión del riesgo y protección de datos que puedan ser adaptadas al contexto nacional. Asimismo, este análisis comparativo ofrece a las instituciones financieras una referencia clara respecto de los niveles de cumplimiento que podrían ser necesarios para alcanzar estándares internacionales, anticipando riesgos, brechas y oportunidades de mejora

En términos generales, la Ley N°21.719 se inspira directamente en los principios, estructuras y mecanismos del GDPR, con el objetivo de alinear a Chile con los estándares internacionales de privacidad y protección de la información. Ambos cuerpos normativos comparten los fundamentos de licitud, finalidad, proporcionalidad, seguridad, transparencia y responsabilidad proactiva, lo que evidencia una convergencia sustantiva en la orientación regulatoria. Sin embargo, el grado de desarrollo institucional y la madurez operativa del modelo europeo aún representan un desafío importante para el contexto chileno.

En el caso del GDPR, el cumplimiento se estructura sobre una arquitectura de gobernanza sólida, que incluye la figura del Delegado de Protección de Datos (DPO), la obligación de realizar Evaluaciones de Impacto en Privacidad (DPIA) en tratamientos de alto riesgo, la notificación obligatoria de incidentes dentro de 72 horas, y un régimen sancionatorio de alcance global, con multas que pueden alcanzar el 4% de la facturación anual. Estos elementos configuran un sistema robusto, preventivo y de rendición de cuentas permanente, en el que las empresas deben demostrar en todo momento la trazabilidad y legitimidad de sus decisiones sobre el tratamiento de datos personales.

Por su parte, la Ley N°21.719 replica la mayoría de estos principios y estructuras, aunque con un grado de desarrollo adaptado a la realidad institucional chilena. La nueva ley introduce, por primera vez, la figura del Delegado de Protección de Datos (DPO), la obligación de mantener registros de actividades de tratamiento, la realización de Evaluaciones de Impacto en Privacidad (DPIA), la notificación de brechas de seguridad y la creación de una Agencia de Protección de Datos Personales como autoridad de control independiente. Además, establece un sistema de sanciones escalonado (infracciones leves, graves y gravísimas) con multas que pueden alcanzar montos significativamente altos, lo que representa un avance sustancial respecto del marco anterior (Ley N°19.628).

No obstante, persisten brechas relevantes en aspectos operativos, ya que la legislación chilena aún no define plazos exactos para la notificación de incidentes, ni procedimientos detallados para las transferencias internacionales de datos o para las decisiones automatizadas. Estos elementos serán precisados mediante los reglamentos complementarios que deberá dictar la nueva Agencia de

Protección de Datos. Por su parte, el GDPR ya cuenta con un desarrollo bien detallado y con una interpretación muy desarrollada, reforzado por guías, criterios y decisiones emitidas por la autoridad europea y los tribunales comunitarios, ofreciendo reglas más claras y una mayor previsibilidad para quienes deben cumplirlo.

En cuanto a la aplicación práctica en el sector financiero, el GDPR ha demostrado que la implementación de políticas de privacidad integrales genera beneficios concretos en la reducción de riesgos reputacionales y en el fortalecimiento de la confianza del consumidor. Según London Economics, el cumplimiento de las normativas impuestas por el GDRP provoca un incremento de la confianza del consumidor, convirtiéndose en una ventaja competitiva para las organizaciones que lo aplican correctamente, al demostrar transparencia y responsabilidad en la gestión de datos. Asimismo, Deloitte señala que el GDRP debe considerarse como una oportunidad estratégica para evolucionar modelos de negocio y fortalecer la relación con los clientes, ya que la protección de datos reduce riesgos reputacionales y consolida la credibilidad corporativa. Estos hallazgos evidencian que la privacidad no es solo un requisito legal, si no un factor clave para la sostenibilidad y competitividad en el sector financiero. En cuanto a Chile, la adopción de un enfoque similar requerirá incorporar la privacidad como parte del modelo de gestión de riesgos, integrando las funciones de cumplimiento, auditoría, tecnología y gobierno corporativo. Las instituciones deberán crear estructuras internas estables, encabezadas por el Delegado de Protección de Datos, con autonomía y recursos suficientes, además de definir métricas e indicadores que permitan evaluar la efectividad del cumplimiento.

Otro aprendizaje relevante derivado del GDPR es la importancia del principio de privacidad desde el diseño y por defecto (*privacy by design and by default*), el cual establece que la protección de datos debe incorporarse desde el desarrollo de los procesos y sistemas tecnológicos, y no como una medida posterior. Este enfoque es particularmente relevante para el sistema financiero, que depende de plataformas digitales, inteligencia artificial y analítica de datos para operar. La Ley N°21.719 recoge este principio, lo que implicará que los bancos y entidades financieras deban revisar su arquitectura tecnológica, establecer controles de acceso más estrictos y fortalecer sus políticas de ciberseguridad.

Por último, el régimen sancionatorio también presenta diferencias sustanciales. Aunque las multas del GDPR son cuantitativamente más elevadas, el impacto económico y reputacional que puede tener una infracción a la Ley N°21.719 en Chile es igualmente significativo. Además, la nueva ley contempla la **publicación de las sanciones**, lo que agrega un componente reputacional que incentiva el cumplimiento preventivo. En este sentido, la evaluación realizada en el presente estudio demuestra que, para las instituciones financieras, invertir en cumplimiento proactivo resulta más eficiente y

sostenible que asumir los costos de las sanciones o el daño reputacional derivado de un incumplimiento.

En síntesis, el benchmarking estratégico confirma que la Ley N°21.719 se encuentra ampliamente alineada con el GDPR, tanto en sus principios como en su estructura regulatoria. Las brechas identificadas no representan retrocesos, sino etapas pendientes de desarrollo que dependerán de la madurez institucional de la futura autoridad y de la capacidad de las organizaciones para adaptar sus procesos internos.

8) RESULTADOS FINALES

8.1.1 Impactos operacionales

La nueva ley exige a las instituciones financieras revisar y adecuar sus procesos de tratamientos de datos. Los principales efectos operacionales son:

- **Revisión y documentación de flujos de datos**: esto significa que se debe realizar un mapeo de cómo se están recopilando, usando, almacenando y compartiendo la información entre las áreas, desde el primer momento en la atención al cliente hasta la última instancia de eliminación del dato.

- **Fortalecimiento de medidas de seguridad**: tiene que haber un aumento significativo de las exigencias de los procesos de recepción, monitoreo, gestión de incidentes y control de accesos.

- **Atención de los nuevos derechos de los titulares**: esto provoca la creación de canales para la recepción, protocolos y plazos formales para las solicitudes de los derechos ARSOP.

Estos cambios generan un aumento de la carga operativa y requieren coordinación entre las distintas áreas internas.

8.1.2 Impactos estratégicos

La protección de datos deja de ser sólo un tema técnico y pasa a ser un elemento estratégico dentro del gobierno corporativo. Los principales efectos son los siguientes:

- **Creación del Delegado de Protección de Datos (DPO)**: este es una nueva figura que al tener autonomía de supervisión eleva el cumplimiento al nivel directivo.

- **Necesidad de una cultura organizacional orientada a la privacidad**: esto implica que se implementen capacitaciones transversales y nuevas políticas internas.

- **Ajustes en iniciativas tecnológicas y de innovación**: los modelos basados en Big Data, analítica y automatización deben alinearse con principios como minimización de datos y transparencia.

8.1.3 Impactos financieros

El impacto económico es uno de los más relevantes, dado que la ley incorpora multas significativamente más altas que la normativa anterior. Esto provoca:

1. **Aumento del costo de cumplimiento**: la implementación de la ley implica un incremento significativo en los costos operacionales de las empresas, especialmente para aquellas que no presentan un sistema solido de ciberseguridad. Estos costos pueden incluir:

    - **Inversiones tecnológicas**: adquisición o actualización de sistemas de seguridad, herramientas de monitoreo continuo, sistemas de detección y respuesta a incidentes, cifrado de datos, entre otros.

    - **Servicios de auditorías y consultorías**: algunas organizaciones requieren apoyo externo para evaluar brechas, definir los planes de acción, implementar controles o validar el cumplimiento de la normativa.
    - **Capacitación obligatoria para los colaboradores**: se tiene que capacitar al personal en cuanto a buenas prácticas de ciberseguridad y respuesta a incidentes, lo cual lleva tiempo, recursos y continuidad.
    - **Contratación de personal especializado**: como responsables de ciberseguridad, analistas o equipos dedicados a la gestión y reporte de incidentes.

En conjunto, estos gastos pueden representar una carga significativa, especialmente para empresas pequeñas o medianas, que deben equilibrar el cumplimiento normativo con sus limitados recursos financieros.

2. **Riesgo financiero por sanciones**: la ley establece multas históricamente altas en Chile para las infracciones graves y gravísimas, lo que genera un riesgo financiero considerable para las

organizaciones. Si bien los bancos tradicionales poseen mayor capacidad financiera, otras entidades reguladas, como Fintech, cooperativas de ahorro y crédito, cajas de compensación o emisores de prepago, podrían enfrentar serias dificultades para absorber sanciones de alto monto. Dependiendo de la magnitud de la infracción y del tamaño de la institución, una multa muy alta podría comprometer su solvencia, provocar la necesidad de recapitalización urgente, afectar su liquidez o incluso generar riesgos de cierre o disolución.

Aunque la disolución no es explícitamente la consecuencia jurídica directa de la ley, sí puede materializarse como un efecto económico indirecto, especialmente en empresas cuya estructura financiera es frágil o tiene margen reducido para contingencias.

Esto se debe a que:

- Las multas deben pagarse incluso cuando afectan la continuidad del negocio.
- Los incidentes graves suelen incluir costos adicionales (consultorías, medidas correctivas, refuerzo de seguridad).
- La pérdida de confianza de los consumidores puede generar una fuga de clientes.
- Los reguladores financieros pueden exigir medidas estrictas de corrección que pueden incrementan los gastos.

Además, las sanciones no son solo económicas, la Ley también contempla:

- Suspensión parcial de actividades de tratamiento.
- Prohibición temporal de ciertos procesos.
- Obligación de eliminar bases de datos obtenidas ilícitamente.
- Medidas correctivas impuestas por la Agencia de Protección de Datos.

Estas consecuencias pueden traducirse en pérdidas operacionales significativas, disminución de ingresos y dificultades para mantener la continuidad del negocio, afectando directamente la estabilidad financiera de la institución.

8.1.4 Impacto Comercial

La Ley de Protección de Datos Personales introduce un cambio significativo en la forma en que las organizaciones chilenas gestionan la información, con efectos directos en su competitividad, reputación y oportunidades de negocio.

Este impacto se refleja en tres áreas clave:

- **Competitividad y Posicionamiento:**

La adopción de estándares alineados con normativas internacionales, como el GDRP, provoca un fortalecimiento de las empresas chilenas en mercados globales. Al cumplir con la ley permite facilitar transferencias internacionales de datos, requisito esencial para operar en entornos digitales y colaborar con socios extranjeros. Las organizaciones que se adapten rápidamente podrán convertir la protección de datos en una ventaja competitiva, diferenciándose al ofrecer mayor transparencia y confianza.

- **Reputación y confianza del cliente:**

En un contexto donde la privacidad es un valor creciente, la implementación efectiva de la ley significa una mayor credibilidad y fidelización. Las instituciones financieras, que manejan información sensible para sus procesos, pueden reforzar su imagen como actores responsables, lo que impacta directamente en la retención de clientes y en la atracción de nuevos segmentos que priorizan la seguridad de sus datos.

- **Nuevas oportunidades de negocio:**

La normativa impulsa la creación de modelos de gobernanza de datos y abre espacio para el desarrollo de servicios especializados en ciberseguridad, consultoría legal y soluciones tecnológicas. Además, fomenta la innovación de productos financieros basados en datos, siempre bajo un marco regulatorio que garantice la protección y el consentimiento informado.

La nueva normativa no solo representa un desafío regulatorio, sino también una oportunidad estratégica para que las empresas chilenas fortalezcan su reputación, accedan a mercados internacionales y desarrollen ventajas competitivas basadas en la confianza digital. Aquellas organizaciones que integren la protección de datos como parte de su propuesta de valor estarán mejor posicionadas en un entorno cada vez más exigente y globalizado.

8.1.5 Propuesta Plan de Acción

El plan de acción tiene como finalidad establecer las medidas estratégicas, operativas y tecnológicas necesarias para garantizar el cumplimiento efectivo de la nueva Ley N°21.719 en las instituciones financieras. Este documento se fundamenta en el análisis previo del impacto normativo y en la identificación de brechas críticas que podrían comprometer la seguridad de la información y la confianza de los clientes.

El plan propone un conjunto de acciones concretas orientadas a fortalecer la gobernanza de datos, implementar protocolos de privacidad, optimizar la infraestructura tecnológica y promover una cultura organizacional basada en la protección de la información. Su alcance abarca todas las áreas involucradas en el tratamiento de datos personales, desde el momento en que se reciben en atención al cliente hasta su almacenamiento, procesamiento, transmisión y eventual eliminación, asegurando que cada etapa cumpla con los principios de licitud, transparencia y seguridad, considerando los plazos establecidos por la normativa y los estándares internacionales en materia de privacidad y ciberseguridad.

8.1.5.1 Alcance y Objetivos del Plan

El alcance del plan de acción engloba todas las áreas y procesos internos de las instituciones financieras que intervienen en el tratamiento de datos personales, incluyendo la gestión tecnológica, la atención al cliente, la gobernanza corporativa y la relación con terceros (proveedores). El plan se orienta a garantizar la adecuación normativa antes de la entrada en vigor de la ley en diciembre de 2026, asegurando que las entidades financieras adopten medidas preventivas y correctivas que reduzcan riesgos legales, operativos y reputacionales.

Es importante destacar que el plan no ejecuta no desarrolla las acciones operativas, sino que establece las directrices y recomendaciones estratégicas que las instituciones deberán implementar para cumplir con la normativa.

Los objetivos específicos del plan son:

- Proponer una estructura de gobernanza que incorpore la figura del Delegado de Protección de Datos y protocolos internos de privacidad.
- Definir lineamientos para procesos y políticas que aseguren el ejercicio efectivo de los derechos ARSOP por parte de los titulares.
- Recomendar mejoras en la infraestructura tecnológica, orientadas a la seguridad por diseño y monitoreo continuo.
- Fomentar una cultura organizacional orientada a la protección de datos, mediante programas de capacitación y sensibilización.
- Establecer mecanismos de gestión de incidentes que permitan una respuesta rápida y transparente frente a brechas de seguridad.

Con el fin de orientar la implementación efectiva y reducir los riesgos asociados al tratamiento de datos personales, se han definido cinco ejes estratégicos que orientan las acciones del plan. Estos ejes representan las áreas críticas que deben ser abordadas de manera integral: desde la gobernanza corporativa y la definición de roles, hasta la adopción de medidas tecnológicas, la creación de políticas internas, la capacitación del personal y la gestión de incidentes. Cada eje busca asegurar que cada institución financiera no solo cumpla con la normativa, sino que también fortalezcan su cultura de privacidad y resiliencia frente a amenazas digitales.

Los ejes estratégicos son los siguientes:

1. **Gobernanza y Roles**

Establecer una estructura organizacional que garantice el cumplimiento normativo, incorporando la figura del Delegado de Protección de Datos (DPO) con autonomía funcional y la creación de un Comité de Privacidad para supervisar políticas y procesos.

2. **Procesos y Políticas**

Diseñar y formalizar protocolos internos para el tratamiento de datos personales, incluyendo la gestión de derechos ARSOP (Acceso, Rectificación, Supresión, Oposición y Portabilidad), así como la documentación de flujos y registros de actividades.

3. **Tecnología y Seguridad**

Implementar medidas técnicas orientadas a la seguridad por diseño y por defecto, como cifrado de datos, monitoreo continuo, control de accesos y sistemas de detección y respuesta ante incidentes.

4. **Capacitación y Cultura Organizacional**

Desarrollar programas de formación continua para todo el personal, orientados a la concientización sobre la protección de datos y la prevención de riesgos, fomentando una cultura de privacidad en la organización.

5. **Gestión de Incidentes y Notificación**

Definir protocolos claros para la identificación, reporte y comunicación de brechas de seguridad, asegurando la notificación a la autoridad y a los titulares en plazos preventivos.

A continuación, se encuentras las acciones que se deberían implementar para cada eje estratégico con su responsable a cargo:

Tabla 2. Acciones por Eje Estratégico

Eje estratégico	Acción	Responsable dentro de la institución
Gobernanza y Roles	Designación del Delegado de Protección de Datos.	Gerencia General
	Creación de Equipo de Protección de Datos y definición de funciones.	Gerencia de Cumplimiento
Procesos y Políticas	Elaborar política interna de protección de datos.	Área Legal / Compliance
	Implementar protocolos para derechos ARSOP	Atención al cliente
	Crear registros de actividades de tratamiento	TI / Cumplimiento
Seguridad y Tecnología	Implementar cifrado en bases de datos y comunicaciones	Área TI
	Instalar herramientas de monitoreo y detección de incidentes	Área TI / Seguridad

	Aplicar principio de seguridad por diseño en nuevos desarrollos	Desarrollo TI
Capacitación y Cultura	Programa anual de formación en protección de datos	RRHH / Cumplimiento
	Campañas internas de concientización	RRHH / Comunicaciones
Gestión de Incidentes	Crear protocolo de notificación de brechas.	Cumplimiento / TI
	Simulacros de respuesta ante incidentes	TI / Cumplimiento

Elaboración propia.

El plan de acción propuesto se estructura en nueve componentes que representan las etapas esenciales para garantizar el cumplimiento efectivo de la Ley N°21.719 en instituciones financieras. Cada componente aborda un ámbito crítico del tratamiento de datos personales, desde la identificación de brechas hasta la implementación de medidas tecnológicas y la formación del personal, asegurando un enfoque integral que combine gobernanza, procesos, seguridad y cultura organizacional.

1. **Diagnóstico**

Esta etapa inicial consiste en evaluar el estado actual de la institución en materia de protección de datos. Incluye la revisión de políticas internas, procesos operativos, infraestructura tecnológica y nivel de conocimiento del personal. El diagnóstico permite identificar brechas y riesgos prioritarios, sirviendo como base para definir acciones concretas y asignar recursos.

Costo estimado: $8.000.000 – $48.000.000 CLP
Beneficio: Identificación de brechas críticas y riesgos prioritarios.

El costo estimado entre $8.000.000 y $48.000.000 CLP, lo que incluye la revisión de políticas internas, procesos operativos, infraestructura tecnológica y entrevistas con personal clave para comprender el proceso en el que actualmente están utilizando para la protección de datos. Además, contempla el uso de herramientas de análisis y consultoría especializada para identificar brechas y riesgos prioritarios. El rango varía según el tamaño de la organización y la complejidad de sus sistemas. También tener en cuenta, que existen empresas que dan sus servicios, especialmente en estos tiempos que el plazo de adaptación y de toma de medidas cada vez es menor.

El costo puede ser estimado en base al uso de personal interno más la contratación de personal externo o sólo personal externo calificado. El costo del personal externo puede llegar a las UF100. Dos recursos externos por seis meses pueden llegar a costar aproximadamente $48.000.000 CLP.

2. Gobernanza de Datos

Es necesario establecer una estructura organizacional que garantice la supervisión del cumplimiento normativo. Esto implica la designación del Delegado de Protección de Datos (DPO) con independencia funcional, la creación de un equipo de protección de datos y la definición de roles y responsabilidades de las áreas que gestionen datos personales y de las que están encargadas de su resguardo. Este componente asegura que la protección de datos sea parte del gobierno corporativo y no solo una tarea operativa.

Este eje establece la estructura organizacional necesaria para garantizar el cumplimiento normativo y la supervisión efectiva del marco normativo. Además de la designación del Delegado de Protección de Datos (DPO) con independencia funcional, se propone la creación de un Equipo de Protección de Datos compuesto por:

- **Jefe de Protección de Datos**: Responsable de coordinar la estrategia de privacidad, actuar como enlace con la Agencia de Protección de Datos y supervisar el cumplimiento normativo.
- **Analistas especializados**: Cuatro encargados de gestionar el registro de actividades de tratamiento (RAT), realizar evaluaciones de impacto en la privacidad (DPIA), monitorear riesgos y apoyar en la implementación de políticas internas.

Costo estimado:

- DPO / Jefe: $3.500.000 – $5.000.000 mensuales → $42.000.000 – $60.000.000 anuales
- Analistas (4): $1.500.000 – $2.000.000 mensuales c/u → $72.000.000 – $96.000.000 anuales

Beneficio: Identificación de brechas críticas y riesgos prioritarios.

Este equipo permitirá una gestión integral y proactiva, asegurando que la protección de datos sea parte del gobierno corporativo y no solo una función operativa. La inversión estimada para este componente, considerando contratación interna, se sitúa entre $114.000.000 y $156.000.000 CLP anuales, lo que incluye remuneraciones y costos asociados. Los valores se basan en remuneraciones promedio del mercado chileno, incluyendo beneficios y costos asociados. Si bien existe la opción de externalizar parte del equipo, permitiendo una reducción del gasto en un 40%, esta alternativa limita la autonomía y la cultura interna de privacidad.

3. Nuevo Marco Normativo

Consiste en la adopción de políticas internas alineadas con la Ley N°21.719 y los estándares internacionales. Esto incluye la formalización de protocolos para el tratamiento de datos, la gestión de consentimientos y la atención de derechos ARSOP. En este paso se establecen reglas claras y uniformes para todos los procesos, reduciendo riesgos legales y fortaleciendo la transparencia.

Costo estimado: $5.000.000 – $24.000.000 CLP

Beneficio: Cumplimiento legal y transparencia.

El rango de $5.000.000 a $24.000.000 CLP se explica por el diseño e implementación de políticas internas alineadas con la normativa y estándares internacionales. Este componente incluye la formalización de protocolos para el tratamiento de datos, la gestión de consentimientos y la atención de derechos ARSOP. También contempla talleres internos para validación y capacitación. El costo depende de si se contrata consultoría externa o se desarrolla internamente.

El costo indicado se justifica por la utilización de recursos internos de la empresa o la contratación de recursos calificados para tal tarea. Contratar un recurso externo (UF100 por mes) por seis meses puede tener un costo aproximado de $24.000.000 CLP.

4. **Levantamiento de Tratamientos**

Implica la implementación del Registro de Actividades de Tratamiento (RAT), que documenta todos los procesos que involucran datos personales. Este registro permite trazabilidad y control, y es la base para identificar tratamientos de alto riesgo, sobre los cuales se aplicarán Evaluaciones de Impacto en la Privacidad (DPIA). Ambas herramientas son esenciales para demostrar cumplimiento ante la autoridad.

- **Registro de Actividades de Tratamiento (RAT)**: Es un procedimiento interno que consiste en la revisión sistemática de procesos, sistemas y proyectos que involucran tratamiento de datos personales, con el objetivo de verificar el cumplimiento de la normativa aplicable. Permite identificar brechas, riesgos y oportunidades de mejora en la gestión de datos personales, asegurando que las actividades se ajusten a los principios y obligaciones legales.

- **Evaluaciones de Impacto en la Privacidad (DPIA)**: Es una herramienta exigida por la Ley N° 21.719 y recomendada por estándares internacionales. Consiste en una evaluación previa al tratamiento de datos personales, especialmente cuando dicho tratamiento puede implicar un alto riesgo para los derechos y libertades de los titulares. Permite identificar, analizar y mitigar riesgos asociados al tratamiento de datos, y su realización será obligatoria en ciertos casos definidos por la ley.

Primero se realiza la RAT, que consiste en documentar todas las actividades que implican tratamiento de datos personales dentro de la organización, lo que permite identificar qué datos se procesan, con qué finalidad y quiénes son responsables. Luego, utilizando la información obtenida en la RAC, se determina si alguna actividad de tratamiento requiere una DPIA al identificar las actividades de alto riesgo.

Ambas herramientas funcionan de manera complementaria: la RAT proporciona la base de información para identificar actividades de alto riesgo, y la DPIA permite gestionar y mitigar esos riesgos, asegurando el cumplimiento normativo y la protección efectiva de los datos personales según la Ley N° 21.719.

Costo estimado: $4.000.000 – $16.000.000 CLP
Beneficio: Control y documentación para auditorías.

El costo estimado entre $4.000.000 y $8.000.000 CLP corresponde a la implementación del Registro de Actividades de Tratamiento (RAT) y la realización de Evaluaciones de Impacto en la Privacidad (DPIA). Estas herramientas son exigidas por la normativa y requieren análisis detallado de procesos, documentación y uso de metodologías especializadas. El rango varía según la cantidad de procesos involucrados y el nivel de automatización requerido.

El costo indicado se justifica por la utilización de recursos internos de la empresa o la contratación de recursos calificados para tal tarea. Contratar un recurso externo (UF100 por mes) por 4 meses puede tener un costo aproximado de $16.000.000 CLP. Este es un costo único por el primer año.

5. Gestión de Riesgos y Ciberseguridad

Este componente aborda la protección técnica de la información. Incluye la aplicación del principio de seguridad por diseño, cifrado de datos, monitoreo continuo, control de accesos y protocolos para prevenir incidentes. Además, contempla la realización de DPIA en proyectos críticos, asegurando que los riesgos sean evaluados y mitigados antes de implementar nuevas tecnologías.

Costo estimado: $25.000.000 – $50.000.000 CLP
Beneficio: Reducción de vulnerabilidades y protección ante ataques.

El costo estimado entre $25.000.000 y $50.000.000 CLP se justifica por la implementación de medidas técnicas orientadas a la protección de la información. Este componente incluye la aplicación del principio de seguridad por diseño, cifrado de datos, monitoreo continuo, control de accesos y protocolos para prevenir incidentes. Además, contempla la realización de DPIA en proyectos críticos, asegurando que los riesgos sean evaluados y mitigados antes de implementar nuevas tecnologías. El beneficio principal es la reducción de vulnerabilidades y protección ante ataques.

El costo indicado se basa en propuestas comerciales y técnicas de empresas especialistas en el rubro de la Ciberseguridad que van desde las UF775 hasta las UF1250. Este costo es único por el primer año.

6. Gestión de Consentimientos

Se enfoca en garantizar que el consentimiento de los titulares sea libre, informado y trazable. La institución debe implementar mecanismos claros para obtener, registrar y gestionar consentimientos, evitando ambigüedades y asegurando transparencia en el uso de datos personales.

Costo estimado: $20.000.000 – $200.000.000 CLP
Beneficio: Garantía de licitud en el tratamiento de datos.

El costo estimado entre $20.000.000 y $200.000.000 CLP considera el desarrollo o adquisición de herramientas que permitan capturar el consentimiento de manera clara, registrar la información con trazabilidad (fecha, canal y finalidad) y ofrecer la posibilidad de revocación en cualquier momento.

Para optimizar este proceso y reducir riesgos de incumplimientos, se recomienda incorporar soluciones tecnológicas especializadas, como **OneTrust – Consent Management Module**, plataforma líder en privacidad y cumplimiento normativo, ampliamente utilizada a nivel internacional.

Su módulo de gestión de consentimientos ofrece:

- Captura y registro centralizado de consentimientos en tiempo real.
- Integración con canales digitales (sitios web, aplicaciones móviles, CRM).
- Configuración dinámica según tipo de dato y finalidad del tratamiento.
- Generación de reportes y auditorías para demostrar cumplimiento ante la Agencia de Protección de Datos Personales.
- Compatibilidad con estándares internacionales (GDPR, LGPD), lo que asegura interoperabilidad y buenas prácticas.

La implementación del uso de este tipo de software no solo garantiza la licitud en el tratamiento de datos, sino que también fortalece la confianza del cliente y mejora la eficiencia operativa, posicionando a la institución en un nivel superior de gobernanza de datos. Al adoptar herramientas tecnológicas robustas, se garantiza un proceso transparente, seguro y eficiente, reduciendo riesgos legales y fortaleciendo la relación de confianza con los titulares de datos.

El costo estimado va desde desarrollos a medida con soluciones de software básicas, con la utilización de recursos internos o externos, hasta la implementación de herramientas (licencias) destinadas para tal efecto y su implementación. Este licenciamiento y la implementación en canales digitales y presenciales puede tener un costo aproximado de hasta UF5.000 para empresas de gran tamaño. Este costo es único y por el primer año.

7. Derechos ARSOP

Este punto establece canales y procedimientos para atender solicitudes de acceso, rectificación, supresión, oposición y portabilidad. La institución debe definir plazos internos, crear formularios y capacitar al personal para responder de manera eficiente, cumpliendo con las exigencias legales y fortaleciendo la confianza del cliente.

Costo estimado: $3.000.000 – $40.000.000 CLP
Beneficio: Garantía de licitud en el tratamiento de datos.

El costo estimado entre $3.000.000 y $6.000.000 CLP corresponde a la creación de canales y procedimientos para atender solicitudes de acceso, rectificación, supresión, oposición y portabilidad. Incluye la elaboración de formularios, definición de plazos internos y capacitación del personal. Es un componente de bajo costo relativo, dado que se centra en procesos organizacionales más que en infraestructura tecnológica.

El costo puede ser asumido de manera interna. Los costos expuestos son costos de oportunidad de las personas dedicadas a tal función. El tiempo involucrado puede ser de 2 meses. Este costo también es único.

8. Herramientas TI

Incluye la implementación de soluciones tecnológicas que soporten la gestión de datos y la seguridad. Esto abarca sistemas para monitoreo de incidentes, cifrado, automatización de procesos y plataformas que faciliten la atención de derechos ARSOP. Las herramientas TI son el soporte operativo del plan.

Costo estimado: $20.000.000 – $100.000.000 CLP
Beneficio: Eficiencia operativa y seguridad.

El rango de $20.000.000 a $100.000.000 CLP se explica por la implementación de soluciones tecnológicas que soporten la gestión de datos y la seguridad. Esto abarca sistemas para monitoreo de incidentes, cifrado, automatización de procesos y plataformas para la atención de derechos ARSOP. El costo depende de la complejidad de las herramientas y del modelo de adquisición (licencias, desarrollo propio o servicios en la nube). Los costos rondan en cotizaciones a proveedores con competencia en el rubro desde las UF500 hasta las UF2500. Este costo es anual.

Para cumplir con el principio de licitud establecido en la Ley N°21.719, es indispensable implementar una solución tecnológica que permita gestionar de manera eficiente, segura y trazable los consentimientos otorgados por los titulares de datos personales. Esta funcionalidad asegura que el tratamiento de datos se realice conforme a la normativa, evitando riesgos legales y reputacionales.

9. Capacitación y Comunicaciones

Este componente busca consolidar una cultura organizacional orientada a la privacidad, debido a que el proceso de cumplimiento normativo no depende únicamente de herramientas tecnológicas, sino también del compromiso y conocimiento del personal. Para ello, se deben implementar programas de capacitación distribuidos en grupos de interés, según la estructura y tamaño de la empresa, junto con campañas internas y comunicación efectiva para sensibilizar al personal sobre la importancia de la protección de datos y la prevención de riesgos. La capacitación es clave para reducir errores humanos y garantizar la sostenibilidad del cumplimiento, fortaleciendo la transparencia y confianza de la organización.

Costo estimado: $3.000.000 – $60.000.000 CLP
Beneficio: Cultura organizacional orientada a la privacidad.

El costo estimado entre $3.000.000 y $8.000.000 CLP incluye programas de capacitación segmentados por áreas, campañas internas y materiales de comunicación. El rango varía según el número de empleados y la modalidad de formación (presencial, virtual o mixta).

El costo puede ser asumido de manera interna con apoyo de expresas externas. Se incluye además la incorporación de las áreas de Recursos Humanos en los programas de capacitación. Los costos de expresas competentes en las áreas de capacitación rondan entre los UF100 y UF200. El costo es único en el primer año.

8.1.6 Viabilidad económica

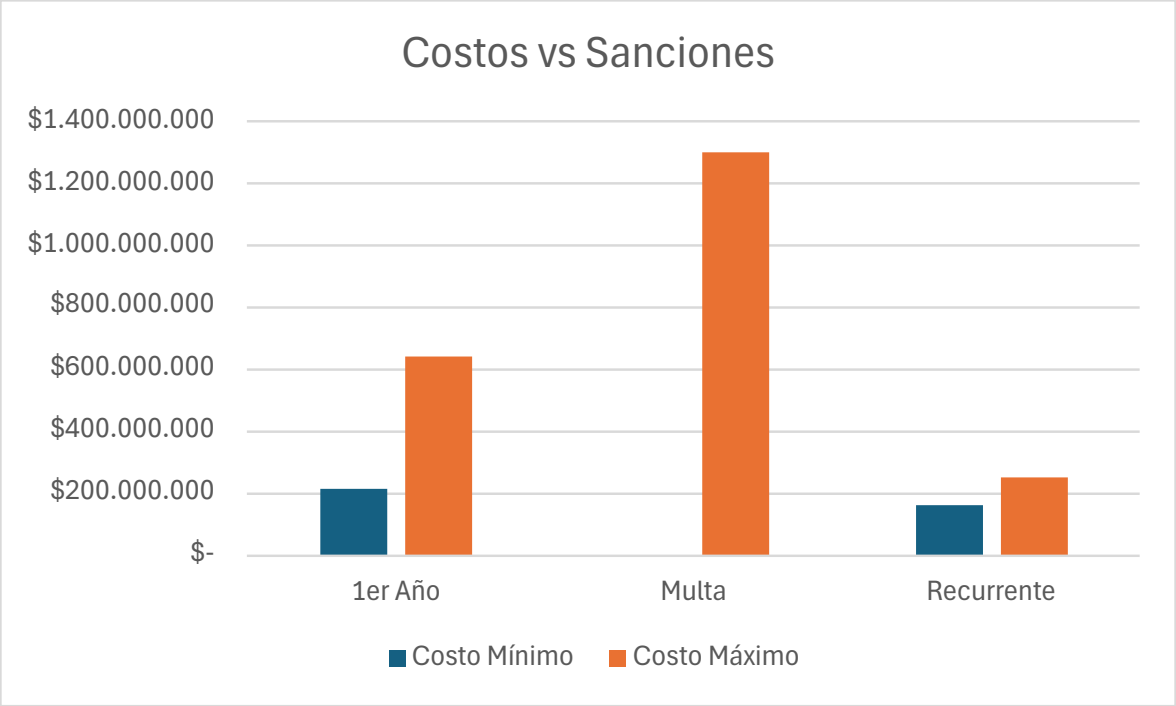
El plan de acción propuesto constituye una hoja de ruta integral que aborda las dimensiones críticas del cumplimiento normativo: gobernanza, procesos, tecnología y cultura organizacional. Cada componente ha sido diseñado para garantizar la adecuación a la nueva normativa, reducir riesgos legales y fortalecer la confianza del cliente. Más allá de su carácter operativo, este plan representa una inversión estratégica que permitirá a las instituciones financieras consolidar su resiliencia frente a amenazas digitales y proyectarse hacia estándares internacionales de privacidad.

La implementación del plan no debe interpretarse únicamente como una respuesta normativa, sino como una estrategia corporativa que impacta directamente en la competitividad y la reputación institucional. En un sector donde la confianza del cliente es el activo más valioso, la protección de datos se convierte en un diferenciador clave. Cumplir con la ley no solo evita sanciones, sino que refuerza la credibilidad ante clientes, reguladores y socios estratégicos, asegurando la sostenibilidad del negocio en un entorno digital cada vez más exigente.

El verdadero desafío no radica únicamente en la implementación inicial, sino en mantener el cumplimiento en el tiempo. Esto implica auditorías periódicas, actualización de tecnologías, capacitación continua y métricas de desempeño que permitan evaluar la efectividad de las medidas adoptadas. En este sentido, se debe establecer métricas y auditorías periódicas, definiendo indicadores (KPIs) y realizando evaluaciones internas y externas que permitan medir el nivel de cumplimiento y detectar oportunidades de mejora. La sostenibilidad del cumplimiento garantiza que la protección de datos no sea una acción puntual, sino una práctica permanente integrada en la cultura organizacional.

La evaluación económica demuestra que el costo de implementar el plan propuesto, aunque significativo, resulta inferior al riesgo económico y reputacional derivado del incumplimiento. Las multas contempladas por la Ley N°21.719 pueden alcanzar hasta 20.000 UTM, lo que equivale a montos millonarios capaces de comprometer la solvencia de las instituciones. Sin embargo, el impacto reputacional y la pérdida de confianza del cliente son aún más costosos, pudiendo afectar la continuidad del negocio. Las instituciones financieras, por la naturaleza de su actividad, son altamente

sensibles a los riesgos reputacionales, por lo que invertir en cumplimiento proactivo no solo es más eficiente, sino indispensable para preservar la credibilidad y la estabilidad.



Elaboración Propia

Como se aprecia en la imagen anterior, el costo de inversión mínimo del plan de acción al primer año se estima en $212.000.000 CLP y el recurrente es de $159.00.000 CLP, en cuanto al costo máximo es de aproximadamente al primer año $639.000.000 CLP, mientras que el recurrente alcanza los $251.000.000 CLP. En contraste, la multa máxima por incumplimiento (correspondiente a infracciones gravísimas) puede llegar a $1.300.000.000 CLP. Esta comparación refleja claramente que el costo de implementar el plan es menor que el valor de una sanción, lo que convierte la inversión en cumplimiento en una decisión estratégica.

Más allá del aspecto económico, es importante considerar que las instituciones financieras son altamente sensibles al riesgo reputacional. Una multa no solo implica un desembolso significativo, sino también un impacto negativo en la confianza del cliente, la credibilidad institucional y la competitividad en el mercado. Por ello, invertir en medidas preventivas no debe verse como un gasto, sino como una inversión en sostenibilidad, reputación y resiliencia operativa, asegurando que la organización cumpla con los estándares regulatorios y mantenga su posición en un entorno digital cada vez más exigente.

Finalmente, la adopción de este plan prepara a las instituciones para enfrentar futuras exigencias regulatorias y tecnológicas, consolidando una cultura organizacional orientada a la privacidad y la resiliencia digital. En un contexto global donde la protección de datos se ha convertido en un estándar competitivo, este plan posiciona a las entidades financieras chilenas en línea con las mejores prácticas internacionales, asegurando su capacidad de adaptación frente a nuevos desafíos.

9) CONCLUSIONES

El análisis realizado confirma que la Ley N°21.719 sobre Protección de Datos Personales constituye un hito en la regulación chilena y un cambio estructural en la forma en que las instituciones financieras deben gestionar, administrar y proteger la información de sus clientes. A diferencia de marcos normativos anteriores, esta ley incorpora un enfoque basado en derechos fundamentales, otorgando a los titulares un rol activo en la relación con las organizaciones y elevando la privacidad a un estándar equiparable a las legislaciones internacionales más exigentes, como el Reglamento General de Protección de Datos (RGPD) europeo. Esto refleja un avance significativo en la protección de datos en Chile y demanda transformaciones profundas a nivel organizacional, tecnológico y cultural dentro del sector financiero.

Los resultados del estudio evidencian que cumplir con los principios de licitud, finalidad, minimización de datos, responsabilidad proactiva y seguridad requiere que las instituciones adopten un enfoque integral, que abarquen no solo herramientas tecnológicas, sino también procesos internos, estructuras de gobernanza y capacitación constante. Esto implica que la protección de datos no puede concebirse como un proyecto aislado, sino como un componente transversal de la estrategia corporativa. En este sentido, la figura del Delegado de Protección de Datos (DPO), la existencia de un equipo dedicado a la protección de datos y la implementación de modelos de gobernanza sólidos se vuelven elementos imprescindibles para asegurar la continuidad del cumplimiento y la toma de decisiones informadas en relación a los riesgos.

Uno de los hallazgos más relevantes es que el cumplimiento normativo no debe interpretarse únicamente como un gasto adicional o una obligación regulatoria, sino como una inversión estratégica en confianza, reputación y sostenibilidad operativa, que aporta beneficios directos. La evaluación costo-beneficio realizada demuestra que el costo de implementar medidas de cumplimiento, que incluye gobernanza, tecnología, procesos y capacitación, es significativamente menor que el riesgo asociado al incumplimiento. En particular, las sanciones contempladas por la Ley N°21.719 pueden alcanzar hasta 20.000 UTM en casos de infracciones gravísimas, cifras que equivalen a montos

millonarios capaces de comprometer la solvencia de las instituciones, especialmente en el caso de entidades medianas o Fintech, cuyos márgenes operativos suelen más estrechos. No obstante, más allá del impacto monetario, el mayor impacto del incumplimiento se manifiesta en la pérdida de confianza, un daño reputacional difícil de revertir que puede afectar la fidelización, la captación de clientes y la posición competitiva en el mercado.

Los resultados también confirman que las instituciones financieras, por la naturaleza de su negocio, operan en un entorno altamente sensible, donde los riesgos reputacionales, regulatorios y tecnológicos están profundamente interconectados. La presencia de vulnerabilidades o brechas de datos no solo expone a las organizaciones a sanciones económicas, sino que además puede comprometer la estabilidad del sistema financiero, dada la criticidad de su infraestructura digital. En este contexto, invertir en tecnologías de seguridad por diseño, cifrado avanzado, autenticación robusta, auditorías continuas y evaluación de riesgos se vuelve una medida esencial para garantizar la integridad, confidencialidad y disponibilidad de la información.

Asimismo, la implementación del plan de acción propuesto permite visualizar que el cumplimiento normativo puede convertirse en una ventaja competitiva relevante en un entorno digital cada vez más regularizado y exigente. Cumplir con la Ley N°21.719 implica adoptar estándares internacionales de privacidad y ciberseguridad, lo que no solo asegura la conformidad legal, sino que facilita la interoperabilidad con sistemas regulados y fortalece la confianza de los consumidores, quienes actualmente valoran de manera creciente la transparencia en el tratamiento de sus datos. Además, promueve una cultura organizacional centrada en la responsabilidad y el respeto por la información personal, lo que contribuye a un clima laboral más consciente, ético y alineado con las demandas tecnológicas del entorno digital.

Por otro lado, la investigación muestra que la protección de datos no se limita a un aspecto técnico, sino que constituye un pilar fundamental de la gobernanza corporativa. Esto implica que la alta dirección y los equipos estratégicos deben integrar los criterios de privacidad en la toma de decisiones, en la planificación institucional y en la gestión de riesgos. La consolidación de una cultura orientada a la privacidad requiere protocolos claros, mecanismos permanentes de monitoreo, trazabilidad de los procesos y una participación activa de todas las áreas de la organización, desde las unidades operativas hasta los niveles ejecutivos.

En síntesis, la evidencia demuestra que el cumplimiento proactivo de la Ley N°21.719 no solo constituye la alternativa más eficiente desde una perspectiva económica, sino que es un requisito indispensable para garantizar la continuidad operativa, la sostenibilidad reputacional y la

competitividad del sector financiero chileno. La protección de datos no debe entenderse como una obligación legal aislada, sino como un instrumento estratégico que permite a las instituciones enfrentar un entorno digital dinámico, altamente regulado y expuesto a amenazas crecientes. En consecuencia, invertir en privacidad, seguridad y gestión de riesgos no solo protege a los clientes, sino que fortalece a la organización, contribuye a su resiliencia y asegura su proyección en la era digital.

10) BIBLIOGRAFÍA

- Autoridade Nacional de Proteção de Dados (ANPD). (2020). Lei Geral de Proteção de Dados Pessoais (LGPD). Recuperado de https://www.gov.br/anpd/pt-br
- Banco Central de Chile. (2023). Informe de Estabilidad Financiera – Segundo semestre 2023. Banco Central de Chile. Recuperado de https://www.bcentral.cl/documents/33528/133214/and-22112023.pdf
- Biblioteca del Congreso Nacional de Chile. (2024). Ley N°19.628 sobre Protección de la Vida Privada. Recuperado de https://www.bcn.cl/leychile/navegar?idNorma=141599
- Biblioteca del Congreso Nacional de Chile. (2024). Ley N°21.719 sobre Protección de Datos Personales. Recuperado de https://www.leychile.cl/leychile/navegar?idNorma=1209272
- Comisión para el Mercado Financiero (CMF). (2023). Presentación: Regulación y Ciberseguridad en el sistema financiero. CMF Chile. Recuperado de https://www.cmfchile.cl/portal/prensa/615/articles-83832_doc_pdf.pdf
- Consejo de Europa. (2018). Convenio 108+ para la protección de las personas con respecto al tratamiento automatizado de datos personales. Recuperado de https://www.coe.int/es/web/data-protection/convention108
- Contreras, P. (2017). La ley chilena de protección de datos personales: análisis crítico y perspectivas de reforma. Revista Chilena de Derecho y Tecnología, 6(2), 109–137. Recuperado de https://revista.uai.cl/index.php/rchdt/article/view/1678
- European Union. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, Reglamento General de Protección de Datos (GDPR). EUR-Lex. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679
- IDC. (2021). The Digitization of the World: From Edge to Core. International Data Corporation. Recuperado de https://www.idc.com
- Naciones Unidas. (1948). Declaración Universal de los Derechos Humanos. Recuperado de https://www.un.org/es/about-us/universal-declaration-of-human-rights
- OCDE. (2022). Going Digital to Advance Data Governance for Growth and Well-being. OECD Publishing. Recuperado de https://www.oecd.org/digital/going-digital-to-advance-data-governance-for-growth-and-well-being.htm

- SERNAC. (2024). Oficio a Banco Santander por filtración de datos. Servicio Nacional del Consumidor. Recuperado de https://www.sernac.cl/portal/604/w3-article-79979.html
- Soto, P. (2020). Protección de datos personales y ciberseguridad en Chile: hacia un nuevo paradigma regulatorio (Tesis de Magíster). Universidad de Chile. Recuperado de https://repositorio.uchile.cl/handle/2250/180176
- State of California. (2018). California Consumer Privacy Act (CCPA). Office of the Attorney General. Recuperado de https://oag.ca.gov/privacy/ccpa
- Unión Europea. (2000). Carta de los Derechos Fundamentales de la Unión Europea. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:12012P/TXT
- Deloitte. (s.f.). Análisis del presupuesto de ciberseguridad de las entidades financieras en España. Recuperado de https://www.deloitte.com/es/es/services/risk-advisory/blogs/cyber-pills/analisis-presupuesto-ciberseguridad-entidades-financieras-espana.html
- Deloitte. (s.f.). *GDPR: Retos y oportunidades para las empresas*. Recuperado de https://www.deloitte.com/es/es/services/risk-advisory/perspectives/gdpr-retos.html
- Deloitte. (s.f.). *The cost of compliance and regulatory productivity*. Recuperado de https://www.deloitte.com/us/en/services/consulting/articles/cost-of-compliance-regulatory-productivity.html
- IBM. (s.f.). *IBM Cloud cost estimator*. Recuperado de https://www.ibm.com/es-es/products/cloud/cloud-calculator
- Laborum. (s.f.). *Salarios en Chile*. Recuperado de https://www.laborum.cl/salarios
- Microsoft. (s.f.). *Microsoft Purview Suite pricing*. Recuperado de https://www.microsoft.com/es-mx/security/business/purview-suite-pricing

11) ANEXOS

11.1.1 Benchmarking comparativo.

Dimensión Analizada	Ley 21.719 (Chile)	GRDP (UE)	Brechas o diferencias relevantes	Riesgo para el sector financiero chileno	Recomendaciones estratégicas para instituciones financieras
Principios rectores del tratamiento	Define principios modernos: licitud, lealtad, transparencia, minimización, responsabilidad proactiva y seguridad.	Establece los mismos principios, ampliamente desarrollados y con guías operativas de la EDPB.	Falta de guías técnicas oficiales en Chile y ausencia de jurisprudencia consolidada.	Interpretaciones dispares, incumplimientos involuntarios, riesgo reputacional.	Implementar políticas internas basadas en guías del GDPR para reducir ambigüedades.
Derechos de los titulares	Reconoce acceso, rectificación, supresión, oposición y portabilidad.	Reconoce los mimos derechos, con mayor detalle y estándares estrictos.	En Chile faltan plazos y procedimientos tan concretos como en GDPR.	Riesgo de incumplimiento operacional (gestión de solicitudes masivas).	Crear un "Catálogo de Derechos" con plazos internos inferiores a los legales.
Delegado de Protección de Datos (DPO)	Obligatorio en entidades de alto riesgo, como instituciones financieras. Rol similar al europeo.	Obligatorio en organismos públicos y organizaciones que traten datos sensibles sistemáticamente.	En Chile aún no existe un estándar de certificación profesional ni guías de independencia funcional.	DPO con escasa autoridad interna o formación insuficiente → riesgo sancionatorio.	Establecer DPO con autonomía, reporte al directorio y capacitación continua.

Evaluaciones de Impacto (DPIA)	Obligatorias cuando el tratamiento implique alto riesgo. La ley define criterios, pero no detalla metodología.	DPIA obligatoria y muy reguladas; existen guías, listas de verificación y metodologías formales.	Ausencia de un marco metodológico oficial en Chile.	Realizar DPIA deficientes o formales, afectando la gestión de riesgo.	Adoptar metodologías GDPR como estándar interno.
Medidas de seguridad	Existe seguridad desde el diseño y por defecto, no define un estándar mínimo.	Exige seguridad fuerte con estándares exigentes y jurisprudencia consolidada.	Mayor flexibilidad en Chile podría llevar a mínimos insuficientes.	Mayor probabilidad de ciber incidentes, filtraciones y sanciones.	Implementar medidas para elevar los estándares operativos.
Brechas de seguridad y notificación	Debe notificarse a la Agencia y a titulares. Plazo aún no especificado; se espera criterio similar al GDPR.	Notificación obligatoria en 72 horas a la autoridad y sin demora injustificada a titulares.	Ley 21.719 no indica un plazo rígido.	Retrasos en notificaciones → sanciones y pérdida de confianza pública.	Establecer un protocolo interno como estándar preventivo.
Sanciones y multas	Multas hasta 20.000 UTM (~USD 1,3 millones).	Hasta 20 millones de euros o 4% del volumen de negocios global.	GDPR tiene sanciones muchísimo más altas.	En Chile puede ser más barato "pagar la multa" que cumplir → riesgo sistémico.	Evaluar costo-beneficio del cumplimiento vs. multas, integrando riesgo reputacional.

Gobernanza y cultura organizacional	Recién implementándose, sin práctica consolidada.	Cultura de cumplimiento madura, con auditorías, certificaciones y jurisprudencia.	Chile carece de experiencia práctica y casos reales.	Bancos podrían adoptar cambios superficiales en vez de estructurales.	Crear un Programa de Privacidad completo: políticas, roles, KPIs y auditoría interna.
Supervisión y autoridad	Crea la Agencia de Protección de Datos; aún sin trayectoria.	Autoridades consolidadas (ex: CNIL, AEPD).	Falta de criterios interpretativos en Chile.	Incertidumbre regulatoria, dificultad para planificar.	Prepararse bajo "estándares europeos", que son más exigentes y seguros.

11.1.2 Tabla Resumen del Plan de Acción

N°	Componente	Costo Mínimo	Costo Máximo	Beneficio	Justificación	Periodicidad
1	Diagnóstico	$8.000.000	$48.000.000	Identificación de brechas críticas y riesgos prioritarios	Evaluación integral del estado actual, uso de consultoría y herramientas especializadas.	Único
2	Gobernanza de Datos	$114.000.000	$156.000.000	Gestión integral y proactiva	Creación de estructura organizacional, contratación de DPO y analistas especializados.	Anual
3	Nuevo Marco Normativo	$5.000.000	$24.000.000	Cumplimiento legal y transparencia	Diseño e implementación de políticas internas y	Único

					protocolos ARSOP.	
4	Levantamiento de Tratamientos	$4.000.000	$16.000.000	Control y documentación para auditorías	Implementación del RAC y realización de DPIA.	Único
5	Gestión de Riesgos y Ciberseguridad	$25.000.000	$50.000.000	Reducción de vulnerabilidades y protección ante ataques	Medidas técnicas: cifrado, monitoreo, control de accesos y DPIA en proyectos críticos.	Anual
6	Gestión de Consentimientos	$30.000.000	$200.000.000	Garantía de licitud en el tratamiento de datos	Implementación de mecanismos para obtener, registrar y gestionar consentimientos.	Único
7	Derechos ARSOP	$3.000.000	$40.000.000	Garantía de licitud en el tratamiento de datos	Creación de canales y procedimientos para atender solicitudes ARSOP.	Único
8	Herramientas TI	$20.000.000	$45.000.000	Eficiencia operativa y seguridad	Implementación de soluciones tecnológicas para monitoreo, cifrado y automatización.	Anual
9	Capacitación y	$3.000.000	$60.000.000	Cultura organizacional	Programas de formación,	Único

	Comunicaciones			orientada a la privacidad	campañas internas y materiales educativos.	

-