

UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
VALPARAÍSO - CHILE



**“Propuesta de un Framework de Cumplimiento
Ley N° 21.719 de Protección de Datos Personales
para su implementación en una Institución
Pública”**

FABIÁN ANTONIO SEPÚLVEDA ESPINOZA

TESINA PARA OPTAR AL GRADO
DE MAGÍSTER EN TECNOLOGÍAS DE
LA INFORMACIÓN

Profesor Guía: DANIEL HORMAZÁBAL OCAMPO



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: Propuesta de un Framework de Cumplimiento Ley N° 21.719 de Protección de Datos Personales para su implementación en una Institución Pública

Nombre del candidato(a): Fabián Antonio Sepúlveda Espinoza

Carrera / Grado: Magíster en Tecnologías de la Información

Campus: San Joaquín **Departamento:** Informática

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, Daniel Hormazábal Ocampo, 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 (marcar una opción)

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

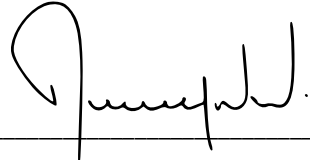
☐ El trabajo **CONTIENE** información con potenciales implicancias de propiedad industrial o intelectual y requiere un periodo de confidencialidad (**embargo**) por (**marcar una opción**):

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

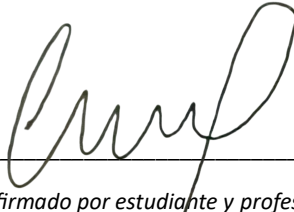
Fundamentación de la necesidad de confidencialidad (obligatorio si se solicita embargo):

4.- FIRMAS

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

Fecha: 27/10/2026 Firma: 

Estudiante o Candidato(a):

Fecha: 27/10/2026 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.



Propuesta de un Framework de Cumplimiento Ley N° 21.719 de Protección de Datos Personales para su implementación en una Institución Pública

Fabián Antonio Sepúlveda Espinoza

Instituto Geográfico Militar
Avenida Santa Isabel 1651, Santiago, Región Metropolitana

fabian.sepulveda@sansano.usm.cl

Resumen: El Instituto Geográfico Militar (IGM) de Chile es un organismo público de infraestructura crítica que debe cumplir con la Ley N° 21.719 sobre Protección de Datos Personales antes de que entre en vigor en diciembre de 2026. Este trabajo diseña e implementa un Modelo de Gobernanza de Datos Personales (MGDP) basado en estándares internacionales (ISO/IEC 27701 y DAMA-DMBOK) mediante la metodología *Design Thinking*, para permitir el cumplimiento normativo dentro de las limitaciones de recursos propias de una institución pública.

El diagnóstico institucional levantó 146 registros de datos personales en los 26 departamentos y secciones del IGM, consolidados en 42 tratamientos activos conforme al Art. 14 quáter de la ley. El análisis de brechas encontró 11 ítems de incumplimiento respecto al deber de información y transparencia, y el diagnóstico técnico del ERP institucional detectó 8 hallazgos de seguridad, de los cuales 3 son de criticidad crítica.

El MGDP diseñado considera 7 componentes: estructura de gobernanza con 3 roles formales, Registro de Actividades de Tratamiento (RAT) con 42 tratamientos documentados, metodología de Evaluación de Impacto (EIPD) para 7 tratamientos de alto riesgo, 5 flujos de atención ARCO+, modelo de prevención con 10 riesgos clasificados y *roadmap* de implementación y políticas y procedimientos institucionales. La validación por juicio experto de 2 evaluadores dio un impacto medio de 4,21 sobre 5 y una viabilidad de 3,50 sobre 5. La diferencia en la estimación de cumplimiento entre evaluadores, sustancial (70–89%) versus mínimo (<40%) nos señala que la automatización sistémica como condición necesaria complementaria al *marco* de gobernanza para alcanzar cumplimiento pleno de la ley.

Palabras Clave: Protección de Datos Personales, Gobierno de Datos, Arquitectura Empresarial
Ley N° 21.719

1 Introducción

El presente trabajo se enmarca en el cumplimiento de la Ley 21.719 “Regula la Protección y el Tratamiento de los Datos Personales y Crea la Agencia de Protección de Datos Personales”, que reemplaza la ley 19.628 “Sobre Protección de la Vida Privada” y que se alinea con los estándares internacionales como el GDPR de la Unión Europea.

El Reglamento General de Protección de Datos (GDPR), es la normativa vigente de la Unión Europea desde mayo de 2018, que protege la privacidad y los datos personales, obligando a las organizaciones que traten con datos personales a ser transparentes, tener consentimiento explícito y garantizar la seguridad de la información,



buscando empoderar a las personas sobre su identidad digital frente al uso masivo de datos por parte de las empresas.

La Ley 21.719 añade una mejora profunda respecto al marco regulatorio vigente, fortaleciendo los derechos ARCO (acceso, rectificación, cancelación y oposición) existente, agregando nuevos elementos como la portabilidad de los datos. Considera también la oposición al tratamiento de decisiones automatizadas, establece criterios de transferencia internacional de datos. Una de las diferencias entre las dos leyes es la exigencia de consentimiento explícito e inequívoco. Además, se establecen los siguientes principios: licitud, finalidad, proporcionalidad y responsabilidad proactiva (*accountability*).

Tal como el nombre de la ley lo señala, se crea la Agencia de Protección de Datos (APDP) quien es el organismo especializado para velar el cumplimiento de la normativa, a contraparte de la ley anterior, que eran los tribunales de justicia quienes dirimían los casos. La ley establece multas de acuerdo a los incumplimientos que se producen (leves, graves, gravísimos), las cuales pueden alcanzar las 20.000 UTM y administrando el Registro Nacional de Incumplimiento.

1.1 Contexto del problema

El Instituto Geográfico Militar es una institución dependiente del Ministerio de Defensa Nacional, responsable de la cartografía oficial de Chile y el levantamiento geodésico del territorio nacional. Diariamente el IGM procesa datos personales de aproximadamente 200 funcionarios entre civiles y militares, además de información de sus clientes. Estos datos incluyen información laboral, administrativa, financiera, académica e información biométrica.

La ley N° 21.719, publicada el 13 de diciembre de 2024, establece un nuevo marco regulatorio para el tratamiento de datos personales en Chile, perfeccionando la ley N° 19.628 de 1999. Esta normativa introduce conceptos alineados con el Reglamento General de Protección de Datos (GDPR) de la Unión Europea y los lineamientos de la OCDE, tales como: principios de minimización y limitación de finalidad, derechos ampliados de los titulares (acceso, rectificación, supresión, portabilidad), obligaciones de evaluación de impacto de privacidad, y designación de delegados de protección de datos [1].

El problema recae en que el IGM, no cuenta actualmente con una herramienta de cumplimiento para esta nueva normativa, al igual que muchos organismos del sector público. Los sistemas de información que utilizan fueron diseñados sin considerar principios de *Privacy by Design*, los procesos de tratamiento de datos no poseen una trazabilidad formal, y no existe un inventario documentado de activos de datos personales ni de sus flujos de procesamiento, como se puede observar en la auditoría de la CGR 651/2023 de año 2024 [2]. El plazo de implementación para iniciar el cumplimiento obligatorio es el 1 de diciembre 2026, lo que genera urgencia, pero la relevancia del cambio requiere un enfoque estructurado y fundamentado.

El IGM trabaja con recursos tecnológicos de instituciones públicas de tamaño medio. Su infraestructura tecnológica es soportada por un equipo de 5 profesionales (2 desarrolladores de sistemas y 3 desarrolladores web) responsables del desarrollo, mantenimiento y soporte de todas las aplicaciones institucionales. Los sistemas han sido desarrollados internamente. El presupuesto de TI está mayoritariamente comprometido en operación y mantenimiento, teniendo poco espacio para inversiones en nuevas plataformas. Esta realidad hace que cualquier solución de cumplimiento trabaje sobre la infraestructura existente sin requerir adquisición de software.

1.2 Propuesta de solución

La solución propuesta consiste en diseñar un *framework* para su implementación de cumplimiento estructurado en cuatro etapas: (1) diagnóstico técnico del estado actual mediante análisis de flujos de datos y evaluación de brechas de cumplimiento, (2) desarrollo de un *framework* para la propuesta de cumplimiento de la Ley 21.719 (3) desarrollo de un *roadmap* de implementación con arquitectura técnica de controles y procesos y (4) evaluar la viabilidad del modelo propuesto aplicando juicio experto para identificar mejoras y estimar el grado de cumplimiento normativo.

El impacto esperado traspasa el IGM, generando un modelo replicable para otras instituciones públicas que

enfrentan el mismo desafío. La contribución al campo de TI radica en adaptar *frameworks* internacionales existentes de protección de datos al contexto específico del sector público, considerando las particularidades normativas, presupuestarias y organizacionales.

1.3 Objetivo general

Establecer un *framework* para el cumplimiento de la ley de protección de datos personales (21.719), a ser implementada en el IGM y que pueda ser utilizado por otras instituciones, evitando las sanciones asociadas al incumplimiento de la ley obligatoria.

1.4 Objetivos específicos

- Diagnosticar el estado actual del tratamiento de datos personales en el IGM mediante análisis de flujos de información y evaluación de brechas de cumplimiento respecto a la Ley N° 21.719 para establecer la línea base y priorizar áreas críticas de intervención (OE1).
- Diseñar un Modelo de Gestión de Datos Personales (MGDP) alineado con la Ley N° 21.719 e ISO/IEC 27701 mediante la adaptación de *frameworks* internacionales al contexto institucional del IGM, para proporcionar una arquitectura de controles técnicos y organizacionales implementable con recursos existentes (OE2).
- Elaborar un roadmap de implementación del *framework* propuesto mediante la estructuración de fases temporales, identificación de dependencias críticas y especificación de la arquitectura técnica de controles y procesos, para proporcionar una hoja de ruta ejecutable que guíe la adopción gradual del MGDP en la institución (OE3).
- Evaluar el impacto potencial del *framework* de cumplimiento diseñado mediante juicio experto, para identificar mejoras, viabilidad de implementación y estimar grado de cumplimiento de la ley (OE4).

1.5 Hipótesis

El diseño de un framework de cumplimiento estructurado en estándares internacionales (ISO/IEC 27701 y DAMA-DMBOK) y validado mediante metodología Design Thinking permitirá al Instituto Geográfico Militar establecer los mecanismos de gobernanza, procedimientos operativos y capacidades institucionales necesarias para alcanzar el cumplimiento de la Ley N° 21.719 dentro de las restricciones de recursos propias de una entidad pública.

La verificación de esta hipótesis se circunscribe al diseño del *framework* y no a los efectos de su implementación. Al cierre de este trabajo el MGDP se encuentra en fase de diseño y no ha sido desplegado en el IGM, por lo que la hipótesis se contrasta evaluando la viabilidad de implementación y el impacto esperado de cada componente del modelo mediante juicio experto, y no midiendo resultados posteriores a su puesta en marcha.

1.5.1 Variable Independiente (Causal):

- Diseño del *framework* de cumplimiento (MGDP) estructurado en estándares internacionales (ISO/IEC 27701 y DAMA-DMBOK) y adaptado al contexto institucional del IGM.

1.5.2 Variables Dependientes (Efecto):

- Viabilidad de implementación de cada componente del MGDP en las condiciones de recursos, plazos y capacidades del IGM.
- Impacto esperado de cada componente sobre el cumplimiento de las obligaciones de la Ley N° 21.719.
- Cobertura normativa del *framework* respecto de los requisitos esenciales de la Ley N° 21.719 (RAT, EIPD, derechos ARCO+, seguridad y responsabilidad proactiva).
- Grado de cumplimiento normativo estimado que el IGM alcanzaría tras la ejecución completa del *roadmap* propuesto.

1.5.3 Metodología de Validación:

- Aplicación de un instrumento estructurado de juicio experto compuesto por tres partes: perfil del evaluador, evaluación por componente del MGDP en escala Likert de 1 a 5 (viabilidad e impacto) y juicio

global con preguntas abiertas.

- Evaluación de los siete componentes del MGDGP por dos evaluadores con perfiles complementarios y experiencia acreditada en protección de datos, cumplimiento normativo y ciberseguridad.
- Consolidación de los promedios de viabilidad e impacto por componente y análisis de la divergencia entre evaluadores como hallazgo cualitativo de la investigación.
- Contraste de las brechas levantadas en el diagnóstico (*checklist* del Art. 14 ter y diagnóstico técnico del ERP) con los componentes del MGDGP que las abordan, para verificar la cobertura del diseño.

1.6 Beneficios esperados

Se espera que los beneficios de este trabajo se vean reflejados en tres aspectos. Primero, se espera contar con funcionarios capacitados y conscientes de sus responsabilidades en el tratamiento de datos personales, viéndose traducido en la reducción de los incidentes relacionados con el desconocimiento o la negligencia en el manejo de información personal.

En relación con los procesos de *compliance*, el *framework* busca que la entidad pública se encuentre preparada para cumplir con los requisitos establecidos en la Ley 21.719.

En materia de gestión de la información, se espera alcanzar un mayor nivel en la gobernanza de datos, con procesos documentados, trazables y auditables que permitan una gestión eficiente y segura de los datos personales.

1.7 Estructura de trabajo

Este trabajo está compuesto por 5 capítulos que a continuación se detallan:

- **Introducción:** Se presenta contexto de la problemática que motivan este trabajo. Se expone la solución propuesta, los objetivos, la hipótesis de investigación, beneficios esperados y el método de validación
- **Marco teórico y estado del arte:** Se desarrollan los principales conceptos que dan sustento a este trabajo y se mencionan trabajos relacionados.
- **Desarrollo:** Se desarrolla la propuesta, el *framework* y de *roadmap* detallado para la implementación de las instituciones públicas.
- **Validación de la propuesta:** Se evalúa la viabilidad del *framework* mediante juicio experto, estimando el grado de cumplimiento alcanzable.
- **Conclusiones:** Se presentan las conclusiones del trabajo desarrollado, junto con el análisis de trabajos futuros.

2 Marco teórico y Estado del arte

2.1 Ley 19.628 “Sobre Protección de la Vida Privada”

La ley 19.628 “Sobre Protección de la Vida Privada” (LPDP) vigente desde agosto 1999 hasta la entrada en vigencia de las modificaciones introducidas por la Ley N° 21.719 el 1 de diciembre de 2026, estableció el marco normativo que regula la protección de datos personales y el tratamiento de estos en los distintos ámbitos de la vida, como los económicos, médicos y judiciales, entre otros [3].

La Ley 19.628 establece su ámbito de aplicación sobre el tratamiento de datos personales en registros o bancos de datos, tanto de organismos públicos como privados. Define datos personales como “*los relativos a cualquier información concerniente a personas naturales, identificadas o identificables*” (Art. 2° letra f), y crea una categoría especialmente protegida denominada datos sensibles, que abarca características físicas o morales, origen racial, ideologías políticas, creencias religiosas, estados de salud y vida sexual. La ley conceptualiza el tratamiento de datos como cualquier operación técnica (automatizada o no) que permita recolectar, almacenar, organizar, comunicar, transferir o cancelar datos personales [3]

La LPDP establece cinco principios rectores para el tratamiento de datos personales: (1) licitud, que exige autorización legal o consentimiento expreso del titular; (2) información, según el cual el consentimiento debe ser debidamente informado respecto al propósito del almacenamiento y su posible comunicación pública; (3) veracidad, que obliga a corregir datos erróneos, inexactos o incompletos; (4) finalidad, limitando el uso de datos exclusivamente a los fines para los cuales fueron recolectados (salvo fuentes públicas); y (5) confidencialidad, que impone obligación de secreto a quienes trabajan con datos provenientes de fuentes no

accesibles al público. Estos principios constituyeron el marco básico que permitió ordenar el tratamiento de datos y evitar abusos manifiestos durante su vigencia [3]. Además de reconocer cuatro derechos fundamentales (ARCO) (Tabla 1):

Derecho	Descripción
Acceso	Saber el tipo de datos procesados, su procedencia, destino, propósito del almacenamiento y destinatarios habituales
Rectificación	Exigir la modificación de datos erróneos, inexactos o incompletos
Cancelación	Eliminar datos cuando su almacenamiento carezca de fundamento legal, estén caducos o cese el consentimiento
Oposición	Impedir el tratamiento sin eliminar los datos, aplicable alternativamente a la cancelación cuando los datos fueron proporcionados voluntariamente o se usen para comunicaciones comerciales

Tabla 1: Derechos ARCO, ley 19.628 “Sobre la Protección de la Vida Privada”

El mecanismo de ejercicio de estos derechos es mediante exigencia directa al responsable del banco de datos, con ciertas limitaciones para organismos públicos. En caso de denegación o falta de respuesta, la ley contempla una acción denominada *habeas data* que permite a los titulares hacer valer judicialmente sus derechos ante tribunales civiles ordinarios [3].

2.2 Ley 21.719 “Regula la Protección y el Tratamiento de los Datos Personales y Crea la Agencia de Protección de Datos Personales”

La ley 21.719, publicada el 13 de diciembre de 2024, regula la Protección de Datos Personales y crea la Agencia de Protección de Datos Personales (APDP), modificando la ley 19.628 y estableciendo un nuevo marco legal para el tratamiento de datos personales, en esencia la ley busca que cualquier entidad que recopile, almacene, use o transfiera datos personales lo haga de manera transparente, segura, y con el consentimiento explícito del titular.

La Ley 21.719 modifica sustancialmente a su predecesora sin derogarla completamente, convirtiendo un sistema robusto alineado con el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. Esta alineación facilita el intercambio internacional de datos mediante convergencias clave: consentimiento libre, específico e informado; obligación de demostrar cumplimiento con medidas técnicas y organizativas; Evaluaciones de Impacto en Protección de Datos (EIPD) para tratamientos de alto riesgo; y notificación obligatoria de brechas de seguridad a la autoridad y afectados cuando existan riesgos significativos [4].

La nueva ley impone obligaciones a los responsables del tratamiento (quienes deciden sobre el tratamiento) y a los encargados (quienes tratan datos por cuenta del responsable), en torno a principios fundamentales: el principio de licitud exige una base legal clara (consentimiento, cumplimiento de obligación legal, ejecución contractual, protección de intereses vitales, interés público o interés legítimo); el principio de finalidad requiere fines específicos, explícitos y legítimos sin tratamientos posteriores incompatibles; el principio de proporcionalidad y minimización limita la recolección a datos estrictamente necesarios; el principio de calidad obliga a mantener datos exactos, completos y actualizados con obligación de rectificación o supresión de información inexacta; el principio de seguridad demanda medidas técnicas y organizativas adecuadas contra tratamientos no autorizados, pérdida o daño; y el principio de transparencia e información exige comunicar claramente a los titulares cómo, por qué y por cuánto tiempo se tratan sus datos, además de sus derechos. Adicionalmente, las organizaciones deben mantener un Registro de Actividades de Tratamiento detallado, realizar Evaluaciones de Impacto en Protección de Datos (EIPD) para tratamientos de alto riesgo, y notificar a la Agencia y a los afectados las brechas de seguridad que supongan riesgos significativos para derechos y libertades [4].

La Ley 21.719 protege cualquier información relativa a persona natural identificada o identificable, tal como se aprecia en la Figura 1. Dentro de los cambios que trae la ley es la creación de la agencia, quien tiene por objetivo velar por la protección de los derechos que garantizan la vida privada de las personas y sus datos personales. Las atribuciones de la agencia consideran: fiscalizar el cumplimiento de la ley, determinar las infracciones e incumplimiento de los encargados de datos, resolver reclamos de los titulares, entre otros [5]. Las multas asociadas pueden alcanzar hasta las 20.000 UTM y están relacionadas con las infracciones que pueden ser catalogadas como leves, graves y gravísimas. Además, la APDP será la encargada de administrar el Registro Nacional de Sanciones y Cumplimiento, de carácter público, que documentará por un periodo de hasta cinco años las instituciones sancionadas por infracciones a la ley [6].



Figura 1: Tipos de Datos Personales, Ley 21.719. Fuente: <http://bit.ly/3ZtNDjW>

Al comparar ambas leyes podemos encontrar las siguientes diferencias (Tabla 2):

Característica	Ley 19.628	Ley 21.719
Enfoque Principal	Protección de la vida privada.	Protección y tratamiento de datos personales.
Autoridad de Control	Inexistente (acción vía tribunales).	Crea la Agencia de Protección de Datos Personales (APDP).
Derechos de Titulares	Derechos ARCO (Acceso, Rectificación, Cancelación, Oposición).	Derechos ARCO+ (suma Portabilidad y S suspensión).
Multas Máximas	Hasta 50 UTM	Hasta 20.000 UTM (o el 4% de ingresos anuales).
Principios de Tratamiento	Consentimiento y finalidad básica.	Responsabilidad proactiva, transparencia, minimización y seguridad.
Transferencia Internacional	Sin regulación específica robusta.	Regulada bajo criterios de país seguro o cláusulas contractuales.
Nuevas Figuras	No contempladas.	Introduce al Delegado de Protección de Datos (DPO).

Tabla 2: Diferencia entre las leyes 19.628 y 21.719

2.3 Gobierno de Datos

El gobierno de datos es la disciplina de gestión de datos que se centra en la calidad, seguridad y disponibilidad de los datos de una organización, con el fin de ayudar a garantizar la integridad y seguridad de los datos mediante la definición e implementación de políticas, estándares y procedimientos para la recopilación, propiedad, almacenamiento y uso de datos [7], obteniendo los siguientes beneficios [8]:

- Obtener datos confiables y consistentes
- Prevenir conflictos e inconsistencias
- Minimizar el riesgo en la toma de decisiones y análisis
- Armonizar los procesos de negocio
- Utilizar más eficientemente los recursos
- Cumplir las normativas de protección de datos personales

En este sentido el linaje de dato, que se define como el proceso de seguimiento de flujo de datos a lo largo del tiempo, ayuda a comprender dónde se originan los datos, como han cambiado y su destino final dentro un flujo de datos. Esto ayuda a que una organización pueda mantener la calidad y seguridad de los datos a lo largo del tiempo. El gobierno de datos crea la estructura dentro de las organizaciones para gestionar los activos de datos mediante políticas, reglas y procesos a lo largo del ciclo de vida de los datos [9]. El linaje de datos ayuda a los equipos de gobernanza de datos a garantizar que los datos cumplan con dichos estándares. Además, esta

herramienta proporciona un seguimiento de auditoría de los datos a un nivel muy granular; en el contexto de la ley es esencial para identificar, localizar y auditar datos personales, facilitando la gestión de derechos como el acceso, la rectificación y el olvido [10].

En este aspecto, la División de Gobierno Digital de Chile junto con la Universidad Adolfo Ibañez [11], desarrollaron el Marco de Referencia de Gestión de Datos del Estado (MGDE), herramienta para la administración pública, basada en la adaptación del estándar internacional DAMA (Data Management *Body of Knowledge*) a la realidad de las instituciones [12] [13]. Integrado como un requisito técnico del Sistema de Transformación Digital 2025, el MGDE permite a los organismos realizar un diagnóstico de brechas a través de 12 dimensiones (Figura 2) clave para gestionar los datos como activos estratégicos que generen valor público. En este escenario, su relación con la protección de datos personales es directa y operativa, ya que el marco incorpora criterios específicos de privacidad y seguridad, y establece como principio rector el uso ético de la información en estricto cumplimiento de la normativa vigente, integrando a las áreas jurídicas en la definición de políticas de cumplimiento legal.



Figura 2: Dimensiones Marco de Referencia de Gestión de Datos

2.4 ISO 27.701.

La norma ISO/IEC 27701 es una extensión de la ISO 27001 en materia de privacidad de datos, consiste en un sistema de gestión de la privacidad de la información (PIMS) que se integra con la seguridad de la información para proteger datos personales de forma sistemática y demostrable. La norma proporciona un marco estructurado y reconocido internacionalmente que ayuda a las organizaciones a demostrar su responsabilidad, gestionar los riesgos en torno a la información de identificación personal (IIP) [14].

Los elementos principales y componentes son [15]:

- Estructura basada en ISO 27001: Comparte la estructura de los sistemas de gestión ISO y su lógica de mejora continua, alineándose con la gestión de la seguridad de la información.
- Definición de roles: Distingue responsables del tratamiento y encargados de tratamiento de IIP.
- Evaluación de riesgos: Amplía la gestión de riesgos para incluir los riesgos de la privacidad, derechos y libertades de las personas.
- Gestión Documental: Exige documentación detallada sobre el tratamiento de datos personales, políticas de privacidad, transferencia de datos y respuesta ante incidentes.
- Cumplimiento Legal: Diseñada para ayudar a las organizaciones a cumplir con la normativa de protección de datos.

La ley 21719 y la ISO 27701 se alinean dado que la norma ISO proporciona un marco certificable para implementar con evidencias demostrables, en particular la ley exige *accountability* y la norma entrega controles que cubren consentimiento, transparencia, derecho de titulares y auditorías, entregando registros para posterior control de la Agencia de Protección de Datos.

2.5 Design Thinking

El *Design Thinking* es una metodología de resolución de problemas centrada en las personas, desarrollada en el Instituto de Diseño de Stanford [16]. Su objetivo es abordar problemas complejos o mal definidos mediante

un enfoque empático, colaborativo e iterativo, combinando herramientas del diseño, las ciencias sociales y la ingeniería para generar soluciones innovadoras.

El proceso se estructura en cinco fases no lineales (Figura 3): Empatizar (comprender profundamente a los usuarios afectados por el problema), Definir (formular una declaración de problema clara y centrada en el ser humano), Idear (generar la mayor cantidad de soluciones posibles mediante lluvia de ideas), Prototipar (crear versiones simplificadas de las soluciones) y Probar (evaluar los prototipos con usuarios reales para identificar mejoras). Al ser iterativo, el proceso puede reiniciarse en cualquier etapa según los hallazgos.



Figura 3: Etapas *Design Thinking*

Entre sus principales ventajas destacan que impulsa la acción y la creatividad, fomenta el pensamiento "fuera de la caja", reduce riesgos al aprender de errores en etapas tempranas y promueve la colaboración interdisciplinaria. Es especialmente útil en contextos de innovación, rediseño de procesos de negocio y gestión del cambio.

3 Desarrollo

3.1 Aplicación de la Metodología *Design Thinking* al MGD

El presente capítulo organiza el desarrollo de la propuesta siguiendo las cinco fases del modelo de *Design Thinking* del Instituto de Diseño de Stanford, referenciado en el marco teórico. Cada fase se traduce en un conjunto de actividades concretas que responden a los cuatro objetivos específicos de la investigación, garantizando que el *framework* resultante sea coherente con las necesidades del Instituto Geográfico Militar (IGM) y viable dentro de sus capacidades.

La Tabla 3 sintetiza la correspondencia entre las fases de *Design Thinking*, las actividades desarrolladas y los objetivos específicos que cada una aborda:

Etapas	Descripción	Objetivo Específico
Empatizar	Diseño y aplicación de 3 cuestionarios por rol (<i>Data Owners</i> , <i>Data Stewards</i> , <i>Data Custodians</i>). Reuniones de trabajo con 26 departamentos y secciones del IGM.	OE1 (Diagnóstico)
Definir	Levantamiento de 146 registros de datos personales. Análisis de brechas de cumplimiento. Informe de Hallazgos conforme Guía SGD.	OE1 (Diagnóstico)
Idear	Diseño del Modelo de Gestión de Datos Personales (MGDP) con 7 componentes, entre ellos el RAT y el Modelo Operacional de protección de datos.	OE2 (Diseño MGD)
Prototipar	<i>Roadmap</i> de implementación con 4 horizontes temporales. Arquitectura técnica objetivo del ERP. Plan de mitigación de 9 acciones.	OE3 (<i>Roadmap</i>)
Testear	Validación mediante juicio experto: viabilidad e impacto por componente del MGD y grado de cumplimiento estimado.	OE4 (Evaluación)

Tabla 3: Relación entre fases de *Design Thinking* y objetivos específicos de la investigación.

3.2 Diagnóstico del Estado Actual del Tratamiento de Datos Personales (OE1)

El diagnóstico corresponde a las fases de Empatizar y Definir del modelo de *Design Thinking*. Su objetivo fue establecer la línea base del estado actual del tratamiento de datos personales en el IGM, identificar las brechas de cumplimiento respecto a la Ley N° 21.719 y priorizar las áreas críticas de intervención. El proceso se estructuró en cuatro etapas complementarias: aplicación de instrumentos de recolección de información por rol, levantamiento sistemático de datos personales en todas las unidades institucionales, análisis de brechas de cumplimiento normativo y diagnóstico técnico de la infraestructura de datos.

3.2.1 Instrumentos de Recolección de Información por Rol

De acuerdo con el principio de empatía del *Design Thinking*, y con el propósito de comprender las prácticas de tratamiento de datos personales desde la perspectiva de quienes las ejercen, se diseñaron tres instrumentos de recolección de información diferenciados según el rol funcional de los encuestados, siguiendo la clasificación de roles

del marco DAMA-DMBOK adoptado en este trabajo.

El instrumento dirigido a los Responsables de Datos (**Data Owner**) compuesto por 23 preguntas sobre las finalidades del tratamiento, las bases de licitud utilizadas, los criterios de conservación de datos y de riesgo institucional respecto al incumplimiento de la Ley N° 21.719. El instrumento dirigido a los Administradores de Datos (**Data Stewards**), compuesto por 25 preguntas, se centra en los procesos operativos de tratamiento, la calidad y completitud de los registros, y la gestión de incidentes. El instrumento dirigido a los Custodios Técnicos de Datos (**Data Custodians**), compuesto por 23 preguntas, aborda la seguridad técnica de los sistemas de información, los controles de acceso implementados y la trazabilidad de las operaciones sobre datos personales. Los instrumentos fueron respondidos por 10 funcionarios: 4 *Data Owners*, 3 *Data Stewards* y 3 *Data Custodians*.

Los instrumentos fueron implementados mediante Formularios de Google (**Anexo 1**), la recopilación estructurada de las respuestas. Los resultados muestran una contradicción estructural: 4.5/5 de disposición al cambio convive con 0 procedimientos, 0 inventarios y 0 responsables designados. Esto dice que el problema no es cultural ni de falta de voluntad, es de liderazgo y asignación de recursos. El radar de madurez (Figura 4) muestra que las dimensiones de gobernanza y operativa son las más críticas (nivel 1/5), mientras que la normativa es la más avanzada (2.5/5) porque al menos existe conciencia de la ley

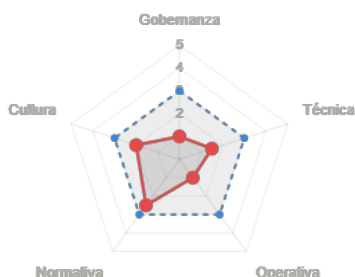


Figura 4: Radar de Madurez de la Organización

Cuando se miran los resultados por rol encontramos la siguiente información:

Los Custodios Técnicos de Datos (**Data Custodians**), tienen 6 de 7 capacidades técnicas evaluadas están en 0. Lo más grave es la trazabilidad cero ante un incidente. Además, se sienten poco preparados (2.3/5) pero creen que la infraestructura alcanza (3.7/5), lo que puede llevar a planificaciones optimistas.

El Responsable de Datos (**Data Owner**) tiene la brecha más estratégica, el argumento más efectivo para movilizarlos no es el legal (sanciones), sino el reputacional fue el único riesgo mencionado por todos.

El Administrador de Datos (**Data Stewards**) tiene la brecha más operacional: si ocurriera un incidente hoy, nadie en el nivel operativo sabría qué hacer. El hallazgo positivo es que el único funcionario que recibió, aunque sea capacitación informal (RRHH) muestra métricas notablemente mejores que los otros, evidencia directa del impacto que tendría un programa de capacitación institucional.

3.2.2 Levantamiento de Datos Personales

El levantamiento de información se realizó conforme a la metodología establecida en la Sección 3 de la Guía Práctica para la Implementación de la nueva Ley de Datos Personales publicada por la Secretaría de Gobierno Digital, utilizando la Matriz de Levantamiento de Información como instrumento base. Se distribuyó dicho insumo a todos los departamentos y secciones y se realizaron instancias de capacitación grupal y resolución de consultas individuales a fin de facilitar la realización del levantamiento de la información. Se incorporaron 26 departamentos y secciones del IGM, incluyendo áreas como Asesoría Jurídica, Finanzas, Sanidad y Seguridad Militar.

Lo anterior generó un total de 146 registros individuales de datos personales distribuidos en 26 departamentos y secciones (**Anexo 2**). Cada registro documenta, entre otros campos: la categoría del dato, el universo de titulares, si es o no sensible, la base de datos asociada, la finalidad del tratamiento, la habilitante legal, la fuente de procedencia, los destinatarios, el responsable interno, el plazo de conservación, los sistemas de información involucrados y los riesgos identificados. Los 146 registros individuales fueron posteriormente consolidados en 42 actividades de tratamiento distintas (RAT), agrupando aquellos registros que comparten finalidad, base de licitud y categoría de datos, conforme a la estructura del Registro de Actividades de Tratamiento exigido por el artículo 14 quáter de la Ley N° 21.71.

El análisis de flujos de información se realizó a partir de los campos de la matriz que describen el recorrido de cada



dato dentro y fuera del IGM: fuente de procedencia, sistemas y plataformas asociados, accesos, lugar de almacenamiento, plazo de conservación y transferencias o comunicaciones a terceros. Este análisis permitió identificar los puntos de exposición del ciclo de vida del dato: 6 tratamientos con transferencias internacionales o comunicaciones a terceros sin base legal documentada (RAT-006, 017, 027, 031, 032 y 037), tratamientos soportados en sistemas que no permiten acreditar trazabilidad de accesos, la publicación de datos personales en plataformas web e intranet y la ausencia de plazos de conservación definidos en la mayoría de los registros. Estos puntos de exposición se recogen en el Modelo de Prevención de Riesgos (Tabla 10) y orientan la priorización del *roadmap*.

Parte de los registros fue remitida por los departamentos sin el visto bueno de la jefatura de área: 40 registros indican "Pendiente de V°B°" y otros dejaron ese campo sin completar. Estos registros se incorporaron igualmente al análisis, por cuanto su contenido fue entregado formalmente por cada unidad.

La Tabla 4 presenta las estadísticas principales del levantamiento:

Indicador	Resultado	Observación
Total de registros levantados	146	Distribuidos en 26 departamentos y unidades del IGM.
Departamentos cubiertos	26 de 26 (100%)	Cobertura total de la estructura organizacional.
Tratamientos RAT consolidados	42	Agrupación lógica de los 146 registros por actividad.
RAT con datos sensibles	18 (43%)	Biometría, salud, credo, datos de menores.
Tratamientos con riesgo ALTO	13 (30%)	Requieren Evaluación de Impacto (EIPD).
Registros con plazo indefinido	Mayoría	Brecha directa al principio de limitación del plazo (Art. 3 g).
Sistemas con datos biométricos	3	SICE, UCTL, videovigilancia CCTV.

Tabla 4: Estadísticas principales del levantamiento de datos personales en el IGM.

3.2.3 Análisis de Brechas de Cumplimiento Normativo

A partir de la información recopilada en el levantamiento, se realizó un análisis de brechas de cumplimiento respecto al *checklist* establecido en el artículo 14 ter de la Ley N° 21.719, que regula el deber de información y transparencia de los responsables de datos. Este análisis fue realizado de acuerdo a la Sección 4 de la Guía Práctica de la Secretaría de Gobierno Digital y clasifica cada ítem en tres niveles, aplicando el siguiente criterio:

- **Brecha Total:** Cuando no se cuenta con ningún instrumento, procedimiento o evidencia documental que dé cumplimiento al requisito.
- **Brecha Parcial:** Cuando existe un elemento concreto y verificable que satisface parcialmente un requisito, pero aún quedan condiciones por cumplir que no permiten declararlo conforme.
- **Sin Brecha:** Cuando el requisito se encuentra completado.

La Tabla 5 presenta los resultados del análisis para cada uno de los 12 ítems obligatorios:

N°	Obligación (Art. 14 ter Ley 21.719)	Estado IGM	Justificación
1	Política de tratamiento de datos adoptada, con fecha y versión.	Brecha Total	
2	Individualización del responsable y del DPD si existiere.	Brecha Parcial	El responsable del tratamiento está designado mediante resolución institucional vigente y el DPD está formalmente designado. Condición no cumplida: los datos de contacto del DPD no están publicados en el sitio web institucional, requisito exigido por el Art. 14 ter.
3	Canal oficial de contacto para solicitudes ARCO+ de titulares.	Brecha Total	
4	Categorías de datos, titulares, destinatarios, finalidades y bases de licitud.	Brecha Total	
5	Política y medidas de seguridad para la protección de bases de datos.	Brecha Total	
6	Derecho del titular a solicitar acceso, rectificación, supresión, oposición y portabilidad.	Brecha Parcial	Existe una cuenta de correo institucional habilitada para recibir solicitudes

			ARCO+. Condición no cumplida: los procedimientos de atención están en desarrollo y no se encuentran formalizados; el canal no está publicitado oficialmente a los titulares.
7	Derecho del titular a recurrir ante la Agencia ante respuesta insatisfactoria.	Brecha Parcial	El formulario de consentimiento para tratamiento de datos biométricos informa al titular sobre sus derechos, incluyendo la posibilidad de recurrir ante la autoridad. Condición no cumplida: esta información no se extiende al universo completo de titulares ni a la totalidad de los tratamientos activos.
8	Transferencias internacionales y nivel de protección del país de destino.	Brecha Total	
9	Período de conservación de los datos personales.	Brecha Total	
10	Fuente de procedencia de los datos.	Brecha Parcial	La fuente de procedencia está documentada en un subconjunto de las fichas RAT levantadas. Condición no cumplida: la documentación no cubre la totalidad de los 42 tratamientos activos, incumpliendo el estándar de exhaustividad del Art. 14 ter.
11	Derecho a retirar el consentimiento cuando el tratamiento se basa en éste.	Brecha Parcial	El Art. 14 ter exige informar sobre el derecho a retirar el consentimiento con independencia de si el consentimiento es la base de licitud empleada. Condición no cumplida: el IGM no cuenta con ningún instrumento ni aviso que informe a los titulares sobre este derecho.
12	Existencia de decisiones automatizadas o elaboración de perfiles.	Sin Brecha	

Tabla 5: Análisis de brechas respecto al *checklist* del Art. 14 ter, Ley N° 21.719.

Los resultados indican que el IGM presenta brechas totales en 6 de los 12 ítems obligatorios (50%), brechas parciales en 5 ítems (42%) y 1 ítem sin brecha (8%), correspondiente a la ausencia de decisiones automatizadas o elaboración de perfiles. Este diagnóstico evidencia que el IGM debe desarrollar desde cero sus principales instrumentos de cumplimiento normativo.

3.2.4 Diagnóstico Técnico de Seguridad del ERP Institucional

Complementando el levantamiento organizacional, la Sección de Informática del IGM elaboró entre los meses de febrero y abril 2026 un Diagnóstico de Seguridad en Acceso a Bases de Datos del ERP Institucional [17], que identificó brechas técnicas directamente vinculadas al incumplimiento de los artículos 14 bis, 14 quinquies y 14 sexies de la Ley N° 21.719, relativos a las obligaciones de seguridad, confidencialidad y responsabilidad en el tratamiento de datos personales.

El documento de diagnóstico es de circulación restringida, por lo que no se incorpora como anexo; sus resultados se reproducen en la medida necesaria para sustentar el diagnóstico.

La criticidad de cada brecha técnica se clasifica conforme a tres criterios acumulativos:

- **Crítico:** Cuando la brecha permite acceso no autorizado a datos personales sin posibilidad de detección ni trazabilidad posterior, o cuando su explotación no requiere privilegios especiales;
- **Alto:** cuando la brecha compromete la integridad o confidencialidad de los datos, pero su explotación requiere conocimiento técnico específico o acceso previo al sistema; y
- **Medio:** Cuando la brecha representa una debilidad de configuración que, en ausencia de otros controles compensatorios, podría facilitar un incidente.

El ERP institucional opera sobre SQL Server y utiliza una arquitectura de acceso que concentra a todos los usuarios bajo una única cuenta compartida, con autenticación y control de privilegios gestionados íntegramente a nivel de la aplicación cliente (desarrollada en VB6), sin controles de seguridad en la capa de base de datos. Esta arquitectura genera las brechas técnicas que se presentan en la Tabla 6:

Nº	Criticidad	Brecha Identificada	Artículo Vulnerado
1	Crítico	Cuenta SQL compartida: todos los usuarios acceden con las mismas credenciales, sin trazabilidad individual. Ante una brecha, es imposible determinar quién accedió a qué datos.	Art. 14 quinquies + Art. 14 sexies
2	Crítico	Seguridad solo en capa de presentación (VB6): cualquier usuario con conocimientos técnicos puede eludir los controles de acceso conectándose directamente a la base de datos.	Art. 14 quinquies
3	Crítico	Credenciales hardcodeadas en código fuente VB6: la contraseña de la cuenta de sql puede ser extraída por cualquier persona con acceso al equipo.	Art. 14 quinquies
4	Alto	Tabla de privilegios modificable: un usuario puede escalar sus propios privilegios en el sistema sin detección.	Art. 14 quinquies
5	Alto	Contraseñas con cifrado propio reversibles	Art. 14 quinquies + Art. 14 bis
6	Alto	Sin auditoría nativa de SQL Server: no existe registro de quién accedió a qué datos personales ni cuándo.	Art. 14 sexies
7	Medio	Conexiones sin cifrado TLS: datos personales pueden ser interceptados en la red interna.	Art. 14 quinquies
8	Medio	Sin control de sesiones concurrentes: facilita el uso indebido de credenciales.	Art. 14 quinquies

Tabla 6: Brechas técnicas identificadas en el ERP institucional del IGM. Fuente: Informe Técnico N.º 05/2026, Sección Informática, Computación y Estadísticas IGM (abril 2026).

Las tablas del ERP expuestas por estas brechas incluyen datos de alta sensibilidad: identificación del personal (RUT, nombre, dirección), turnos y permisos (licencias médicas), remuneraciones (sueldo, AFP, Isapre/Fonasa) y privilegios de acceso (credenciales del sistema). La brecha más crítica desde la perspectiva del cumplimiento normativo es la imposibilidad de acreditar trazabilidad individual, requerido para dar cumplimiento al principio de responsabilidad proactiva (Art. 13) y para responder adecuadamente ante una eventual brecha de seguridad (Art. 14 quáter).

3.2.5 Hallazgos Principales del Diagnóstico

El resumen del diagnóstico se encuentra en el Informe de Hallazgos elaborado conforme a la metodología de la Secretaría de Gobierno Digital [18]. Dicho documento institucional es de circulación restringida por lo que no se incorpora como anexo, sus resultados se reproducen a continuación y permiten identificar los siguientes hallazgos principales:

- El 43% de los tratamientos identificados en el IGM involucra datos de categorías sensibles, incluyendo biometría, datos de salud, credo y datos de menores de edad, todos los cuales requieren base de licitud reforzada y medidas de seguridad especiales conforme al artículo 2 letra g) de la Ley N° 21.719.
- Ninguno de los tratamientos cuenta con base de licitud documentada formalmente, lo que impide al IGM demostrar el cumplimiento del principio de responsabilidad proactiva (Art. 13, Ley N° 21.719).
- La mayor parte de los registros del levantamiento no define plazos de conservación, constituyendo una infracción directa al principio de limitación del plazo (Art. 3 g), Ley N° 21.719).
- El sistema SICE, que trata datos biométricos faciales y dactilares del personal, declaró un riesgo de hackeo.
- La arquitectura del ERP institucional, basada en una cuenta SQL compartida sin trazabilidad individual, es incompatible con los principios de seguridad y responsabilidad de la Ley N° 21.719, y su corrección no requiere inversión adicional en software ni hardware, siendo posible subsanar utilizando las herramientas ya disponibles en la infraestructura del IGM.

3.3 Diseño del Modelo de Gestión de Datos Personales MGDGP (OE2)

El diseño del Modelo de Gestión de Datos Personales (MGDGP) corresponde a la fase de Ideación del modelo de *Design Thinking*. A partir de los hallazgos del diagnóstico, se diseñó un modelo que integra los requisitos de la Ley N° 21.719, las mejores prácticas de ISO/IEC 27701 y la estructura de roles de DAMA-DMBOK, adaptados a la realidad del IGM como institución pública. La adopción de la clasificación de roles de DAMA-DMBOK asegura además la compatibilidad del modelo con el Marco de Referencia de Gestión de Datos del Estado (MGDE), por ser este la adaptación de DAMA a los órganos de la Administración del Estado, sin que el MGDE constituya un insumo directo del diseño. El MGDGP se estructura en dos instrumentos principales: el Registro de Actividades de Tratamiento (RAT) y el Modelo Operacional de Protección de Datos.

3.3.1 Estructura del MGDGP

El MGDGP se concibe como un sistema integrado de instrumentos, roles y procedimientos que operan de manera coordinada para garantizar el cumplimiento continuo de la Ley N° 21.719. Su estructura responde a dos dimensiones complementarias: la dimensión documental, que comprende el RAT y las políticas institucionales; y la dimensión operacional, que abarca los procesos, roles y protocolos que hacen viable el cumplimiento en la práctica cotidiana del IGM. El MGDGP se compone de siete elementos, evaluados individualmente en la validación (Tabla 12): la estructura de gobernanza, el RAT, la metodología EIPD, los flujos de atención ARCO+, el modelo de prevención de riesgos, la hoja de ruta de implementación y las políticas y procedimientos institucionales.

3.3.2 Registro de Actividades de Tratamiento (RAT)

El Registro de Actividades de Tratamiento (RAT) es el instrumento central del MGDGP. Conforme al artículo 14 quáter de la Ley N° 21.719, el responsable del tratamiento debe llevar un registro interno de sus actividades de tratamiento, de carácter privado y disponible ante requerimiento de la Agencia de Protección de Datos Personales. El RAT diseñado para el IGM documenta 14 campos obligatorios por cada tratamiento, incluyendo el identificador único, la finalidad, la base de licitud, las categorías de datos e interesados, los destinatarios, los plazos de conservación, las medidas de seguridad y el nivel de riesgo.

A partir del levantamiento de 146 registros individuales, se consolidaron 42 actividades de tratamiento distintas. La Tabla 7 presenta la distribución del RAT por sección:

Área/ Sección	ID Rat	N° Tratamientos	Datos Sensibles
Sección 1 “Personal”	010-011,012-015, 036-040	11	Sí, datos funcionarios, remuneraciones, previsionales
Departamento Comercial (DCOM)	001-003, 031	4	No
Abastecimiento (ABAS)	005-006	2	Sí, información compra pasaje aéreos
Asesoría Jurídica (ASJUR)	007-008	2	No
Biblioteca	026	1	No
Departamento Finanzas (DFZA)	009-011	3	Sí, datos de remuneraciones
Departamento Geográfico (DGEO)	016-018,027,039	5	Sí, datos pasaportes
Departamento Ingeniería (DING)	016,028,033	3	No
Departamento de Producción Gráfica (DPGR)	004	1	No
OFCOM	029,034,039-040	4	Sí, imágenes del personal
Unidad Cuartel- Sanidad (UCTL-Sanidad)	019-020,042	3	Sí, información médica
Control Interno (SECOI)	030	1	No
Sección Informática, Computación y Estadísticas (SICE)	025,032,035,041	4	Sí, información biométrica
Seguridad Militar (SSMO)	021-023	3	Sí, información del personal y videovigilancia
Unidad de Cuartel (UCTL)	024	1	Sí, información biométrica

Tabla 7: Distribución del RAT del IGM por área institucional.

3.3.3 Modelo Operacional de Protección de Datos

El Modelo Operacional es el componente del MGDGP que define cómo el IGM gestionará, protegerá y responderá por los datos personales en su operación diaria. Se estructura en seis componentes interdependientes, descritos a continuación:

1. **Estructura de Gobernanza:** adopta la clasificación de roles de DAMA-DMBOK para distribuir las responsabilidades de protección de datos en tres niveles. Los *Data Owners* (propietarios del dato), correspondientes a los jefes de departamento, son responsables de definir las finalidades y aprobar los tratamientos de su unidad. Los *Data Stewards* (gestores del dato), correspondientes a analistas o profesionales de área, son responsables de la gestión operativa, incluyendo la actualización del RAT y la coordinación de solicitudes de derechos de titulares. Los *Data Custodians* (custodios del dato), correspondientes al Departamento de TI del IGM (SICE), son responsables de la seguridad técnica de la infraestructura.
2. **Delegado de Protección de Datos (DPD):** figura central del Modelo Operacional, responsable de supervisar el cumplimiento de la Ley N° 21.719, asesorar a las unidades del IGM, actuar como punto de contacto oficial ante la Agencia de Protección de Datos, gestionar las solicitudes ARCO+ y coordinar la respuesta ante brechas de seguridad. El DPD ha sido formalmente designado por el IGM, conforme a lo establecido en el artículo 14 ter de

la Ley N° 21.719. Sus datos de contacto deberán ser publicados en el sitio web institucional y comunicados a la Agencia.

3. **Mecanismo de Derechos ARCO+:** define el flujo de atención de solicitudes de titulares de datos. La Ley N° 21.719 amplía el catálogo de derechos respecto a su predecesora, incorporando el derecho de portabilidad (Art. 11 quinquies). El flujo diseñado para el IGM contempla 7 etapas: recepción y generación de ticket, verificación de identidad, análisis de admisibilidad, coordinación con el Responsable de los Datos (*Data Owner*) del área correspondiente, elaboración de respuesta fundada, registro y cierre del caso, y escalamiento a la Agencia en caso de disconformidad del titular. El plazo legal de respuesta es de 30 días hábiles para todos los derechos. A continuación, se presentan los flujos de datos

- **Mecanismo de Ejercicio del Derecho de Acceso:** El proceso (**Figura 5**) se inicia con la recepción de la solicitud por parte del DPD a través del canal oficial habilitado (formulario web o correo institucional). Se evalúa si la solicitud cuenta con los antecedentes mínimos de identificación del titular; de no ser así, se deriva hacia una tarea de requerimiento de información adicional, con un plazo acotado para que el titular complemente su solicitud. Una vez admitida, el DPD coordina con el o los Responsables de Datos (*Data Owners*) de las áreas que figuren en el RAT como responsables de tratamientos asociados al titular.

Luego evalúa si el IGM efectivamente posee datos del titular solicitante. En caso afirmativo, el responsable del dato (*Data Owner*) extrae la información desde los sistemas correspondientes y la consolida en un reporte. Si no existen datos, el proceso termina con una respuesta formal de inexistencia. El DPD elabora la respuesta oficial, la notifica al titular dentro del plazo de 30 días hábiles.

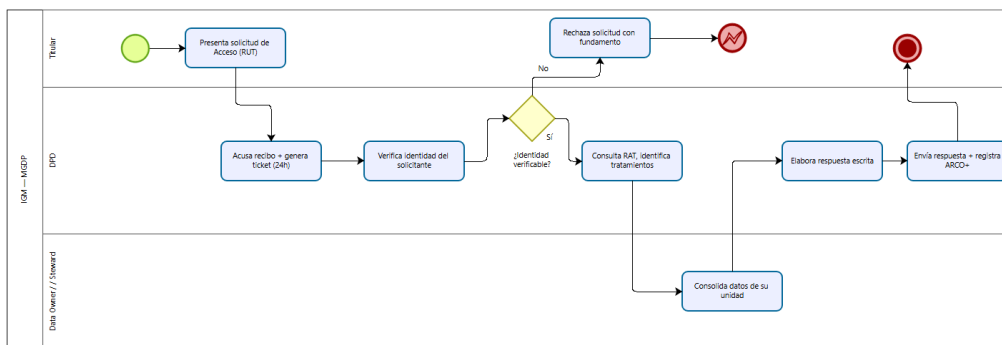


Figura 5: Mecanismo Derecho Acceso

- **Mecanismo de Ejercicio del Derecho de Rectificación:** El proceso para la corrección de datos personales inexactos, incompletos o desactualizados que el IGM posea sobre un titular (**Figura 6**). A diferencia del derecho de acceso, este flujo involucra una modificación efectiva en los sistemas de información, lo que añade una dimensión técnica al proceso y requiere la participación activa del Custodio Técnico de Datos (*Data Custodian*).

Tras la recepción y verificación de identidad del titular, el DPD evalúa la admisibilidad de la solicitud: si los datos cuestionados están sujetos a la ley y son efectivamente incorrectos o incompletos, el proceso avanza hacia la rectificación; si no corresponde rectificar (dato correcto, dato fuera del ámbito de la ley, o dato no poseído por el IGM), el flujo termina con una resolución denegatoria fundada. Se evalúa si el dato rectificado fue transmitido previamente a terceros destinatarios; de ser así, el IGM está obligado por ley a comunicar la rectificación a dichos destinatarios, tarea que recae en el DPD con apoyo del Responsable del Dato (*Data Owner*).

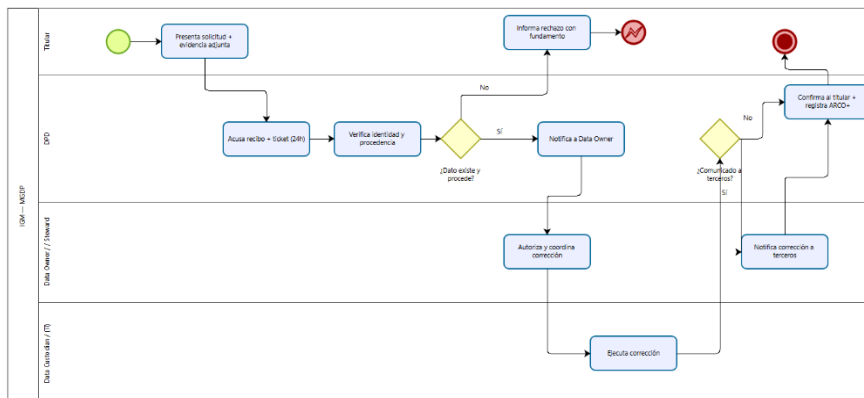


Figura 6: Mecanismo Derecho Rectificación

- **Mecanismo de Ejercicio del Derecho de Cancelación:** EL proceso de cancelación es el proceso más complejo del mecanismo ARCO+ desde la perspectiva técnica, a diferencia de los derechos de acceso y rectificación, la cancelación puede implicar la eliminación definitiva de registros en múltiples sistemas, lo que requiere una verificación previa exhaustiva de si existen obligaciones legales de conservación que primen sobre el derecho del titular.

El flujo (Figura 7) evalúa si los datos que pueden ser suprimidos inmediatamente y aquellos que deben ser bloqueados temporalmente por obligaciones legales de conservación (por ejemplo, datos de remuneraciones sujetos a plazos tributarios o previsionales, o datos de personal militar con retención obligatoria). En el caso de bloqueo, el dato se marca como "bloqueado" en el sistema y no puede ser tratado para ninguna finalidad distinta de la conservación legal, hasta que venza el plazo de retención. Se evalúa si el dato cancelado fue comunicado a destinatarios externos, generando la misma obligación de notificación que en el derecho de rectificación. La ejecución técnica de la supresión requiere la intervención del Custodio Técnico de Datos (*Data Custodian*), quien debe garantizar que la eliminación se realice en todos los sistemas donde el dato esté replicado, incluyendo respaldos y archivos físicos cuando corresponda.

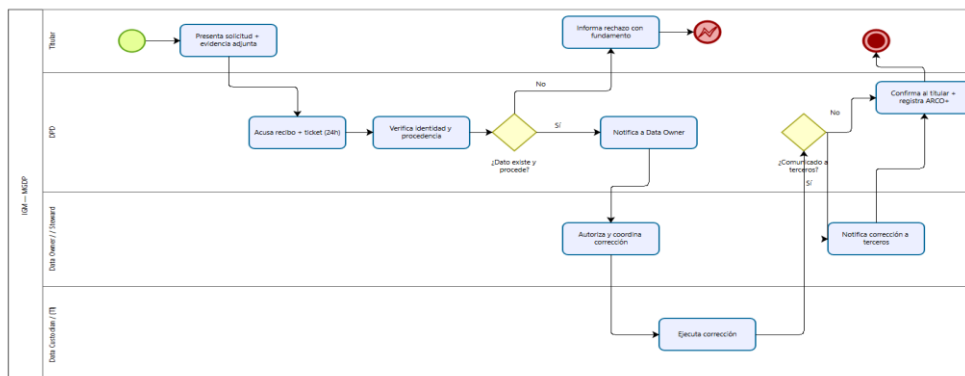


Figura 7: Mecanismo Derecho Cancelación

- **Mecanismo de Ejercicio del Derecho de Oposición:** El proceso de atención del derecho de oposición (Figura 8) permite al titular oponerse a que el IGM continúe tratando sus datos personales en tratamientos específicos. Este derecho tiene una estructura jurídica más compleja que los anteriores, porque no opera automáticamente: el IGM puede rechazar la oposición si demuestra que existen motivos legítimos imperiosos para el tratamiento que prevalecen sobre los intereses del titular.

El flujo contempla evaluación jurídica en la que el DPD, con apoyo del Departamento Jurídico del IGM, analiza si la base de licitud del tratamiento cuestionado admite oposición (los tratamientos basados en obligación legal no son oponibles) y si existen razones imperiosas que justifiquen continuar el tratamiento. Si se acoge la oposición, el Custodio Técnico de Datos (*Data Custodian*) ejecuta la suspensión del tratamiento específico sin eliminar los datos. La suspensión es reversible si las circunstancias cambian.

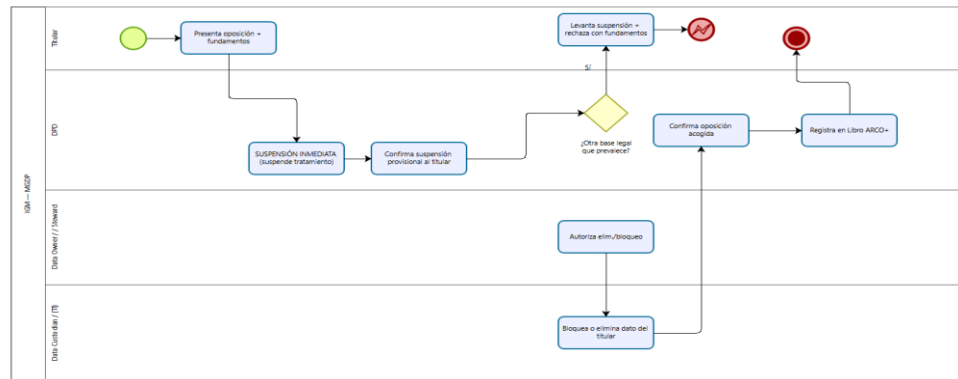


Figura 8: Mecanismo Derecho Oposición

- **Mecanismo de Ejercicio del Derecho de Portabilidad:** El proceso para el ejercicio del derecho de portabilidad, el único derecho nuevo que la Ley N° 21.719 incorpora respecto a su predecesora. Su implementación implica para el IGM no solo entregar los datos al titular, sino hacerlo en un formato técnicamente interoperable (CSV, JSON, XML estructurado), lo que añade un requisito técnico que los demás derechos no tienen.

El flujo (**Figura 9**) es el más lineal de todos los mecanismos ARCO+, porque no contempla la posibilidad de rechazo fundado en obligaciones imperiosas: si el IGM posee los datos y estos fueron proporcionados por el propio titular bajo consentimiento o para la ejecución de un contrato, el derecho de portabilidad es prácticamente irrechazable. Se evalúa únicamente si los datos solicitados caen dentro del ámbito del derecho (datos que el titular proporcionó activamente, no datos derivados o inferidos por el IGM) y si la transmisión directa a un tercero es técnicamente posible.

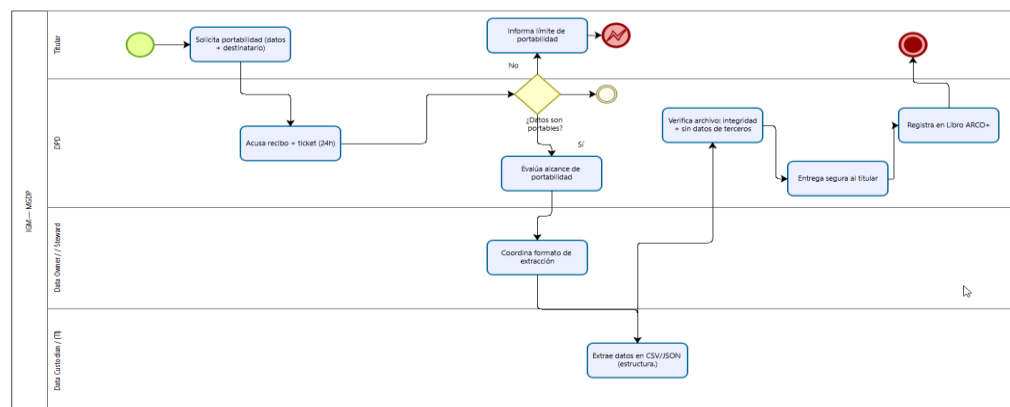


Figura 9: Mecanismo Derecho Portabilidad

- **Proceso de Desarrollo de Software Seguro:** El proceso transversal de incorporación de requisitos de privacidad en el ciclo de vida del desarrollo de software del IGM, en aplicación del principio de *Privacy by Design*. A diferencia de los flujos ARCO+, este proceso no es reactivo (no responde a una solicitud de un titular), sino preventivo: su objetivo es garantizar que ningún nuevo sistema de información sea puesto en producción sin haber evaluado y documentado sus implicancias en la protección de datos personales.

El proceso comienza con el inicio de cualquier proyecto que involucre el tratamiento de datos personales, incluyendo el desarrollo de nuevas aplicaciones, la modificación sustancial de sistemas existentes y la contratación de servicios tecnológicos externos. El DPD actúa como evaluador de privacidad, ejecutando un *checklist* de 8 preguntas obligatorias:

- ¿Qué categorías de datos personales se tratarán?
- ¿Cuál es la base de licitud que ampara el tratamiento?
- ¿Se están tratando solo los datos estrictamente necesarios?
- ¿Quién tendrá acceso a los datos y con qué controles?

- ¿Existe una planificación de auditoría técnica del sistema?
- ¿Se han definido los plazos de conservación y eliminación de los datos?
- ¿El proyecto involucra transferencias internacionales de datos?
- ¿Este proyecto requiere una Evaluación de Impacto en la Protección de Datos (EIPD)?

El diagrama (**Figura 10**) determina si el proyecto requiere Evaluación de Impacto en Protección de Datos (EIPD) obligatoria, conforme a los criterios del artículo 16 de la Ley N° 21.719. Los criterios de activación de EIPD son: tratamiento de datos sensibles a gran escala, uso de tecnologías de vigilancia o geolocalización, decisiones automatizadas con efectos jurídicos, y tratamientos que involucren menores de edad. Si el proyecto no supera la compuerta de EIPD, avanza directamente a la validación técnica de seguridad; si la supera, la EIPD debe completarse y ser aprobada por el DPD antes de proceder al desarrollo.

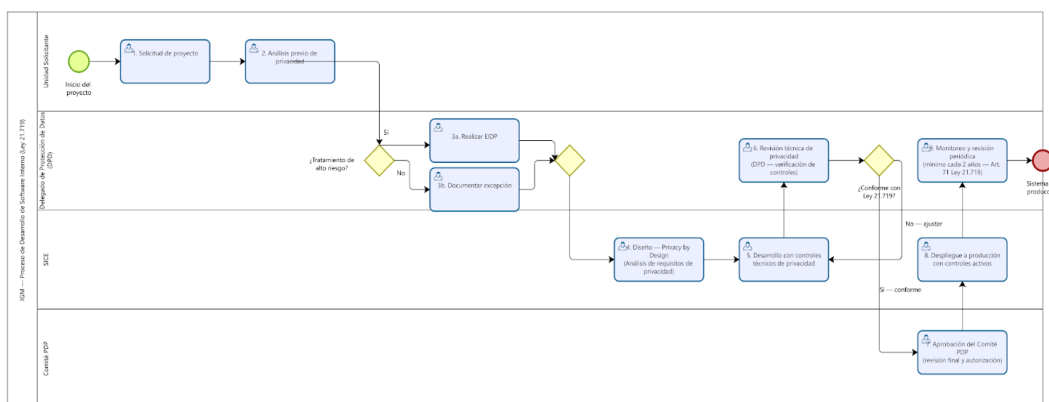


Figura 10: Proceso Desarrollo de Software Seguro

4. **Protocolo de Notificación de Brechas de Seguridad:** Establece el procedimiento de respuesta ante incidentes de seguridad que afecten datos personales, conforme al artículo 14 quáter de la Ley N° 21.719. Las brechas se clasifican en tres niveles (Crítica, Significativa y Menor) según el tipo y volumen de datos afectados y el riesgo para los titulares. Para brechas de nivel Crítico y Significativo, el protocolo contempla la notificación obligatoria a la Agencia dentro de un plazo máximo de 72 horas desde que se tomó conocimiento de la brecha, y la notificación a los titulares afectados sin demora indebida cuando el riesgo para sus derechos sea alto.
5. **Privacy by Design:** Integra los siete principios de privacidad desde el diseño en los procesos de desarrollo e implementación de nuevos sistemas del IGM. El componente establece un *checklist* de 8 preguntas que debe ser respondido afirmativamente antes de la aprobación de cualquier nuevo proyecto que involucre datos personales, garantizando que la protección de la privacidad se incorpore desde la concepción y no como una medida correctiva posterior. Adicionalmente, se identifican los tratamientos que requieren Evaluación de Impacto en Protección de Datos (EIPD) obligatoria según los criterios del artículo 16 de la Ley N° 21.719, cuya metodología de ejecución se describe a continuación:
 - **Metodología de Evaluación de Impacto en la Protección de Datos (EIPD):** La EIPD es el instrumento establecido en el artículo 16 de la Ley N° 21.719 para evaluar, antes de iniciar un tratamiento de alto riesgo, el impacto que dicho tratamiento puede producir sobre los derechos y libertades de los titulares. Su ejecución es obligatoria cuando concurre al menos uno de los criterios de activación definidos por la ley y no puede ser sustituida por otras medidas de seguridad.
 - **Criterios de activación obligatoria (Art. 16, Ley N° 21.719):** La obligación de realizar una EIPD se activa cuando el tratamiento proyectado cumple al menos uno de los siguientes criterios, verificados por el DPD en el *checklist* de Privacy by Design:
 - **Tratamiento de datos sensibles a gran escala:** Datos de salud, datos biométricos, datos relativos a condenas o infracciones penales, o cualquier categoría sensible del artículo 4 de la ley, cuando el volumen o la sistematicidad del tratamiento genere un riesgo elevado para los titulares.
 - **Uso de tecnologías de vigilancia o geolocalización:** sistemas de reconocimiento facial, huella dactilar, cámaras de vigilancia sistemática, rastreo de ubicación o cualquier tecnología que permita el seguimiento de personas en espacios públicos o de acceso controlado.

- **Decisiones automatizadas con efectos jurídicos o significativos:** elaboración de perfiles que produzca efectos jurídicos sobre el titular o le afecte de modo igualmente significativo, incluyendo la denegación automática de acceso a servicios o la evaluación sistemática del desempeño.
- **Tratamientos que involucren datos de menores de edad:** cualquier tratamiento sistemático de datos personales de personas menores de 14 años, o de menores de 18 años cuando el tratamiento pueda afectar su desarrollo, privacidad o seguridad.
- **Fases del procedimiento EIPD.** Una vez verificada la obligación de EIPD, el Delegado de Protección de Datos (DPD) coordina su ejecución en cuatro fases estructuradas. El Responsable de Datos (*Data Owner*) del tratamiento evaluado actúa como contraparte y provee la información necesaria para cada fase (Figura 11):

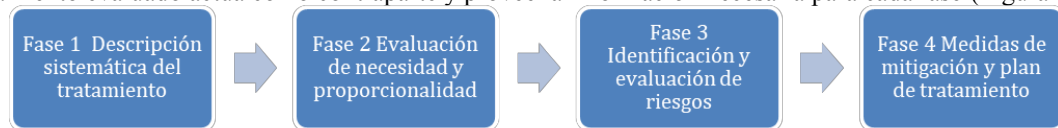


Figura 11: Fases del Procedimiento EIPD

- **Fase 1 Descripción sistemática del tratamiento:** Se documenta con precisión la naturaleza, finalidad, alcance y contexto del tratamiento. Esto incluye las categorías de datos tratados, los flujos de datos internos y externos, los sistemas de información involucrados, los encargados del tratamiento, los plazos de conservación y la base de licitud que ampara el tratamiento. El insumo principal es la ficha RAT correspondiente, incluyendo entrevistas al Responsable de Datos y al Custodio Técnico (*Data Custodian*) del sistema involucrado.
- **Fase 2 Evaluación de necesidad y proporcionalidad:** Se verifica que el tratamiento es adecuado, necesario y proporcional respecto a su finalidad declarada. Se examina la aplicación del principio de minimización de datos, la relación entre la finalidad y la base de licitud, la posibilidad de alcanzar los mismos objetivos con datos menos sensibles o en menor volumen, y la existencia de medidas técnicas de seudonimización o anonimización aplicables.
- **Fase 3 Identificación y evaluación de riesgos para los derechos de los titulares:** Se identifican las amenazas específicas del tratamiento sobre los derechos y libertades de los titulares, distinguiendo entre riesgos de acceso ilegítimo, modificación no autorizada y pérdida o destrucción de los datos. Cada riesgo se valora en función de su probabilidad de materialización y la gravedad de sus consecuencias para los titulares, utilizando la escala ordinal del Modelo de Prevención del MGD (Crítico, Alto, Medio, Bajo).
- **Fase 4 Medidas de mitigación y plan de tratamiento de riesgos:** Para cada riesgo identificado en la fase anterior, el DPD define medidas técnicas y organizativas específicas orientadas a reducir la probabilidad o la gravedad del riesgo a un nivel residual aceptable. Las medidas se clasifican en controles preventivos (que reducen la probabilidad), controles de detección (que reducen el tiempo de exposición) y controles correctivos (que mitigan las consecuencias). El plan de tratamiento asigna responsable, plazo y recursos estimados para cada medida, y es aprobado formalmente por el Responsable de Datos antes de que el tratamiento sea autorizado para operar.
- **Estructura del informe EIPD.** El resultado de las cuatro fases se consolida en un informe formal que constituye el documento acreditativo de cumplimiento del artículo 16 de la ley. El informe EIPD del IGM contiene: (a) identificación del tratamiento evaluado y referencia al RAT correspondiente; (b) descripción sistemática del tratamiento con flujo de datos; (c) juicio de necesidad y proporcionalidad; (d) mapa de riesgos con valoración de probabilidad e impacto; (e) plan de medidas de mitigación con responsables y plazos; (f) conclusión del DPD sobre la viabilidad del tratamiento; y (g) decisión formal del Responsable de Datos autorizando, condicionando o rechazando el tratamiento. El informe se archiva en el sistema de gestión documental del IGM, permanece disponible ante requerimiento de la Agencia y se revisa periódicamente o ante cambios sustanciales en el tratamiento.
- **Consulta previa obligatoria a la Agencia.** Cuando la EIPD concluye que el tratamiento presenta riesgos residuales altos que no pueden mitigarse con las medidas disponibles en el IGM, el artículo 16 inciso final de la Ley N° 21.719 impone la obligación de consultar previamente a la Agencia de Protección de Datos Personales antes de iniciar el tratamiento. En este supuesto, el DPD remite a la Agencia el informe EIPD completo junto con las medidas de mitigación propuestas, y el tratamiento queda suspendido hasta la respuesta de la Agencia o hasta el transcurso del plazo legal sin pronunciamiento, lo que habilita al IGM a continuar

conforme a sus propias medidas de mitigación documentadas.

6. **Clasificación de Datos:** Define la matriz de clasificación aplicable al IGM, distinguiendo tres categorías: datos públicos (no sujetos a la ley, como el RUT de personas jurídicas o el número de cuenta corriente institucional), datos personales (sujetos a la ley) y datos sensibles (subconjunto con protección reforzada). La matriz aborda también casos especiales identificados en el levantamiento, incluyendo las Empresas Individuales de Responsabilidad Limitada (EIRL) con nombre de persona natural, los documentos publicados por obligación de transparencia que contienen datos personales, y el uso de fotografías del personal en difusión institucional pública.

La identificación de los tratamientos que requieren EIPD obligatoria se realizó mediante la aplicación de los criterios del artículo 16 de la Ley N° 21.719 a la totalidad de los 42 tratamientos registrados en el RAT institucional. Esta aplicación incorpora el tratamiento RAT-024 (control biométrico dactilar de la UCTL), no considerado en el Informe de Hallazgos [18], por tratarse de datos biométricos cuya base de licitud no se encuentra acreditada, en los mismos términos que el RAT-025. Un tratamiento activa la obligación de EIPD cuando cumple al menos uno de los cuatro criterios legales. De los 42 tratamientos evaluados, **7 activan la obligación de EIPD** conforme a los criterios que se presentan en la Tabla 8:

N°	RAT	Tratamiento	Criterio Art. 16 que activa la EIPD	Depto.
1	010	Pago de Remuneraciones del Personal	Datos sensibles a gran escala: situación socioeconómica y afiliación previsional y de salud (AFP, Isapre/Fonasa) de la totalidad del personal; tratamiento base de la visualización de liquidaciones en intranet (RAT-038).	DFZA / S-1
2	015	Archivo Digital y Físico de Personal (CAP/TAP/HAO)	Datos sensibles a gran escala: múltiples categorías simultáneas (religión, grupo sanguíneo, fotografía, demandas judiciales, datos familiares, remuneratorios y previsionales) correspondientes a la totalidad del personal en servicio activo y en retiro.	S-1
3	019	Atención de Salud -Fichas Clínicas Anuales	Datos de salud a gran escala: datos clínicos completos (diagnósticos, enfermedades crónicas, resultados de laboratorio, resoluciones médicas) de la totalidad del personal; máxima categoría de sensibilidad conforme al Art. 2 letra g).	SANIDAD
4	022	Sistema de Videovigilancia - Cámaras CCTV	Tecnología de vigilancia sistemática: captación de imagen en tiempo real con potencial de reconocimiento facial biométrico; cubre la totalidad del personal, visitantes y terceros en instalaciones institucionales.	SSMO
5	024	Control Biométrico Dactilar de Asistencia - UCTL	Datos biométricos (huella dactilar): máxima categoría de sensibilidad conforme al Art. 2 letra g); base de licitud pendiente de definición legal; ausencia de mecanismo de oposición documentado	UCTL
6	025	Sistema Biométrico SICE - Control Facial y Dactilar	Datos biométricos de doble modalidad (reconocimiento facial + huella dactilar): máxima categoría de sensibilidad; riesgo de hackeo declarado por la unidad; medidas de seguridad calificadas como insuficientes en el diagnóstico.	SICE / S-1
7	038	Visualización de Liquidaciones de Sueldo	Datos sensibles de afiliación previsional y de salud (AFP, Isapre/Fonasa) que revelan el sistema de salud del funcionario; clasificados erróneamente como no sensibles en el inventario original y corregidos en el RAT definitivo.	S-1 / SICE

Tabla 8: Tratamientos que requieren EIPD obligatoria conforme al Art. 16, Ley N° 21.719

3.3.4 Alineación del MGDGP con ISO/IEC 27701 y Ley N° 21.719

El MGDGP diseñado para el IGM se alinea con los requisitos de la ISO/IEC 27701 en sus aspectos fundamentales. La Tabla 9 presenta la correspondencia entre los componentes del MGDGP, los controles de ISO/IEC 27701 y los artículos de la Ley N° 21.719 que cada uno aborda:

Componente MGDGP	Control ISO/IEC 27701	Artículo Ley N° 21.719
RAT 42 tratamientos documentados	7.2.8 Registros de tratamiento de IIP	Art. 14 quáter
Gobernanza. roles DAMA	5.2 Roles y responsabilidades; 6.2.1 Responsable del tratamiento	Art. 3 k); Art. 13
DPD designado	6.2.1.2 Encargado de protección de datos	Art. 14 ter

Mecanismo ARCO+	7.3 Derechos del interesado	Art. 11 y ss.
Protocolo de brechas	6.13.1.2 Notificación de violaciones de datos	Art. 14 quáter
Privacy by Design	7.4 Evaluación del impacto sobre la privacidad	Art. 16
Clasificación de datos	7.2.2 Inventario de IIP y base de licitud	Art. 2; Art. 12

Tabla 9: Alineación del MGDGP con ISO/IEC 27701 y Ley N° 21.719.

3.3.5 Modelo de Prevención de Riesgos

El Modelo de Prevención de Riesgos identifica, clasifica y asigna tratamiento a los riesgos de incumplimiento de la Ley N° 21.719 derivados del diagnóstico institucional (OE1). Estos se identificaron a partir de los riesgos asociados declarados en la Matriz de Levantamiento (146 registros), del análisis de brechas respecto del checklist del Art. 14 ter y del diagnóstico técnico del ERP, y se consolidaron en el Informe de Hallazgos [18].

Cada riesgo se clasifica en una escala ordinal de cuatro niveles, construida sobre los criterios de gestión de riesgos de ISO 31000 e ISO/IEC 27005 y sobre la graduación de infracciones de la Ley N° 21.719:

- **Crítico:** compromete datos sensibles o biométricos a gran escala, o impide acreditar el cumplimiento ante un incidente de seguridad. Expone a infracciones gravísimas (hasta 20.000 UTM) y requiere acción inmediata.
- **Alto:** afecta datos sensibles con controles insuficientes, clasificación incorrecta o sin una política que regule su tratamiento. Expone a infracciones graves (hasta 10.000 UTM) y se aborda en el corto y mediano plazo.
- **Medio:** incumplimiento documental o contractual sin exposición directa de datos sensibles. Se aborda en el mediano y largo plazo.
- **Bajo:** incumplimiento formal de menor entidad, sin afectación de los derechos de los titulares. Se gestiona en las revisiones periódicas del RAT. El diagnóstico no identificó riesgos de este nivel.

La Tabla 10 presenta los 10 riesgos identificados, su nivel, los tratamientos afectados, las disposiciones de la ley comprometidas y el componente del MGDGP que los mitiga:

N°	Nivel	Riesgo	Tratamientos	Ley N° 21.719	Componente del MGDGP que lo mitiga
R-01	Crítico	Vulneración del sistema biométrico SICE, cuyo equipo operador declaró riesgo de hackeo	RAT-025	Art. 2 g), Art. 16	Metodología EIPD; Hoja de ruta
R-02	Crítico	Imposibilidad de acreditar trazabilidad de accesos en el ERP por uso de cuenta SQL compartida	Tratamientos soportados por el ERP	Art. 13, Art. 14 sexies	Hoja de ruta (arquitectura técnica objetivo)
R-03	Crítico	Ausencia de inventario y control de accesos administrativos en sistemas web e intranet	RAT-031 a RAT-042	Art. 14 quinquies	Estructura de gobernanza; Políticas y procedimientos
R-04	Alto	Tratamiento de datos sensibles sin política de tratamiento aprobada y publicada	18 tratamientos con datos sensibles	Art. 14 ter	Políticas y procedimientos
R-05	Alto	Datos de salud del personal sin controles de acceso diferenciados	RAT-013, RAT-019, RAT-020	Art. 14 quinquies, Art. 16	Metodología EIPD; Políticas y procedimientos
R-06	Alto	Remuneraciones y afiliación previsional clasificadas erróneamente como datos no sensibles en la intranet	RAT-038	Art. 2 g), Art. 16	RAT; Metodología EIPD
R-07	Alto	Imposibilidad de acreditar trazabilidad de acciones administrativas en sistemas web e intranet	RAT-031 a RAT-042	Art. 13, Art. 14 sexies	Políticas y procedimientos
R-08	Medio	Transferencias internacionales sin base legal documentada ni contrato de encargado	RAT-006, 017, 027, 031, 032, 037	Art. 25	RAT; Políticas y procedimientos
R-09	Medio	Datos de clientes en comercio electrónico y formularios web sin contrato de encargado formalizado	RAT-031, RAT-032	Art. 14 bis	Estructura de gobernanza; Políticas y procedimientos

Nº	Nivel	Riesgo	Tratamientos	Ley N° 21.719	Componente del MGDGP que lo mitiga
R-10	Medio	Publicación de decretos y resoluciones con datos personales sin anonimización previa	Documentos publicados por transparencia	Ley N° 20.285 y Ley N° 21.719	Políticas y procedimientos (clasificación de datos)

Tabla 10: Modelo de prevención de riesgos del IGM. Fuente: elaboración propia a partir del Informe de Hallazgos [18].

La distribución resultante es de 3 riesgos críticos, 4 altos y 3 medios. Los riesgos críticos se concentran en sistemas que tratan datos biométricos o que carecen de trazabilidad de accesos, lo que explica que las acciones de horizonte inmediato del *roadmap* se dirijan a la auditoría del SICE y a la contención del ERP. Cada riesgo queda asociado al menos a un componente del MGDGP, de modo que el modelo cubre la totalidad de los riesgos identificados en el diagnóstico. La misma escala se aplica en la Fase 3 de la EIPD para valorar los riesgos específicos de cada tratamiento sujeto a evaluación de impacto.

3.3.6 Políticas y Procedimientos Institucionales

Este componente reúne los instrumentos normativos internos que formalizan el MGDGP y le otorgan obligatoriedad dentro del IGM. Mientras los componentes anteriores definen qué se gestiona y cómo, las políticas y procedimientos determinan quién los aprueba, desde cuándo rigen y cómo se actualizan, condición sin la cual el modelo carece de exigibilidad interna y el Instituto no puede acreditar el principio de responsabilidad del artículo 14 de la Ley N° 21.719.

Este elemento se compone de la Política de Tratamiento de Datos Personales y de los procedimientos operativos definidos en el Modelo Operacional (Sección 3.3.3):

- Política de Tratamiento de Datos Personales: instrumento de carácter público que informa a los titulares cómo el IGM trata sus datos personales. Cierra la brecha del ítem 1 del checklist del Art. 14 ter (Tabla 5).
- Procedimiento de atención de derechos ARCO+: formaliza el flujo de siete etapas y el plazo de 30 días hábiles para las solicitudes de los titulares.
- Procedimiento de Evaluación de Impacto en Protección de Datos: establece los criterios de activación del artículo 16 y las cuatro fases de la evaluación.
- Protocolo de Notificación de Brechas de Seguridad: define la detección, contención, notificación a la Agencia y comunicación a los titulares afectados.
- Proceso de Desarrollo de Software Seguro: incorpora los requisitos de privacidad desde el diseño en el ciclo de desarrollo de los sistemas institucionales.
- Matriz de Clasificación de Datos: distingue datos públicos, personales y sensibles, y fija el tratamiento aplicable a cada categoría.

La Política de Tratamiento de Datos Personales es el instrumento central de este componente, por cuanto consolida en un documento público la información que la ley exige poner a disposición de los titulares. Su contenido mínimo se estructura a partir de los ítems del *checklist* del artículo 14 ter (Tabla 5):

- Identificación del responsable del tratamiento y datos de contacto del DPD (ítem 2).
- Canal oficial para el ejercicio de derechos ARCO+, derecho a recurrir ante la Agencia y derecho a retirar el consentimiento (ítems 3, 6, 7 y 11).
- Categorías de datos y de titulares, destinatarios, finalidades, bases de licitud y fuente de procedencia, obtenidas del RAT (ítems 4 y 10).
- Medidas de seguridad adoptadas para la protección de las bases de datos (ítem 5).
- Transferencias internacionales y nivel de protección del país de destino (ítem 8).
- Plazos de conservación de los datos personales (ítem 9).
- Declaración sobre la existencia de decisiones automatizadas o elaboración de perfiles (ítem 12).

La política se formaliza mediante acto administrativo del Director del IGM, se publica en el sitio web institucional indicando fecha y versión, y se actualiza en conjunto con las revisiones periódicas del RAT, de modo que la información publicada refleje en todo momento los tratamientos vigentes. Su redacción no forma parte del alcance de este trabajo: el *roadmap* de implementación (Tabla 11) la sitúa como acción de prioridad alta en el mediano plazo, y el MGDGP define aquí su estructura, contenido mínimo y mecanismo de aprobación.



Este componente concentra, además, la mitigación de la mayor parte de los riesgos identificados en el Modelo de Prevención (Tabla 10): la política de tratamiento aborda el riesgo R-04, los procedimientos de accesos y trazabilidad los riesgos R-03 y R-07, la documentación de transferencias y los contratos de encargado los riesgos R-08 y R-09, y la matriz de clasificación de datos el riesgo R-10.

3.4 Roadmap de Implementación (OE3)

El *roadmap* de implementación corresponde a la fase de Prototipado del modelo de *Design Thinking*. Su objetivo es proporcionar al IGM una ruta viable, priorizada y compatible con sus recursos institucionales para adoptar el MGDGP antes de la entrada en vigor de la Ley N° 21.719 el 1 de diciembre de 2026. El *roadmap* se estructura en 4 horizontes temporales que permiten una transición ordenada, priorizando en primer lugar las acciones de mayor impacto en el cumplimiento y menor requerimiento de recursos.

3.4.1 Arquitectura Técnica Objetivo

La solución estructural para las brechas técnicas del ERP consiste en migrar la autenticación desde el modelo actual de cuenta SQL compartida hacia *Windows Authentication* integrada con *Active Directory*, de modo que cada funcionario se conecte a SQL Server con sus propias credenciales de dominio. Esto habilita la segregación de permisos a nivel de base de datos, la trazabilidad individual de accesos y la activación de SQL Server Audit para las tablas que contienen datos personales. El plan de mitigación fue diseñado por la Sección de Informática del IGM y estima un tiempo de implementación total de 8 semanas utilizando exclusivamente herramientas y recursos ya disponibles en la infraestructura institucional, sin requerir inversión adicional en software ni hardware.

3.4.2 Fases de Implementación

La Tabla 11 presenta las acciones priorizadas del *roadmap*, organizadas por horizonte temporal y nivel de prioridad:

Horizonte	Acción	Descripción	Prioridad
Inmediato (0–4 semanas)	Auditoría SICE	Revisión técnica del sistema biométrico SICE dado el riesgo de hackeo declarado. Determinar si existe brecha activa.	URGENTE
Inmediato (0–4 semanas)	Contención ERP	Restricción de red al servicio de base de datos, registro de accesos en la aplicación y migración de contraseñas a un algoritmo de hash robusto con salt.	ALTA
Corto plazo (1–3 meses)	Designación DPD	Formalización mediante resolución exenta del Director IGM. Publicación de datos de contacto.	ALTA
Corto plazo (1–3 meses)	Migración Windows Auth	Creación de grupos AD, logins Windows, roles SQL Server con permisos granulares por perfil funcional.	ALTA
Corto plazo (1–3 meses)	Consulta biometría	Obtención de dictamen jurídico (Depto. Jurídico IGM + Contraloría) sobre base legal de sistemas biométricos.	ALTA
Mediano plazo (3–6 meses)	Canal ARCO+	Habilitación de formulario web y correo oficial para solicitudes de derechos de titulares.	ALTA
Mediano plazo (3–6 meses)	SQL Server Audit	Activación de auditoría nativa en tablas con datos personales. Registro de accesos individual e inalterable.	ALTA
Mediano plazo (3–6 meses)	Política de privacidad	Elaboración y publicación de Política de Tratamiento de Datos Personales (cierre brecha ítem 1, Art. 14 ter).	ALTA
Largo plazo (6–9 meses)	EIPDs obligatorias	Elaboración de las 7 Evaluaciones de Impacto: RAT-010, RAT-015, RAT-019, RAT-022, RAT-024, RAT-025 y RAT-038	MEDIA
Largo plazo (9–12 meses)	Capacitación	Capacitación de Data Owners, Stewards y Custodians en principios Ley N° 21.719 y Modelo Operacional.	MEDIA

Tabla 11: Roadmap de implementación del MGDGP en el IGM.

Las acciones del *roadmap* presentan dependencias críticas que determinan su secuencia. En primer lugar, la contención del ERP es condición previa de la migración a *Windows Authentication* y esta, a su vez, de la activación de SQL Server Audit, ya que la auditoría solo registra accesos individuales una vez eliminada la cuenta compartida. En segundo lugar, la designación formal del DPD precede a la política de privacidad, al canal ARCO+ y a las EIPD, que requieren su coordinación y la publicación de sus datos de contacto. En tercer lugar, la consulta jurídica sobre biometría se resuelve en el corto plazo porque condiciona la EIPD del RAT-025 y las decisiones derivadas de la auditoría del SICE, al definir si existe base legal para mantener dicho tratamiento. Finalmente, la política de privacidad depende del RAT consolidado, del cual obtiene las finalidades, bases de licitud y plazos de conservación que debe informar a los titulares.

4 Validación de la Propuesta

4.1 Metodología de Validación

La evaluación del impacto potencial del *framework* MGDGP se realizó mediante juicio experto, utilizando un instrumento estructurado (**Anexo 3**) en tres partes: perfil del evaluador, evaluación por componente en escala Likert de 1 a 5, y juicio global con preguntas abiertas. El instrumento fue diseñado conforme a los criterios del Objetivo Específico 4 y aplicado en septiembre de 2026. Se convocaron dos evaluadores con perfiles complementarios, identificados como E1 y E2.

El **Evaluador E1** es profesional del área de transformación digital y cumplimiento normativo, con cargo de Jefe de Desarrollo Digital en una empresa del sector privado regulado y dos años de experiencia en protección de datos personales y ciberseguridad. Declara conocimiento en profundidad de la Ley N° 21.719. Se deja constancia de que E1 mantiene vínculo familiar con el investigador; en atención a ello, solicitó que su identidad sea mantenida en reserva. La idoneidad técnica de E1 para pronunciarse sobre viabilidad de implementación y cumplimiento normativo se fundamenta en su experiencia práctica en programas de protección de datos en el sector privado, contexto comparable al del IGM en términos de obligaciones bajo la Ley N° 21.719.

El **Evaluador E2** es Sergio Cornejo Alvarado, Gerente de TI de Detacoop, con más de 24 años de experiencia en protección de datos, ciberseguridad y cumplimiento normativo. Cuenta con certificación CISM (ISACA, 2012), Diplomado en Gestión de Seguridad TI (Universidad de Chile, 2011), ITIL v3 *Foundation*, y Magister en Tecnologías de la Información de la Universidad Técnica Federico Santa María. Declara conocimiento en profundidad de la Ley N° 21.719 y autorizó el uso de sus datos en el informe.

4.2 Resultados

La Tabla 12 presenta las puntuaciones asignadas por E1 y E2 (viabilidad e impacto) a cada componente del MGDGP, junto con el promedio entre ambos evaluadores.

N°	Componente del MGDGP	E1 Via	E1 Imp	E2 Viab	E2 Imp	Prom Viab	Prom Imp	Prom Global
1	Estructura de gobernanza de datos	3	5	4	5	3,5	5,0	4,25
2	Registro de Actividades de Tratamiento (RAT)	5	5	4	5	4,5	5,0	4,75
3	Metodología EIPD	4	5	3	4	3,5	4,5	4,0
4	Flujos de atención ARCO+	3	4	3	3	3,0	3,5	3,25
5	Modelo de prevención de riesgos	3	5	4	4	3,5	4,5	4,0
6	Hoja de ruta de implementación	3	5	2	1	2,5	3,0	2,75
7	Políticas y procedimientos institucionales	4	5	4	3	4,0	4,0	4,0
	Promedio general	3,57	4,86	3,43	3,57	3,50	4,21	3,86

Tabla 12: Evaluación Juicio Experto E1 Y E2.

El promedio consolidado de viabilidad es 3,50 sobre 5, indicando que el *framework* es medianamente viable a viable en su conjunto. El RAT obtiene la mayor viabilidad consolidada (4,5), dado que el levantamiento ya fue ejecutado durante el proceso de investigación. El componente de menor viabilidad consolidada es la hoja de ruta (2,5), donde ambos evaluadores coinciden en señalar restricciones de plazo e incertidumbre regulatoria como factores limitantes.

El promedio consolidado de impacto es 4,21 sobre 5. El RAT y la estructura de gobernanza lideran en impacto (5,0 consolidado), mientras que la hoja de ruta registra el impacto más bajo (3,0 consolidado), explicado por la divergencia entre E1 (5,0) y E2 (1,0) la mayor divergencia del instrumento.

4.3 Comentarios

Respecto a la cobertura normativa del *framework* (pregunta 3.1), ambos evaluadores coinciden en que el MGDGP cubre los requisitos esenciales de la Ley N° 21.719. E1 destaca la definición de roles, políticas, derechos ARCO+ y las evaluaciones de impacto. E2, con mayor distancia institucional del IGM, señala que el *framework* se ajusta a lo que organizaciones similares han implementado para adaptarse al nuevo marco normativo y legal, infiriendo que cubriría los requisitos esenciales.

Respecto a las mejoras identificadas (pregunta 3.2), los evaluadores formularon observaciones complementarias:

- **E1:** incorporar cláusulas de protección de datos en licitaciones públicas (ChileCompra); evaluar alternativas no biométricas para titulares que ejerzan oposición; desarrollar tablas de retención documental; complementar el RAT con inventario de datos a nivel de aplicación incluyendo métodos de supresión.



- **E2:** fortalecer el modelo mediante la agrupación de datos por familias y dominios, lo que permitiría que los responsables de datos se mantengan alineados a nivel de familia y dominio, haciendo el modelo de gobierno más robusto en el tiempo.

Respecto al grado de cumplimiento estimado (pregunta 3.3), los evaluadores divergen significativamente:

- **E1** seleccionó Cumplimiento sustancial (70–89%), condicionando su estimación al compromiso de la dirección y a las directrices que emita la APDP una vez operativa.
- **E2** seleccionó Cumplimiento mínimo (< 40%), argumentando que el *framework* apoya la capa de gobierno y la planificación de tareas, pero no aborda los desafíos de automatización sistémica en sistemas y repositorios de datos.

Esta divergencia es relevante y refleja perspectivas complementarias: **E1** evalúa el cumplimiento desde la dimensión de gobernanza y gestión normativa, donde el MGDGP es sólido; **E2** lo evalúa desde la dimensión de implementación técnica sistémica, donde el *framework*, por diseño, no entra al detalle de la automatización en cada sistema, lo que E2 considera una condición necesaria para el cumplimiento efectivo. Ambas lecturas apuntan a una misma conclusión: el MGDGP es condición necesaria pero no suficiente para el cumplimiento pleno, requiriendo en paralelo un programa de adecuación técnica de los sistemas del IGM.

Los resultados consolidados del juicio experto permiten concluir que el *framework* MGDGP es técnicamente viable (promedio 3,50) y tiene impacto sustancial esperado en el cumplimiento de la Ley N° 21.719 (promedio 4,21). La divergencia en la estimación del grado de cumplimiento entre E1 (70–89%) y E2 (<40%) no invalida el *framework*, la explicita como condición necesaria pero insuficiente sin adecuación técnica sistémica paralela, lo que constituye un hallazgo de la investigación e informa directamente las recomendaciones de trabajo futuro. El componente de mayor solidez consolidada es el RAT (4,75), y el de mayor riesgo de implementación es la hoja de ruta (2,75), donde el plazo a diciembre 2026 es cuestionado por ambos evaluadores desde ángulos distintos.

5 Conclusiones

5.1 Conclusiones por objetivos específicos

A continuación, se presentan las conclusiones por objetivos específicos:

1. **Diagnostico Institucional (OE1):** El levantamiento confirmó que el IGM trata datos personales de alta sensibilidad sin un marco formal de gobernanza. Los 146 registros consolidados en 42 tratamientos activos revelan que la institución opera con una estructura de datos atomizada, distribuida en 26 departamentos y secciones sin criterios unificados de clasificación ni documentación de flujos. El análisis de brechas identificó 11 ítems de incumplimiento respecto al Art. 14 ter, de los cuales 5 corresponden a **brecha parcial**, con elementos concretos verificables pero condiciones no cumplidas y el resto corresponde a **brecha total**. El diagnóstico técnico del ERP evidenció 3 hallazgos de criticidad **crítica** directamente vinculados a los artículos 14 quinquies y 14 sexies: cuenta SQL compartida sin trazabilidad individual, seguridad concentrada exclusivamente en la capa de presentación VB6 y credenciales hardcodeadas en código fuente. Estos hallazgos confirman que la arquitectura actual del ERP es incompatible con los principios de seguridad y responsabilidad de la Ley N° 21.719.
2. **Diseño del MGDGP (OE2):** El *framework* diseñado demuestra que es posible construir un modelo de gobernanza de datos personales alineado con la Ley N° 21.719 e ISO/IEC 27701 utilizando exclusivamente los recursos existentes del IGM. La estructura de tres roles (Responsable de Datos, Administrador de Datos y Custodio Técnico) operacionaliza las responsabilidades del Art. 14 sexies sin requerir nuevas contrataciones. La metodología EIPD de 4 fases habilita el cumplimiento del Art. 16 para los 7 tratamientos que activan obligación legal, todos correspondientes a datos biométricos, de salud o vigilancia sistemática. Los 5 flujos ARCO+ formalizados establecen plazos y responsables concretos para dar cumplimiento a los derechos del Título III de la ley.
3. **Roadmap (OE3):** El *roadmap* propuesto es viable en el escenario realista si el IGM prioriza el cierre de las tres brechas de mayor urgencia legal antes de diciembre de 2026: habilitación del canal ARCO+, aprobación de la política de privacidad y resolución de la consulta jurídica sobre biometría. La corrección de los hallazgos **críticos** del ERP no requiere inversión adicional en software ni hardware, lo que elimina la principal barrera económica de implementación.
4. **Validación (OE4):** La evaluación del *framework* por dos expertos con perfiles complementarios arrojó un promedio consolidado de viabilidad de 3,50 e impacto de 4,21 en una escala de máximo 5. La divergencia en la estimación del grado de cumplimiento (E1: sustancial, 70–89%; E2: mínimo, <40%) refleja dos perspectivas

igualmente válidas: E1 evalúa desde la dimensión de gobernanza normativa, donde el MGDGP es sólido; E2 lo evalúa desde la dimensión de implementación técnica sistémica, donde el *framework* no cubre la automatización en sistemas y repositorios de datos. Esta divergencia constituye un hallazgo en sí mismo: el MGDGP es condición necesaria pero no suficiente para el cumplimiento pleno, requiriendo en paralelo un programa de adecuación técnica de los sistemas del IGM.

5.2 Conclusión general

La hipótesis de investigación se valida parcialmente. El *framework* MGDGP diseñado proporciona los mecanismos de gobernanza, procedimientos operativos y capacidades institucionales necesarias para avanzar hacia el cumplimiento de la Ley N° 21.719 dentro de las restricciones de recursos del IGM. Sin embargo, el juicio experto evidencia que el cumplimiento pleno ($\geq 90\%$) requiere adicionalmente un programa de adecuación técnica sistémica que automatice los controles en cada sistema y repositorio de datos del IGM, dimensión que excede el alcance del presente trabajo pero que el MGDGP habilita como paso siguiente natural. En este sentido, el MGDGP cumple su propósito como marco de gobernanza fundacional sobre el cual construir el cumplimiento técnico progresivo.

5.3 Recomendaciones

A partir de los resultados del estudio y las observaciones del juicio experto, se formulan las siguientes recomendaciones para la implementación del MGDGP:

- **Publicar los datos de contacto del DPD** en el sitio web institucional como primera acción de cumplimiento, dado que es la brecha más simple de cerrar y de mayor visibilidad ante los titulares
- **Resolver la consulta jurídica sobre biometría** antes de iniciar las EIPDs de los RAT-024 y RAT-025, dado que la base de licitud de ambos tratamientos determina el diseño de los controles.
- **Desarrollar un programa de adecuación técnica sistémica** que automatice los controles de protección de datos en los sistemas y repositorios del IGM, como condición necesaria para el cumplimiento efectivo de los derechos ARCO+ a escala (observación E2).
- **Incorporar cláusulas de protección de datos en licitaciones públicas (ChileCompra)**, extendiendo las obligaciones del MGDGP a proveedores y terceros (observación E1).
- **Desarrollar tablas de retención documental** con plazos de conservación y métodos de supresión para cada categoría de datos tratada (observación E1).
- **Fortalecer el modelo con agrupación por familias y dominios de datos**, asignando responsables a nivel de familia y dominio para hacer el gobierno de datos más robusto en el tiempo (observación E2).

5.4 Trabajo Futuro

El MGDGP diseñado constituye una primera versión del *framework* de gobernanza del IGM. Las siguientes líneas de trabajo futuro se identifican como extensiones naturales: desarrollo del programa de adecuación técnica sistémica identificado por E2 como condición de cumplimiento pleno; incorporación de métricas de cumplimiento continuo; extensión del modelo a otras instituciones con desafíos similares; y actualización del *framework* una vez que la APDP emita sus primeras directrices y resoluciones de fiscalización.

Referencias

- [1] Biblioteca Congreso Nacional, «LEY 21719 REGULA LA PROTECCIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES Y CREA LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES,» 2024 Noviembre 2025. [En línea]. Available: <https://www.bcn.cl/leychile/navegar?idNorma=1209272>. [Último acceso: Enero 2026].
- [2] Contraloría General de la República, «INFORME FINAL CAJA DE PREVISIÓN DE LA DEFENSA NACIONAL INFORME N°651/2023,» CGR, Santiago, 2024.
- [3] M. Fredes Ziliani, *LA COLISIÓN DE LOS DERECHOS DE ACCESO A LA INFORMACIÓN PÚBLICA* Y, Santiago, 2024.
- [4] alayIATrust, «Ley 21.719: Guía Definitiva para Cumplir y Evitar Multas Millonarias,» 9 Julio 2025. [En línea]. Available: <https://alayiatruster.com/guia-completa-sobre-la-ley-21-719/>. [Último acceso: 3 Febrero 2026].



- [5] Ontier, «Ley 21.719 que Regula la Protección de Datos Personales y Crea la Agencia de Protección de Datos Personales,» 25 Agosto 2025. [En línea]. Available: <https://www.ontier.law/ley-21-719-que-regula-la-proteccion-de-datos-personales-y-crea-la-agencia-de-proteccion-de-datos-personales/>. [Último acceso: 3 Febrero 2026].
- [6] Bigid, «La nueva Ley de Privacidad de Datos de Chile: Una guía de cumplimiento para la legislación aprobada 21.719,» 10 Abril 2025. [En línea]. Available: <https://bigid.com/es/blog/chile-new-data-privacy-law-21-719/>. [Último acceso: 3 Febrero 2026].
- [7] J. Holdsworth y M. Kosinki, «¿Qué es el gobierno de datos?,» [En línea]. Available: <https://www.ibm.com/es-es/think/topics/data-governance>. [Último acceso: 3 Febrero 2026].
- [8] Universidad de Chile, «¿Qué es el gobierno de datos?,» [En línea]. Available: <https://uchile.cl/cienciaabierta/datos-de-investigacion/que-es-el-gobierno-de-datos>. [Último acceso: 3 febrero 2026].
- [9] IBM, «¿Qué es el linaje de datos?,» [En línea]. Available: <https://www.ibm.com/es-es/think/topics/data-lineage>. [Último acceso: 3 Febrero 2026].
- [10] Astera Marketing, «Linaje de datos: una guía completa,» 13 junio 2024. [En línea]. Available: <https://www.astera.com/es/type/blog/data-lineage/#:~:text=El%20linaje%20de%20datos%20es%20un%20mecanismo%20de%20cumplimiento%20para,y%20las%20fuentes%20de%20datos..> [Último acceso: 3 febrero 2026].
- [11] Gobierno Digital de Chile, «Gobernanza de Datos,» [En línea]. Available: <https://www.linkedin.com/feed/update/urn:li:activity:7270423640863563776/>. [Último acceso: 2026 Febrero 10].
- [12] Gobierno Digital, «Guía Técnica: aplicación de un marco de referencia de gestión de datos en los órganos de la Administración del Estado,» 29 Noviembre 2024. [En línea]. Available: https://wikiguias.digital.gob.cl/guias/Gu%C3%ADa_MGDE. [Último acceso: 2026 Febrero 10].
- [13] División Gobierno Digital, «Guía Metodológica del Sistema de Transformación Digital 2025,» [En línea]. Available: <https://wikiguias.digital.gob.cl/guias/guia-metodologica-std>. [Último acceso: 10 Febrero 2026].
- [14] ISO, «ISO/IEC 27701:2025,» [En línea]. Available: <https://www.iso.org/es/norma/27701>. [Último acceso: 3 Febrero 2026].
- [15] factorial, «¿Qué es la Normativa ISO-2770-1? Guía para gestionar la privacidad y cumplimiento de normativas de datos,» 6 Febrero 2025. [En línea]. Available: <https://factorial.es/blog/iso-27701/>. [Último acceso: 3 Febrero 2026].
- [16] Hasso Plattner Institute of Design at Stanford, «An Introduction to Design Thinking: Process Guide,» Stanford University, 2010. [En línea]. Available: <https://web.stanford.edu/~mshanks/MichaelShanks/files/509554.pdf>. [Último acceso: 4 Febrero 2026].
- [17] Sección Informática, Computación y Estadísticas, «Informe Técnico N.º 05/2026: diagnóstico de seguridad en el acceso a bases de datos del ERP institucional,» Instituto Geográfico Militar, Santiago, Chile, 2026. Documento interno de circulación restringida.
- [18] Sección Informática, Computación y Estadísticas, «Informe de Hallazgos N.º 04/2026: diagnóstico de cumplimiento de la Ley N.º 21.719,» Instituto Geográfico Militar, Santiago, Chile, 2026. Documento interno de circulación restringida.



Anexos

Por su extensión, los anexos se entregan en un volumen separado. Su contenido es el siguiente:

- **Anexo 1:** Instrumentos de recolección de información por rol (1a Data Owners, 1b Data Stewards, 1c Data Custodians, 1d Síntesis de respuestas). Disponible en [Anexo 1](#).
- **Anexo 2:** Matriz de Levantamiento de Información de Datos Personales (versión anonimizada). Disponible en [Anexo 2](#).
- **Anexo 3:** Instrumento de validación por juicio experto y respuestas de los evaluadores. Disponible en [Anexo 3](#).