INFORME DE DIAGNÓSTICO

Régimen Diferenciado para PYMES de la Ley 21.719

DIRIGIDO A:

Comisión Asesora Ministerial para la Implementación de la Ley N° 21.719, instancia convocada por el Ministerio Secretaría General de la Presidencia (SEGPRES).

AGPD

09 de octubre 2025, Santiago.

INDICE

1. RESUMEN EJECUTIVO.

Este informe ha sido elaborado por la Comisión de Datos Personales de la **Asociación de Profesionales en Protección de Datos Personales (AGPD Chile)**, en el marco de su compromiso con la promoción de estándares normativos y una cultura de protección de datos personales en Chile.

La AGPD es una organización profesional que agrupa a expertos en derecho, tecnología, ciberseguridad, ética e inteligencia artificial, cuyo propósito es promover la excelencia, la ética y la interdisciplinariedad en el ejercicio profesional de la protección de datos. Nuestra misión es contribuir al perfeccionamiento normativo, fomentar capacidades profesionales y generar incidencia en políticas públicas, desde una perspectiva basada en derechos fundamentales, transparencia e independencia técnica.

El presente informe tiene por objeto analizar el **régimen de diferenciación de estándares de cumplimiento para PYMES** contemplado en el artículo 14 septies de la Ley N.º 21.719, con especial atención a sus vacíos regulatorios, nudos interpretativos y oportunidades de mejora desde una perspectiva comparada y basada en riesgos.

Este documento busca aportar desde una mirada técnico-normativa, basada en el estudio comparado y el estándar internacional del Reglamento General de Protección de Datos (GDPR), con el propósito de contribuir a una implementación eficiente, realista y garantista de la Ley N° 21.719. Las recomendaciones aquí propuestas aspiran a servir como insumo para la elaboración de las instrucciones generales que la Agencia deberá emitir, en cumplimiento de su mandato legal y con pleno resguardo de los principios de proporcionalidad, responsabilidad proactiva y protección efectiva de los derechos de los titulares.

2. INTRODUCCIÓN.

El presente informe se enmarca en el trabajo de la **Comisión Asesora Ministerial para la Implementación de la Ley N° 21.719**, instancia convocada por el Ministerio Secretaría General de la Presidencia (SEGPRES) mediante Decreto Exento N° 12, de 17 de junio de 2025, con el objetivo de elaborar recomendaciones técnicas para facilitar la instalación de la nueva institucionalidad de protección de datos personales y orientar la aplicación práctica de la normativa. En este contexto, la Comisión ha priorizado ciertas materias clave que requieren definiciones regulatorias claras y coherentes con los principios de la Ley. Una de ellas es el artículo 14 septies, relativo a la **diferenciación de estándares de cumplimiento aplicables a PYMEs**[1], en materia de deberes de transparencia y seguridad.

Este informe ha sido preparado por la **Comisión de Datos Personales de la Asociación de Profesionales en Protección de Datos Personales (AGPD Chile)**, como parte de su compromiso institucional en este proceso de diálogo técnico. Nuestra contribución busca aportar desde una mirada interdisciplinaria, orientada por el principio de proporcionalidad, la experiencia comparada y la protección efectiva de los derechos de los titulares. La AGPD reúne a profesionales del ámbito jurídico, técnico y organizacional, con una misión centrada en fortalecer las capacidades del ecosistema de protección de datos, promover estándares éticos y fomentar una cultura robusta de privacidad, en línea con los estándares internacionales y el contexto nacional.

El artículo 14 septies[2] representa una innovación importante dentro de la nueva ley, al contemplar expresamente la posibilidad de modular los estándares de

[1] Las PYMEs representan el **98,6 %** del total de empresas en Chile Fuente: Ministerio de Economia, Consejo de Empresas de Menor Tamaño. Plan de Desarrollo Estratégico (2023). En línea: https://www.consejoconsultivoemt.cl/wp-content/uploads/2025/04/Plan-Desarrollo-Estrategico-MiPymes-4.pdf

[2] **Artículo 14 septies. Diferenciación de estándares de cumplimiento.** Los estándares o condiciones mínimas que se impongan al responsable de datos para el cumplimiento de los deberes de información y de seguridad establecidos en los artículos 14 ter y 14 quinquies, respectivamente, serán determinados considerando el tipo de dato del que se trata, si el responsable es una persona natural o jurídica, el tamaño de la entidad o empresa de acuerdo a las categorías establecidas en el artículo segundo de la ley N° 20.416, que fija normas especiales para las empresas de menor tamaño, la actividad que desarrolla y el volumen, naturaleza y las finalidades de los datos personales que trata. // Los estándares o condiciones mínimas de

cumplimiento exigibles a ciertos responsables, particularmente a micro, pequeñas y medianas empresas, considerando el tipo de dato tratado, el volumen, naturaleza y finalidad del tratamiento, así como el tamaño y características de la organización. Esta norma habilita a la futura **Agencia de Protección de Datos Personales** a establecer, mediante instrucciones generales, estándares diferenciados en las materias reguladas por los artículos 14 ter (deber de información) y 14 quinquies (principio de seguridad), ajustados a las realidades y capacidades de los distintos actores, pero sin comprometer los derechos fundamentales de los titulares.

El informe que aquí se presenta tiene por finalidad analizar los nudos críticos, vacíos interpretativos y desafíos regulatorios que plantea este régimen de diferenciación, proponiendo criterios y lineamientos que la Agencia podrá considerar al momento de elaborar sus instrucciones generales. Se trata de una contribución técnica orientada a promover una implementación eficaz, garantista y proporcional de la Ley N° 21.719, que asegure un equilibrio adecuado entre la protección de los derechos de las personas y la viabilidad del cumplimiento normativo para organizaciones de menor escala.

En particular, el informe analiza cinco dimensiones clave del régimen de estándares diferenciados para PYMEs: (i.) el **alcance del concepto de PYME**, estableciendo criterios para determinar cuándo una entidad puede acogerse a dicho régimen, advirtiendo los riesgos de aplicar un enfoque meramente económico y proponiendo una visión funcional basada en riesgo; (ii.) el **principio de seguridad** en contextos de baja complejidad operativa, promoviendo la implementación de medidas básicas proporcionales pero efectivas; (iii.) los **deberes de transparencia e información**, sugiriendo un estándar mínimo que garantice los derechos de los titulares sin generar cargas desproporcionadas; (iv.) la **relación entre responsables y encargados**, especialmente cuando estos últimos son grandes proveedores, destacando la necesidad de evaluar el estándar aplicable según la escala y riesgos reales del encargado; y (v.) la **designación del Delegado de Protección de Datos en PYMES**, proponiendo

cumplimiento y las medidas diferenciadas a que alude el inciso anterior, serán determinados por la Agencia mediante instrucción general.

criterios interpretativos y orientaciones prácticas que permitan su aplicación flexible, incluida la opción de figuras compartidas o externalizadas.

En definitiva, este documento ha sido elaborado como un insumo técnico para apoyar tanto el trabajo de la Comisión Asesora en su misión de formular recomendaciones para la implementación de la Ley N° 21.719, como también para la futura Agencia en el diseño de sus primeras instrucciones generales. Las propuestas aquí contenidas buscan facilitar una interpretación coherente y operativa del artículo 14 septies, promoviendo una regulación diferenciada que sea jurídicamente sólida, proporcional al riesgo, y funcional para los distintos actores regulados, en particular para el ecosistema de PYMES que deberá adecuarse a la nueva normativa.

3. ALCANCE DEL CONCEPTO DE PYME DEL ARTÍCULO 14 SEPTIES.

3.1 Contexto Normativo.

La Ley Nº 21.719 contempla de su artículo 14 septies la posibilidad de establecer estándares diferenciados para responsables del tratamiento que califiquen como empresas de menor tamaño, remitiendo para ello a la definición de PYME establecida en la Ley Nº 20.416. Esta última clasifica a las empresas según sus ingresos anuales, expresados en UF, considerando los siguientes tramos:

- Microempresa: hasta 2.400 UF
- Pequeña empresa: entre 2.400 y 25.000 UF
- Mediana empresa: entre 25.000 y 100.000 UF

Además, excluye del concepto de PYME a aquellas empresas participadas en más de un 30% por sociedades anónimas abiertas o con valores inscritos en bolsa (art. 2° Ley Nº 20.416). No obstante, la normativa no establece la consolidación de ingresos a nivel de grupo empresarial, lo cual deja espacio para la fragmentación estructural como estrategia para obtener beneficios regulatorios.

3.2 Problemática Interpretativa.

Este enfoque estrictamente económico ignora la naturaleza del tratamiento de datos, su volumen y riesgo. A partir de la información recopilada en la revisión de la European Data Protection Board (EDPB)[3], emergen los siguientes casos complejos que evidencian lagunas interpretativas del concepto de PYME basado únicamente en ingresos:

- **Startups** con bajos ingresos, pero alto nivel de automatización, uso de IA o tratamiento de datos sensibles (biométricos, salud, localización), cuyo nivel de riesgo excede el estándar PYME.

- **Organizaciones sin fines de lucro, universidades o grupos de investigación** con estructuras institucionales complejas o capacidad operativa elevada, pero con ingresos formales bajos, que podrían calificar como PYME pese a su impacto potencial.

- **Fragmentación empresarial** creación de múltiples sociedades con bajo ingreso individual, pero con control conjunto o pertenencia a un mismo grupo económico, que operan funcionalmente como una sola entidad.

- **Disociación entre ingresos y capacidad operativa** empresas con ingresos bajo el umbral pero que tienen decenas de trabajadores, grandes volúmenes de datos o sistemas sofisticados de tratamiento no están necesariamente limitadas en sus capacidades para cumplir con estándares completos de protección de datos.

- **Riesgo de generar incentivos perversos** empresas que, pese a realizar tratamientos complejos o automatizados, podrían beneficiarse de menores estándares por mantenerse dentro de un umbral de ingresos no representativo de su capacidad real.

[3] Disponible en línea: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en

3.3 Propuestas de interpretación

Por su parte, el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, en su artículo 30.5, permite a los estados miembros eximir a responsables y encargados con menos de 250 trabajadores de mantener registros de actividades de tratamiento, excepto cuando se trate de tratamientos de riesgo, sistemáticos o de categorías especiales de datos.

Este enfoque demuestra que los criterios como el número de trabajadores y el nivel de riesgo del tratamiento son considerados tan o más relevantes que los ingresos para determinar si corresponde aplicar un régimen diferenciado.

En atención a lo anterior, se propone adoptar una interpretación funcional y basada en riesgo que incluya los siguientes elementos:

i. **Consolidación de ingresos:** la Agencia debería exigir la consolidación de ingresos cuando las empresas pertenezcan a un grupo económico o existan relaciones de control directo o indirecto, evitando el uso instrumental del concepto de PYME (criterio recogido en diversas prácticas del EDPB y CNIL).

ii. **Incorporar criterios operativos como número de trabajadores y capacidad técnica:** siguiendo el enfoque del artículo 30.5 del GDPR, el número de trabajadores puede ser un indicador complementario para calificar o descalificar a una entidad del régimen diferenciado.

iii. **Evaluación del riesgo como condición de entrada:** empresas que realicen tratamientos considerados de alto riesgo no deberían poder acogerse al régimen PYME, aunque cumplan con el umbral de ingresos. Según las Guidelines 01/2022 del EDPB, esto incluye:

    a. Elaboración de perfiles automatizados.
    b. Tratamiento de categorías especiales de datos.
    c. Monitoreo sistemático.
    d. Volúmenes masivos de tratamiento.

iv. **Enfoque basado en el contexto y naturaleza del tratamiento:** la evaluación de elegibilidad para el régimen diferenciado debe considerar el contexto real de operaciones, incluyendo proveedores tecnológicos, subcontratación de servicios de IA, tratamiento de menores, etc.

3.4 Recomendaciones para la Agencia:

i. Emitir una **guía interpretativa** sobre el concepto de PYME, que aclare cuándo corresponde aplicar el régimen diferenciado de la Ley 21.719, considerando ingresos consolidados, trabajadores, complejidad del tratamiento y riesgos inherentes. Incluir ejemplos prácticos y casos límite en futuras guías, para orientar tanto a startups como a ONGs, universidades y cooperativas. En dicha guía se debe establecer una revisión periódica del estatus de PYME, no puede ser indefinido.

ii. Establecer una "**lista de banderas rojas**", como lo han hecho autoridades como la AEPD (España) o el ICO (Reino Unido), que excluyan automáticamente del régimen diferenciado a empresas que:

a. Traten datos sensibles.
b. Hagan elaboración de perfiles o decisiones automatizadas.
c. Sean prestadoras de servicios tecnológicos que traten datos de terceros.

iii. Exigir la **consolidación de ingresos** cuando existan **relaciones de control** directo o indirecto, particularmente en grupos empresariales, universidades, fundaciones matrices u otros esquemas de dependencia.

iv. Promover **mecanismos de autodiagnóstico obligatorio** (como checklists de riesgo), que permitan a las empresas autoevaluarse antes de aplicar el régimen diferenciado.

v. En caso de organizaciones que cumplan con los requisitos que hacen procedente algún nivel de flexibilización por parte de la Agencia, fomentar

el uso de **Códigos de Conducta** (como parte de un "modelo de prevención de infracciones" o mecanismo de cumplimiento alternativo) que sean diferenciados para estos grupos contemplando sus particularidades y necesidades, debidamente supervisados (art. 40.1 GDPR) y que establezcan formularios estándar de solicitudes de derechos.

vi. Elaboración de **guías simplificadas** para PYMES.

4. PRINCIPIO DE SEGURIDAD DEL ARTÍCULO 14 SEPTIES

4.1 Contexto Normativo.

En alusión a las PYMES, el Artículo 14 septies de la LPDP establece un punto importante respecto a la intensidad con la que debiera aplicarse el deber de seguridad, consagrando la posibilidad de realizar una diferenciación de estándares de cumplimiento. De este modo, el texto legal permite que "*los estándares o condiciones mínimas que se impongan al responsable de datos para el cumplimiento de los deberes de información y de seguridad establecidos (…) serán determinados considerando el tipo de dato del que se trata, si el responsable es una* ***persona natural o jurídica, el tamaño de la entidad o empresa de acuerdo a las categorías establecidas en el artículo segundo de la ley N° 20.416, que fija normas especiales para las empresas de menor tamaño, la actividad que desarrolla y el volumen, naturaleza y las finalidades de los datos personales que trata***". (énfasis propio).

En otras palabras, los factores descritos anteriormente, entre los cuales se encuentran el **tamaño** de la empresa, su **actividad**, y el **volumen**, **naturaleza** y **finalidades** de los datos personales que se tratan, serán elementos clave para determinar cómo se debe cumplir la obligación de establecer medidas de seguridad y, en definitiva, el principio de seguridad en cada caso.

De este modo, y considerando además que los "*estándares o condiciones mínimas de cumplimiento*" y las medidas diferenciadas a que alude el artículo 14

septies serán determinados por la Agencia mediante instrucción general, corresponde entonces determinar cuáles podrían ser tales medidas diferenciadas, pensando especialmente en empresas de menor tamaño, definición que la legislación nacional actual no recoge.

4.2 Experiencia comparada europea.

El RGPD, como bien es sabido, es una norma enfocada en la gestión de riesgos. En este sentido, el principio de "***integridad y confidencialidad"***, que en la Ley 21.719 se denomina de "***seguridad***", abarca la tríada de la clásica de la seguridad de la información - **confidencialidad**, la **integridad** y la **disponibilidad** - y debe considerarse siguiendo un enfoque de proporcionalidad al riesgo, esto es:

"*cuanto mayor sea el riesgo, más rigurosas serán las medidas que deberá adoptar el responsable o el encargado del tratamiento*".

Sin embargo, la pregunta aquí es cómo pueden las PYMES cumplir con estas obligaciones, cuando tales no siempre (o necesariamente) tienen los conocimientos y recursos necesarios para prevenir, detectar y mitigar los riesgos propios de la seguridad de la información.

A continuación, rescatamos algunos ejemplos de la experiencia europea.

AEPD

La AEPD española ha desarrollado una herramienta especial denominada "*FACILITA_RGPD*", enfocada específicamente en "*PYMEs, micropymes y profesionales*" que realizan tratamientos con escaso nivel de riesgo. Su objetivo es proporcionar ayuda para la elaboración del **registro de actividades** de tratamiento, las **cláusulas informativas**, las **cláusulas contractuales** para encargados del tratamiento y las **medidas de seguridad** a adoptar[4].

En este sentido, podría resultar recomendable para la Agencia de protección de datos personales desarrollar herramientas automatizadas o plantillas

[4] Disponible en línea: https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/directrices-de-aplicacion/pymes

estandarizadas que permitan a las PYMES cumplir con sus obligaciones, sin necesidad de incurrir en altos costos de asesoría técnica o legal.

ICO, EDPB y ENISA

Las guías del ICO[5], junto con las del EDPB[6] y ENISA[7], promueven un conjunto de medidas de bajo coste y alto impacto que son el estándar mínimo de seguridad proporcional:

a) **Copias de Seguridad** (Data Backup): Realización regular y almacenamiento seguro (cifrado y ubicación física separada del lugar de trabajo principal).
b) **Seguridad de Acceso**: Uso de contraseñas robustas y, fundamentalmente, la implementación de la autenticación multifactor (MFA) en todas las cuentas y dispositivos que almacenen información personal.
c) **Principio de Mínimo Privilegio**: Limitar el acceso a la información personal solo a aquellos empleados que lo necesiten estrictamente para su función.
d) **Disposición y Software**: Eliminación segura de equipos de TI y registros antiguos, además de mantener el software antivirus y antimalware actualizado.

El énfasis de estas directrices en medidas como la MFA y las copias de seguridad separadas revela una preferencia por soluciones organizacionales que mitiguen el riesgo humano. Estas medidas, que requieren disciplina y formación más que una gran inversión en infraestructura, **ofrecen la mayor mitigación de riesgo por el menor costo, lo que se considera la aplicación práctica y efectiva del principio de proporcionalidad para entidades de menor tamaño**.

Lo anterior tiene especial relevancia, considerando que de acuerdo con el *Data Breach Investigations Report (DBIR) de Verizon* de 2023, "*[e]l 74% de todas las brechas incluyen el elemento humano, con personas involucradas ya sea por*

[5] Disponible en línea: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/
[6] Disponible en línea: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en
[7] Disponible en línea: https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes

Error, Uso indebido de privilegios, Uso de credenciales robadas o Ingeniería social."[8]

ICO

Por su parte, la ICO de UK ha dado un ejemplo claro en su forma de sancionar a las PYMES, considerando que sigue el principio que las multas deben ser "**efectivas, proporcionadas y disuasorias**"[9], y esto conlleva que para que sean realmente justas, tienen que tomar en cuenta el tamaño y la situación financiera de la empresa[10].

El objetivo de la autoridad de datos en UK es entonces evitar que una multa termine ahogando económicamente a una organización, especialmente cuando se trata de PYMES. Se debe considerar que las multas máximas bajo el RGPD y la ley británica pueden alcanzar cifras muy elevadas de hasta £17.5 millones o el 4% de la facturación global anual.

En este sentido, este **criterio de proporcionalidad** es crucial para que las PYMES sancionadas puedan sobrevivir.

Un caso que ilustra muy bien cómo funciona esto en la práctica es el de Advanced Computer Software Group Ltd[11]. La empresa recibió una multa de £3.07 millones después de sufrir un ataque de ransomware que expuso datos sensibles de miles de personas, incluyendo información delicada como detalles de acceso a viviendas de pacientes que recibían atención domiciliaria. El problema de fondo fue la falta de medidas de seguridad básicas (no se tenía autenticación multifactor en cuentas críticas, lo que facilitó el acceso no autorizado).

Aunque la brecha fue grave, la multa terminó siendo menor de lo que se había contemplado inicialmente, porque la empresa actuó de manera proactiva desde

[8] Disponible en línea: https://www.verizon.com/business/resources/reports/dbir/
[9] Disponible en: https://ico.org.uk/about-the-ico/our-information/policies-and-procedures/data-protection-fining-guidance/circumstances-in-which-the-commissioner-would-consider-it-appropriate-to-issue-a-penalty-notice/effectiveness-proportionality-and-dissuasiveness/
[10] Art 83 del GDPR
[11] Disponible en línea: https://ico.org.uk/media2/gdlfddgc/advanced-penalty-notice-20250327.pdf

el primer momento: colaboró rápidamente con las autoridades (NCSC y NCA) y tomó medidas inmediatas para controlar el daño.

Lo anterior demuestra este caso es que la ICO no espera que la seguridad sea perfecta, pero sí que se responda con responsabilidad. Para las PYMES, esto significa que la actitud y la respuesta pueden marcar una diferencia enorme al momento de ser sancionadas.

ENISA

En este aspecto, la *European Union Agency for Network and Information Security* (ENISA) ha propuesto en su guía "*Guidelines for SMEs on the security of personal data processing*" un marco de acción[12] para la gestión de riesgos **simplificado** para las PYMES, a través de una guía práctica y escalonada, para que tales entidades puedan cumplir con sus obligaciones de seguridad de datos de una manera proporcionada a los riesgos que afrontan y a los recursos de los que disponen, de la siguiente forma:

i. **Evaluación de Riesgos de Seguridad.**

- **Paso 1**: Definición de la operación de tratamiento y su contexto. La PYME debe comprender claramente qué datos personales trata, con qué finalidad, por qué medios, dónde se lleva a cabo el tratamiento, quiénes son los interesados y quiénes los destinatarios de los datos.
- **Paso 2**: Comprensión y evaluación del impacto. Se debe evaluar el impacto potencial que un incidente de seguridad podría tener sobre los derechos y libertades de las personas. El texto propone cuatro niveles de impacto: bajo, medio, alto y muy alto.
- **Paso 3**: Definición de posibles amenazas y evaluación de su probabilidad. Este paso consiste en identificar las amenazas para la seguridad de los datos y valorar la probabilidad de que ocurran.

[12] Disponible en línea:https://www.enisa.europa.eu/sites/default/files/publications/WP2016%203-2%206%20Data%20Controllers%20Risk.pdf

- **Paso 4**: Evaluación del riesgo. Finalmente, se combina la evaluación del impacto y la probabilidad de la amenaza para determinar el nivel de riesgo global, que puede ser bajo, medio o alto.

ii. **Implementación de Medidas de Seguridad.** Una vez evaluado el nivel de riesgo, el ENISA propone una serie de medidas de seguridad organizativas y técnicas, clasificadas según el nivel de riesgo (bajo, medio y alto). Esto permite a las PYMES adoptar las medidas más adecuadas a su situación particular:

a. Medidas Organizativas:

- Gestión de la seguridad: Incluye la creación de políticas y procedimientos de seguridad, la definición de roles y responsabilidades, y la gestión de accesos y recursos
- Respuesta a incidentes y continuidad del negocio: Establece planes para gestionar incidentes de seguridad y garantizar la continuidad de las operaciones.
- Recursos humanos: Se enfoca en la confidencialidad y la formación del personal que trata datos personales.

b. Medidas Técnicas:

- Control de acceso y autenticación: Implementación de sistemas para controlar quién accede a los datos.
- Registro y monitorización: Seguimiento de las actividades realizadas sobre los datos personales.
- Seguridad de los datos en reposo y en tránsito: Medidas como el cifrado para proteger los datos almacenados y cuando se transmiten.
- Copias de seguridad (Backups): Procedimientos para realizar y proteger copias de seguridad de los datos.

- Seguridad en dispositivos móviles, ciclo de vida de las aplicaciones, eliminación de datos y seguridad física.

4.3 Recomendaciones para la Agencia.

Recogiendo los puntos mencionados anteriormente, se recomienda a la Agencia mantener un enfoque sobre los siguientes puntos, entendidos como condiciones mínimas de cumplimiento del principio de seguridad para PYMES:

i. **Crear herramientas o marcos de cumplimiento simplificado:** una idea práctica en este ámbito podría ser desarrollar una herramienta digital que guíe a las PYMEs a través de pasos básicos, explicados detalladamente.

ii. **Publicar Guías sobre el deber de seguridad:** Preparar y difundir guías claras que traduzcan las obligaciones de seguridad de la Ley 21.719 en pasos concretos para la realidad de entidades chilenas, enfatizando las medidas técnicas y organizativas de bajo costo (por ej. como MFA, *backup* y políticas de control de acceso).

iii. **Definir criterios de atenuación de sanciones:** Revisar la factibilidad de establecer multas en base a criterios de atenuación basados en la capacidad financiera (UF) y considerando además la proactividad y colaboración de la entidad en la etapa post-brecha. La diferenciación para PYMES debe centrarse en la proporcionalidad de las medidas, no en la exención de obligaciones.

5. PRINCIPIO DE TRANSPARENCIA DEL ARTÍCULO 14 SEPTIES

5.1 Contexto Normativo.

La protección de los datos personales exige entregar a los titulares herramientas efectivas para el ejercicio de sus derechos. Entre éstas, la Ley N° 21.719 contempla un conjunto de reglas que estructuran los deberes de transparencia e información del responsable del tratamiento, configurándolos como un pilar fundamental de los derechos de los titulares.

El debido cumplimiento del principio de transparencia y de los deberes específicos de información permite a los titulares ejercer derechos como: acceso, rectificación, supresión, oposición a determinados tratamientos, bloqueo, portabilidad, a ser informados de vulneraciones de seguridad, conocer el tratamiento de datos de geolocalización y su cesión a terceros, entre otros aspectos.

Por ello, la obligación de transparencia y de informar se entiende como una **garantía instrumental** del derecho a la protección de datos, integrándose en su núcleo esencial.

Dentro de esta garantía se incluyen, entre otros:

- La obligación de informar y poner a disposición los antecedentes que acrediten la licitud del tratamiento (art. 14, letra a).
- El deber de información y transparencia (art. 14 ter).
- El deber de informar vulneraciones relativas a datos sensibles, de menores de 14 años o vinculados a obligaciones económicas, financieras, bancarias o comerciales (art. 14 sexies).
- La información exigida en tratamientos de geolocalización (art. 16 sexies).
- El deber activo de información asociado al derecho de acceso y a tratamientos con decisiones automatizadas o elaboración de perfiles (arts. 5 y 8 bis).
- La información relativa a tratamientos de datos de salud y perfil biológico humano (art. 16 bis).
- El deber de informar sobre el tratamiento de datos biométricos (art. 16 ter).

5.2 Diferenciación de estándares mínimos del artículo 14 ter.

El artículo 14 septies contempla la posibilidad de que la Agencia de Protección de Datos Personales establezca **estándares diferenciados o mínimos de**

cumplimiento respecto del deber de información previsto en el artículo 14 ter, aplicables a los responsables del tratamiento.

Estos estándares deberán considerar:

- El tipo de dato tratado.
- La actividad del responsable, el volumen, naturaleza y finalidades de los datos.
- Si el responsable es persona natural o jurídica.
- El tamaño de la entidad, según las categorías de la Ley N° 20.416.

A primera vista, quedan **excluidos de esta diferenciación** los tratamientos que involucren **datos sensibles**, **categorías especialmente protegidas**, **elaboración de perfiles o decisiones automatizadas** con efectos jurídicos significativos para el titular, o cualquier tratamiento que, en base al **alcance**, **contexto**, **tecnología utilizada**, se pueda producir un **alto riesgo** para los derechos de los titulares.

La cuestión relevante para el presente análisis es determinar cuáles serían los mínimos de cumplimiento exigibles a responsables de menor tamaño[13], que tratan datos de bajo o escaso riesgo, sin que ello genere una vulneración del derecho a la protección de datos.

5.3 Aproximaciones a la aplicación práctica del artículo 14 ter en relación con el artículo 14 septies

Una medida razonable sería exigir del responsable, como mínimo la puesta a disposición del público en su sitio web o medio equivalente, la información contenida en las letras b), c), d), f), g) e i) del artículo 14 ter. De este modo se asegura un nivel básico de transparencia e información, incluso en

[13] La encuesta sobre el grado de preparación de las empresas españolas ante el Reglamento General de Protección de Datos, elaborada por la Agencia Española de Protección de Datos y CEPYME, del año 2018, señala que los recursos que gestionan con más frecuencia las empresas de menor dimensión se concentran en tres agregados principales: los datos de clientes, proveedores y empleados, que son tratados por prácticamente todas las empresas (del 97% al 92%) y, en menor medida, los recursos relativos a videovigilancia (38%) y formularios en Internet (17%).

organizaciones pequeñas o de bajo riesgo, que se asemeja a la información que podrá conocer el titular cuando ejerce el derecho de acceso contemplado en el artículo 5 de la ley.

De ese modo, el titular del dato conocerá:

- La **individualización** del responsable de datos y su representante legal.
- La dirección de **correo electrónico** mediante el cual se le notifican las solicitudes que realicen los titulares.
- **Tipos de datos** que trata; la descripción genérica del **universo de personas** que comprenden sus bases de datos; los **destinatarios** a los que se prevé comunicar o ceder los datos; las finalidades de los tratamientos que realiza; la **base de legitimidad** del tratamiento; y en caso de tratamientos que se basan en la satisfacción de **intereses legítimos**, cuáles serían éstos.
- El derecho que le asiste al titular para solicitar ante el responsable, **acceso**, **rectificación**, **supresión**, **oposición** y **portabilidad** de sus datos personales, de conformidad a la ley.
- El derecho que le asiste al titular de **recurrir ante la Agencia**, en caso de que el responsable rechace o no responda oportunamente las solicitudes que le formule.
- El periodo durante el cual se **conservarán** los datos personales.

5.4 Consideraciones estratégicas

Las condiciones mínimas de información y transparencia de las entidades responsables con escaso riesgo no deben afectar la futura consideración de Chile como país con nivel adecuado de protección de datos a efectos de transferencias internacionales. Para ello la Agencia deberá asegurar estándares de información y seguridad suficientes para cumplir con los **criterios de adecuación**.

Por otro lado, una delimitación inadecuada del estándar diferenciado podría generar **controversias administrativas y judiciales** en torno a la interpretación

y aplicación del artículo 34 bis, letra a), que tipifica el incumplimiento del deber de información del artículo 14 ter.

1.1. Experiencia internacional

Aunque no se encontraron normas idénticas o similares en el derecho comparado, diversas autoridades de protección de datos han desarrollado **mecanismos de apoyo específicos** para PYMES y MICRO-PYMES, respecto de aquellas entidades que realizan tratamientos que suelen implicar menor riesgo.

La Agencia Española de Protección de Datos (AEPD), por ejemplo, creó la herramienta **FACILITA_RGPD**, que ayuda a elaborar registros de actividades de tratamiento, cláusulas informativas y contractuales, así como medidas de seguridad proporcionales. Asimismo, ha suscrito protocolos con la Confederación Española de Organizaciones Empresariales (CEOE) y la Confederación Española de la Pequeña y Mediana Empresa (CEPYME), fomentando el cumplimiento simplificado en este sector.

5.5 Recomendaciones para la Agencia.

Para una correcta implementación del régimen de diferenciación de estándares en materia de transparencia (artículo 14 ter), conforme a lo dispuesto en el artículo 14 septies, se recomienda que la Agencia considere las siguientes líneas de acción:

i. **Establecer un estándar mínimo uniforme y claro**, aplicable a responsables de menor tamaño y bajo riesgo, que incluya obligatoriamente la publicación accesible (por ejemplo, en sitio web o soporte equivalente) de los elementos esenciales de información previstos en el artículo 14 ter, letras b), c), d), f), g) e i). Esta obligación permitirá asegurar un umbral básico de transparencia, sin imponer cargas desproporcionadas a entidades pequeñas.

ii. **Delimitar expresamente los tratamientos excluidos del régimen de diferenciación**, señalando que NO se aplicará a:

a. Tratamientos de datos sensibles o de categorías especiales.
b. Decisiones automatizadas con efectos significativos para los titulares.
c. Actividades de alto riesgo, considerando volumen, tecnología o destinatarios.

iii. **Establecer una matriz de riesgos y proporcionalidad** que permita a los responsables y encargados identificar si su actividad califica para aplicar estándares diferenciados, considerando criterios como: (a) Tipo y volumen de datos tratados. (b) Finalidades del tratamiento. (b) Canales de recolección. (c) Destinatarios previstos y transferencias. (d) Tecnología empleada y nivel de automatización.

iv. **Desarrollar herramientas de cumplimiento simplificadas para PYMES (mediante planillas Excel y/o softwares gratuitos)**, tomando como referencia buenas prácticas internacionales como la herramienta FACILITA_RGPD de la AEPD, con orientación práctica para: (a) Elaborar cláusulas informativas. (b) Documentar las bases legales del tratamiento. (c) Acreditar la adopción de medidas mínimas de transparencia.

v. **Establecer modelos o plantillas tipo de cláusulas informativas**, adaptadas a sectores económicos específicos (comercio, salud, educación, etc.), que puedan ser adoptadas voluntariamente por responsables de menor tamaño como medio para facilitar el cumplimiento.

vi. **Evitar que la diferenciación de estándares derive en una protección insuficiente**, particularmente en lo que respecta a las expectativas razonables de los titulares. La diferenciación no debe ser confundida con exención de obligaciones, y debe mantenerse la posibilidad de evaluación posterior por parte de la Agencia ante incumplimientos.

vii. **Asegurar el cumplimiento de estándares internacionales de adecuación**, en el sentido de que la flexibilidad otorgada a pequeñas

entidades no comprometa la evaluación futura de Chile como país con nivel adecuado de protección de datos conforme al artículo 45 del GDPR.

6. RÉGIMEN DE ENCARGADOS DE TRATAMIENTO – ALCANCE DEL ARTÍCULO 15 Bis, INCISO 4° vs. 14 Septies.

6.1 Contexto Normativo.

El artículo 15 bis regula el tratamiento de datos personales por parte de **terceros mandatarios o encargados**, estableciendo expresamente que estos deben cumplir con los deberes de información y seguridad previstos en los artículos 14 bis y 14 quinquies. A su vez, el inciso 4° dispone que la diferenciación de estándares de cumplimiento establecida en el artículo 14 septies también será aplicable al tercero mandatario o encargado.

> Art. 15 bis (inciso 4°): "*El tercero mandatario o encargado deberá cumplir con lo dispuesto en los artículos 14 bis y 14 quinquies.* ***La diferenciación de estándares de cumplimiento establecida en el inciso primero del artículo 14 septies también será aplicable al tercero mandatario o encargado****. Tratándose de una vulneración a las medidas de seguridad, el tercero o mandatario deberá reportar este hecho al responsable".*

Esta remisión introduce un **régimen de proporcionalidad** aplicable al encargado del tratamiento, lo cual permite ajustar sus obligaciones en función de criterios tales como el tipo de datos, la actividad desarrollada, y las características de la relación con el responsable.

Sin embargo, el texto legal **no especifica** si esta diferenciación se evalúa **desde la perspectiva del encargado**, del responsable, o de ambos.

6.2 Problemática Interpretativa

La falta de precisión respecto al sujeto a considerar para la aplicación de los estándares diferenciados genera dudas relevantes para la implementación del régimen. En particular:

- ¿Es el tamaño del responsable (PYME o gran empresa) lo que habilita al encargado a operar con estándares diferenciados?
- ¿O debe considerarse también el tamaño, naturaleza y capacidades del propio encargado?

Este punto es especialmente relevante en casos en que una PYME contrata a una gran empresa tecnológica como encargado (por ejemplo, un proveedor de servicios de almacenamiento en la nube).

Si la diferenciación se aplica solo por el tamaño del responsable, se permitiría que grandes empresas apliquen estándares mínimos solo por atender a una PYME, lo cual vulneraría el principio de responsabilidad proactiva (*accountability*) y el deber de seguridad del tratamiento.

6.3 Propuesta de interpretación

Se propone interpretar que **la aplicación de estándares diferenciados al encargado debe considerar tanto las características del responsable como las del propio encargado**. Esta interpretación se sustenta en los siguientes principios contenidos en la Ley 21.719 y estándares comparados:

- El artículo 28(1) del GDPR obliga al responsable a seleccionar solo encargados que ofrezcan "*garantías suficientes para aplicar medidas técnicas y organizativas apropiadas*".

- El artículo 32 del GDPR dispone que tanto responsables como encargados deben aplicar medidas de seguridad proporcionales al riesgo, considerando el *"estado de la técnica"*, los costes de implementación y la naturaleza del tratamiento.

- Ambos principios se desprenden también del propio artículo 14 quinquies inciso segundo de la Ley 21.719, relativo a las medidas de seguridad, en cuanto dispone que *"Teniendo en cuenta el **estado de la técnica**, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de los titulares, el responsable y el encargado*

del tratamiento aplicarán ***medidas técnicas y organizativas apropiadas*** *para garantizar un nivel de seguridad adecuado al riesgo*", junto con los aspectos mínimos que tanto responsable como encargado deben considerar. En el mismo sentido, el inciso final del mismo artículo impone al responsable la carga probatoria de acreditar la existencia y funcionamiento de las medidas de seguridad adoptadas en caso de controversia judicial o administrativa.

- En la misma línea, la **EDPB Guidelines 07/2020**[14] enfatiza que los encargados, aunque limitados por las instrucciones del responsable, cuentan con cierto margen de discrecionalidad sobre el modo de servir mejor a los intereses del responsable, de manera que permitan al encargado elegir los medios técnicos y organizativos más adecuados para garantizar la protección de los datos, introduciendo los conceptos de "***medios esenciales y no esenciales***" (Apartado 2.1.4 «Los fines y medios»)

Bajo esta lógica, una gran empresa que actúa como encargado no puede invocar estándares diferenciados mínimos únicamente por prestar servicios a una PYME, ya que sus capacidades y riesgos operacionales justifican un umbral más alto de cumplimiento.

En sentido inverso, cuando el encargado es efectivamente una PYME, corresponderá aplicar los principios de proporcionalidad y adecuación establecidos en el artículo 14 septies, evaluando su tamaño, recursos y nivel de exposición al riesgo, siempre que ello no implique comprometer la seguridad o los derechos de los titulares de datos.

6.4 Recomendaciones para la Agencia

Para evitar interpretaciones laxas o incoherentes con los principios de protección de datos, se recomienda que la Agencia:

[14] https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en

i. **Emita una Instrucción General interpretativa que aclare que la diferenciación de estándares debe considerar**: (a) El perfil del encargado (tamaño, sector, capacidad técnica). (b) El tipo de tratamiento instruido por el responsable y su nivel de riesgo. (c) Las condiciones del responsable del tratamiento.

ii. **Establezca lineamientos específicos para encargados** en función de escalas organizacionales y sectores críticos (Ej. servicios tecnológicos, salud, educación).

iii. **Prohibición expresa** de que encargados de gran escala se acojan a estándares mínimos si su propia estructura y el tratamiento que realizan conllevan riesgos elevados para los titulares de datos.

iv. Poner a disposición **modelos tipo de cláusulas contractuales** que reflejen estos criterios de proporcionalidad y corresponsabilidad entre responsables y encargados.

7. DESIGNACIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS (DPO) EN PYMES. APLICACIÓN DEL ARTÍCULO 14 Septies.

7.1 Contexto Normativo.

La Ley N° 21.719 establece, como principio general, que la designación de un Delegado de Protección de Datos (DPD o DPO) **no es obligatoria** para todos los responsables. En efecto, el **artículo 50** indica que el responsable "***podrá***" designar un DPO, lo que se configura como una **facultad potestativa**, no un deber universal.

No obstante, la situación cambia si la empresa decide voluntariamente implementar un **modelo de prevención de infracciones** (o programa de cumplimiento). En ese caso, el **artículo 49, letra a)** exige como componente obligatorio de dicho modelo la designación de un DPO, que debe ser nombrado por la máxima autoridad de la organización y contar con autonomía funcional.

La ley también contempla condiciones particulares para PYMES, permitiendo que el **dueño o la máxima autoridad** de la empresa asuma personalmente las funciones del DPO, y disponiendo que los **medios y recursos asignados** al DPO deben ser proporcionales al **tamaño y capacidad económica** de la organización (art. 50, inc. final).

Por otro lado, el **artículo 15 ter** exige la realización de una **Evaluación de Impacto** cuando el tratamiento pueda implicar alto riesgo, incluyendo expresamente los supuestos de "tratamiento a gran escala" o "monitoreo sistemático", sin distinguir entre tipos o tamaños de responsables.

7.2 Problemática interpretativa

Si bien la ley establece que la designación de un DPO es en principio voluntaria, surgen dudas sobre si determinados tratamientos realizados por una PYME podrían, por su naturaleza, hacer recomendable o incluso necesaria la designación de esta figura.

Particularmente, se plantea la siguiente pregunta: **¿Una PYME que lleva a cabo tratamiento a gran escala o que realiza seguimiento sistemático debe nombrar un DPO, aunque no haya implementado un modelo de prevención?**

La ley no entrega una respuesta directa. Sin embargo, remite a la **Agencia** la facultad de emitir **instrucciones generales** (art. 14 septies y art. 15 ter), y establece un principio de **proporcionalidad** en el cumplimiento normativo, considerando el **tamaño** del responsable y la **naturaleza** de los datos tratados.

Por tanto, la interpretación de los conceptos **"gran escala"** y **"seguimiento sistemático"** en relación con PYMES deberá ser determinante para establecer si determinadas operaciones deben o no activar la obligación práctica de designar un DPO.

7.3 Propuesta de interpretación

Se propone adoptar una interpretación flexible y contextualizada de los criterios de “gran escala” y “seguimiento sistemático”, aplicables de forma proporcional al tamaño, actividad y riesgo operativo de la PYME.

A continuación, se desarrollan diferentes aspectos a considerar, conforme la normativa vigente y contexto de cada organización:

- **Tratamiento a “*gran escala*”:** Debe entenderse no en términos absolutos (volumen total de registros), sino **relativos al contexto de la organización**. Por ejemplo, una base de 50.000 clientes puede ser significativa para una microempresa, pero no comparable al volumen manejado por una entidad bancaria. La escala debe analizarse en proporción a la **capacidad operativa,** la **infraestructura** y el **nivel de automatización** de cada empresa.

- **Monitoreo sistemático:** Se debe excluir de esta definición prácticas comunes de seguridad interna o localización restringida (por ejemplo, cámaras en el interior de un local comercial) que no implican o no contienen elementos propios de una vigilancia intensiva o constante del comportamiento de personas en espacios públicos.

- **Evaluación de Impacto y DPO:** El artículo 15 ter permite que la Agencia elabore listas de operaciones que requieren o no la ejecución de una evaluación de impacto. Estas listas deberían integrar también **referencias sectoriales** que orienten a PYMES sobre **cuándo se recomienda (o exige de facto)** la designación de un DPO por el tipo de tratamiento.

- **Modelo de prevención y obligación reforzada:** Si bien la adopción del modelo de prevención es voluntaria, su implementación activa una **obligación legal** clara de designar un DPO. En este sentido, esta regla debe – en la práctica – mantenerse o fomentarse como un “incentivo positivo” dirigido a promover un mayor nivel de cumplimiento normativo y autorregulación.

7.4 Recomendaciones para la Agencia

La Agencia de Protección de Datos Personales tendrá un papel clave en la definición de los estándares prácticos de cumplimiento. Al respecto, se recomiendan las siguientes medidas:

i. **Publicar directrices interpretativas sobre los conceptos de "gran escala" y "monitoreo sistemático"** , con el fin de alcanzar una aplicación proporcional y coherente de estos conceptos en organizaciones de menor tamaño. Para estos efectos, la Agencia debería desarrollar directrices interpretativas que integren – entre otros – los siguientes elementos:

   a. **Umbrales orientativos según tipo de organización:** Se propone que la Agencia establezca rangos de referencia adaptados al tamaño y sector de la entidad. Por ejemplo:

      - Para una **microempresa**, podrían considerarse tratamientos "a gran escala" solo aquellos que involucren a más de 10.000 titulares.
      - En el caso de una **mediana empresa**, el umbral podría subir a 100.000 titulares o más, dependiendo del sector.
      - Estos umbrales deben ser **flexibles y orientativos**, permitiendo ajustar la evaluación según el riesgo real y no solo el número de registros.

   b. Definición de ejemplos prácticos sectoriales aplicables a PYMES: Las directrices deberían incluir casos ilustrativos específicos por sector económico, con el fin de reducir ambigüedades y proveer de una mayor seguridad jurídica a los responsables, tales como se ilustra con los siguientes:

      - Una clínica dental con 3.000 pacientes recurrentes puede no requerir DPO, pero una red de laboratorios que procesa datos de salud para 80.000 personas anualmente sí.

- Una tienda de barrio con videovigilancia interior no realiza monitoreo sistemático, mientras que una empresa de seguridad que instala y gestiona cámaras en vía pública sí lo hace.

- Una startup tipo “EdTech” que elabora perfiles de aprendizaje de miles de alumnos podría requerir una evaluación de impacto y eventualmente la designación de un DPO.

c. **Criterios acumulativos o indicativos, no absolutistas:** Se recomienda evitar la aplicación automática de una sola condición (por ejemplo, el número de registros tratados) como factor determinante. En cambio, la evaluación debe considerar un **conjunto de factores combinados**, tales como: (a) Naturaleza y sensibilidad de los datos tratados. (b) Nivel de automatización del tratamiento. (b) Finalidades y alcance territorial. (c) Volumen de titulares afectados en proporción a la actividad de la empresa. (d) Posibilidad de impacto significativo sobre los derechos y libertades de los titulares.

ii. **Incluir, en las listas de operaciones que requieren evaluación de impacto, referencias específicas sobre la necesidad o recomendación de designar un DPO**: La Agencia, al amparo del artículo 15 ter, debe elaborar listas públicas de tratamientos que requieren o no una Evaluación de Impacto en la Protección de Datos (EIPD). Se recomienda que dichas listas incluyan, además, una **indicación expresa de si se considera recomendable o necesaria la designación de un DPO en función del nivel de riesgo asociado a cada tipo de tratamiento**.

Esto permitirá que las PYMES que desarrollen operaciones de riesgo alto – aunque no estén obligadas por defecto – puedan identificar de manera clara cuándo resulta aconsejable contar con un DPO. Esta orientación puede ser especialmente útil en sectores como salud, servicios financieros, tecnología educativa o tratamiento de datos biométricos.

iii. **Fomentar la implementación de modelos de prevención en PYMES como mecanismo voluntario de cumplimiento reforzado:** La normativa chilena contempla la posibilidad de que los responsables implementen modelos de prevención de infracciones, los cuales, al ser adoptados, implican automáticamente la obligación de designar un DPO (art. 49, letra a)). En este sentido, la Agencia debiera **promover activamente la adopción de estos modelos como herramientas de cumplimiento proactivo**, brindando beneficios como: (a) Reducción de riesgos regulatorios. (b) Mejora en la gestión interna de datos. (c) Posibilidad de demostrar accountability frente a auditorías o requerimientos.

Para ello, se recomienda que la Agencia publique **guías sectoriales simplificadas**, con ejemplos adaptados al tamaño de las organizaciones, que integren plantillas, procedimientos sugeridos y mecanismos de autoevaluación.

iv. **Promover el uso de la figura del DPO compartido o externalizado entre PYMES:** Una barrera común en empresas pequeñas (e incluso, medianas) es la dificultad para contar con un DPO interno que reúna todas las competencias requeridas. Por tanto, se recomienda que la Agencia fomente y regule expresamente la posibilidad de: (a) Designar un **DPO compartido** entre varias empresas del mismo grupo o sector. (b) **Externalizar la función del DPO** a consultores o entidades especializadas.

Esta figura ya reconocida en el GDPR (art. 37.2) puede facilitar el cumplimiento normativo en pequeñas organizaciones, siempre que se garanticen: (a) Autonomía funcional del DPO. (b) Ausencia de conflictos de interés. (c) Confidencialidad e independencia en el ejercicio de sus funciones.

v. **Asegurar que toda interpretación respecto la designación de un DPO respete el principio de proporcionalidad:** La aplicación del estándar de cumplimiento diferenciado del artículo 14 septies requiere que toda

interpretación sobre la necesidad de designar un DPO sea **coherente con el principio de proporcionalidad** (art. 3, letra c)). En particular, se recomienda evitar enfoques formalistas que generen cargas administrativas desproporcionadas para organizaciones de baja complejidad o riesgo. La designación del DPO debe responder al **riesgo real y la escala de operación**, no únicamente a requisitos genéricos o abstractos.

vi. **Desarrollar capacitaciones sectoriales sobre la función y beneficios del DPO**: Para fortalecer la cultura de cumplimiento en PYMES, la Agencia debería implementar y promover planes de **formación continua** dirigido a responsables y encargados del tratamiento, así como también a DPO que se están iniciando o asumiendo sus funciones, con foco en: (a) La utilidad del DPO como figura de asesoramiento interno. (b) Sus funciones en la gestión de riesgos, relaciones con titulares y autoridades. (c) Buenas prácticas y casos reales de implementación efectiva.

Estas capacitaciones podrían organizarse en alianza con asociaciones gremiales, cámaras de comercio o instituciones académicas, y enfocarse en sectores económicos con alta presencia de PYMES (comercio, servicios, salud, educación, tecnología).

8. CONCLUSIONES

El presente informe identifica un conjunto de nudos interpretativos, vacíos normativos y desafíos operativos en la implementación del régimen de estándares diferenciados para PYMES, establecido en el artículo 14 septies de la Ley N° 21.719. Sobre la base de una revisión normativa, comparada y práctica, se proponen orientaciones técnicas destinadas a facilitar el trabajo de la Agencia de Protección de Datos Personales en el diseño de sus primeras instrucciones generales.

A continuación, se sistematizan las recomendaciones formuladas, agrupadas por ejes temáticos estratégicos:

i. **Criterios para determinar la elegibilidad al régimen diferenciado.**
   - **a.** Emitir una guía interpretativa del concepto de PYME que incluya criterios económicos, operativos y de riesgo.
   - **b.** Exigir la consolidación de ingresos en grupos empresariales o estructuras con control común.
   - **c.** Incorporar criterios como número de trabajadores, capacidad técnica y volumen de tratamiento.
   - **d.** Establecer una "lista de banderas rojas" que excluya automáticamente a ciertas entidades del régimen (tratamiento de datos sensibles, decisiones automatizadas, servicios tecnológicos).
   - **e.** Promover mecanismos de autoevaluación que permitan a los responsables determinar su calificación bajo este régimen.

ii. **Definición de estándares diferenciados en materia de seguridad.**
   - **a.** Desarrollar herramientas automatizadas y guías prácticas que permitan a las PYMES implementar medidas de seguridad proporcionales y de bajo costo.
   - **b.** Establecer un marco mínimo de medidas técnicas y organizativas, priorizando la autenticación multifactor, respaldo de información y control de accesos.
   - **c.** Incorporar criterios de atenuación de sanciones que consideren la capacidad financiera, proactividad y colaboración del infractor.
   - **d.** Promover un enfoque de mejora continua y respuesta responsable frente a incidentes, más que una expectativa de cumplimiento perfecto.

iii. **Transparencia e información.**
   - **a.** Establecer un estándar mínimo uniforme para PYMES de bajo riesgo, centrado en los elementos esenciales del artículo 14 ter.

b. Excluir expresamente de la aplicación del régimen diferenciado a tratamientos de alto riesgo o con impacto significativo en los derechos de los titulares.

c. Desarrollar herramientas prácticas (plantillas, software, matrices de riesgo) para facilitar el cumplimiento en organizaciones pequeñas.

d. Asegurar que las flexibilizaciones no comprometan el nivel de adecuación internacional del sistema chileno de protección de datos.

iv. <u>Relación entre responsables y encargados</u>.

a. Aclarar que la aplicación de estándares diferenciados al encargado debe considerar sus propias capacidades, no solo las del responsable.

b. Prohibir que grandes encargados se beneficien de estándares mínimos por prestar servicios a PYMES.

c. Publicar modelos de cláusulas contractuales que reflejen criterios de proporcionalidad y corresponsabilidad.

d. Establecer lineamientos diferenciados según sector y escala organizacional del encargado.

v. <u>Designación del Delegado de Protección de Datos (DPO)</u>

a. Desarrollar criterios interpretativos proporcionales sobre los conceptos de “gran escala” y “monitoreo sistemático”, considerando el tamaño y sector de la organización.

b. Promover modelos compartidos o externalizados de DPO, especialmente entre PYMES del mismo sector o territorio.

c. Incluir orientaciones en las listas de Evaluación de Impacto respecto a la recomendación de nombrar un DPO.

d. Fomentar la adopción voluntaria de modelos de cumplimiento con beneficios regulatorios claros y herramientas sectoriales simplificadas.

e. Impulsar programas de capacitación sectorial sobre la función y utilidad estratégica del DPO.