

El rol del DPO en las AFP: generando sinergia

Julián Márquez¹

El contexto actual de la protección de datos personales en Chile propone un panorama lleno de oportunidades. Sin conocer cómo quedará finalmente la nueva Ley de Protección de Datos Personales (en adelante, LPDP), no hay duda que habrá cambios para los actores involucrados. Reguladores, empresas, profesionales y proveedores, tendrán que evaluar sus condiciones actuales contra la nueva norma y aprender a operar bajo un esquema que, hasta ahora, es desconocido.

A nivel de industria se destacan las Administradoras de Fondos de Pensiones, porque prestan servicios y manejan datos de un gran porcentaje de la población nacional. Según las estadísticas de la Superintendencia de Pensiones (en adelante, SP), a marzo de 2024 estaban afiliadas 11.749.951 de personas en alguna de las siete AFP activas. Esta cantidad corresponde a casi el 60% de los habitantes de Chile, estimados para 2024.

Adicionalmente, las prácticas de protección de datos personales y sensibles no son ajenas al sector. La SP ha hecho un gran trabajo incluyendo reglas relacionadas en el Compendio de Normas del Sistema Pensional. Estos lineamientos, constantemente auditados por el regulador, también obligan a las AFP a resguardar información de afiliados según su nivel de sensibilidad (por ejemplo, pidiendo mayores detalles y aprobaciones cuando se usan datos biométricos.)

Sin embargo, dado que la Ley local estará basada en el Reglamento Europeo para Protección de Datos (GDPR), la situación normativa de las Administradoras se hará más compleja. Las problemáticas que contribuyen a esta situación se pueden resumir a continuación:

- **Coordinación:** Aunque el Compendio define obligaciones relacionadas con aspectos de privacidad, la nueva norma definirá medidas que podrían solaparse e incluso contravenir a la SP. Por ejemplo, las reglas referentes al Sistema de Gestión de Seguridad y Ciberseguridad indicadas en el Libro V, Título XVIII del Compendio, funcionarían como base. Sin embargo, no tendrían el nivel de detalle requerido por la nueva LPDP.

¹ Ingeniero electrónico y de telecomunicaciones Universidad San Martín. Data Protection Officer Principal Chile.

- **Adaptación:** Al desplegar procesos para gestionar datos personales, las capacidades instaladas deben complementarse con los requerimientos de la nueva Ley. Un caso para tener mayor referencia se presenta en la gestión de incidentes: la SP tiene lineamientos para facilitar la contención y la respuesta ante incidentes generales (Libro V, Título XIV, Capítulo V). Sin embargo, el Artículo 14 sexies del texto actual de la LPDP incluye obligaciones sobre reporte de incidentes con un nivel de detalle no contemplado por la Superintendencia (por ejemplo, datos sensibles expuestos, clasificación de criticidad según categorías de datos expuestos, datos de menores de edad, entre otros).
- **Implementación:** La LPDP requerirá implementar competencias que no existen en la normativa aplicable a las AFP. Por ejemplo, las metodologías para evaluar el impacto a la privacidad en iniciativas, proyectos o cambios (artículo 15 ter).

En este escenario debe existir una figura como el Oficial de Protección de Datos (DPO) para que las Administradoras puedan abordar los anteriores desafíos. Aunque la versión actual de la LPDP indica que la designación del delegado de protección de datos personales es voluntaria (Artículo 49, literal a), el profesional que ocupe esta posición será clave para avanzar positivamente al asumir estos retos.

Debido a su nivel de especialización, el DPO deberá definir políticas sobre privacidad según los requisitos de la Ley y asegurar que convivan armónicamente con otras reglas de la empresa que se refieran a los datos personales. Por otra parte, debe plantear iniciativas operativas que articulen esa política, y hacer seguimiento a los estados de avance. Lo anterior implica que el DPO deberá evitar ocuparse de tareas rutinarias que le dificulten desarrollar una visión holística de la situación de la AFP en el manejo de la información de personas.

Con ese contexto, a continuación, se presentan actividades sugeridas que ayudarán al DPO en abordar cada factor mencionado anteriormente:

- **Coordinación:**

- Identificar requerimientos de la Ley total o parcialmente cubiertos con las medidas implementadas en la Administradora. Estos requisitos podrían estar relacionados con las normativas de la SP, políticas internas u otras definiciones.
 - Analizar brechas para lograr el cumplimiento, definiendo cómo pueden resolverse y quién debe ser responsable de accionar ese cambio, evitando asumir compromisos operativos de otras áreas.
 - Definir un plan de trabajo priorizado, mapeando sinergias y áreas de conflicto con otros requerimientos normativos.
- **Adaptación:**
 - Aprovechar cualquier sinergia existente para evitar duplicidad o ambigüedad en lineamientos.
 - Evitar la definición de procesos separados sobre privacidad y trabajar con enfoque en complementarlos con conceptos específicos bajo su dominio (por ejemplo, no debe definirse un nuevo proceso para gestión de incidentes de privacidad. Más bien, las definiciones existentes deben complementarse con aspectos asociados a los datos personales, tales como las categorías de datos afectados, su nivel de sensibilidad y la diferenciación de titulares involucrados para definir criticidad del incidente).
- **Implementación:**
 - Identificar procesos y proveedores más impactados por los cambios normativos, y soportar a cada equipo con propuestas de soluciones operativas y tácticas que faciliten la transición.
 - Asegurar que las medidas técnicas estén alineadas con los principios básicos de la norma (una buena estrategia puede ser entregando checklists fáciles de revisar durante el desarrollo de productos, para que los equipos incluyan criterios de privacidad en las consideraciones de diseño).
 - Mantener programas de comunicación y capacitación que refuercen continuamente la importancia de proteger la información personal.
 - Asegurar que cualquier comunicación dentro del programa anterior utilice el lenguaje del área objetivo del mensaje (por ejemplo, las capacitaciones de privacidad para las

áreas de desarrollo de software deben hablar del impacto que tienen estas medidas en cada etapa del ciclo de vida del software).

El camino por recorrer aún tiene muchas incógnitas que se irán resolviendo lentamente. Pese a ello, en el caso de las AFP se podría esperar una transición más suave, gracias a la sólida base normativa y operacional de cada Administradora. Pese a ello, es necesario estar alerta, puesto que la probabilidad de que aparezcan situaciones que amenacen esta proyección es alta. Considerando el dinamismo del entorno actual desde una visión regulatoria, tecnológica y económica, es difícil predecir cómo cambiarán las expectativas de las partes relacionadas.

En consecuencia, este esquema le permitirá al DPO de cada AFP dar conceptos con mayor relevancia y ganar visibilidad. Por el rol que debe asumir, está llamado a aconsejar a la alta gerencia sobre amenazas y vulnerabilidades que puedan alterar el entorno. De este modo, mantendrá la tranquilidad ante la incertidumbre y promoverá una cultura proactiva y colaborativa, donde la transparencia en el manejo de datos sea un hecho, no sólo un deseo.