Marzo 2026

Política de **Protección de Datos Personales**

FONDO AUTÓNOMO
PROTECCIÓN PREVISIONAL

ÍNDICE

Nombre del Documento:	Política Institucional de Protección de Datos Personales
Versión:	1.0
Fecha de Aprobación:	Marzo 2026
Órgano de Aprobación:	Consejo del Administrador del Fondo Autónomo de Protección Previsional
Próxima Revisión:	Diciembre 2026
Responsable:	Dirección de Tecnología y Datos

Política de Protección de Datos Personales del Administrador del Fondo Autónomo de Protección Previsional

CONTEXTO

El Administrador del Fondo Autónomo de Protección Previsional (en adelante, el "Administrador") es un organismo público —de carácter técnico y autónomo—, creado por la Ley N° 21.735 de Reforma Previsional de 2025, cuya función principal es financiar las prestaciones y beneficios del Seguro Social Previsional. Para ello, tiene el mandato de administrar la gestión e inversión de los recursos del Fondo Autónomo de Protección Previsional (en adelante, el "Fondo"), con el objetivo de maximizar su rentabilidad a largo plazo y velar por su sostenibilidad financiera a través de generaciones.

El tratamiento de datos personales efectuado por el Administrador se funda principalmente en el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias, especialmente en lo relativo al financiamiento de prestaciones del Seguro Social Previsional, la administración e inversión de los recursos del Fondo, la evaluación de su sostenibilidad financiera, la contratación y supervisión de servicios necesarios para el ejercicio de sus atribuciones, y el intercambio de información con otros organismos y entidades cuando ello sea procedente conforme a la ley. Esta Política constituye el marco institucional de referencia para orientar la implementación de controles, procedimientos y responsabilidades en materia de protección de datos personales.

El Administrador se compromete a proteger los datos personales de todas las personas con quienes se relaciona, garantizando un tratamiento lícito, leal, transparente y seguro, en cumplimiento de la Regulación Aplicable.

El Administrador tratará datos personales exclusivamente en el marco de sus competencias legales y para el cumplimiento de las finalidades asociadas a su mandato institucional, conforme a la Ley N° 21.735 y la Regulación Aplicable.

Esta Política Institucional de Protección de Datos Personales (en adelante, la "Política") constituye el marco normativo interno que establece los principios, lineamientos y requisitos que orientarán la implementación del sistema de gestión de datos personales del Administrador, debiendo interpretarse de forma coherente con las demás políticas institucionales vigentes.

1. OBJETIVO

Esta Política tiene como propósito declarar formalmente la posición del Administrador respecto a los principios y reglas generales que deben regir el tratamiento de los datos personales, sean estos datos de afiliados, beneficiarios, cotizantes, pensionados, proveedores, postulantes a empleos, personal, extrabajadores o cualquier individuo que se relacione con el Administrador.

En particular, los objetivos de esta Política son:

a) Establecer los principios rectores y lineamientos generales para el tratamiento lícito, leal, transparente y proporcional de datos personales por parte del Administrador, en cumplimiento de su calidad de órgano público.
b) Actuar de forma coordinada con los controles establecidos en la Política General de Seguridad de la Información y Ciberseguridad del Administrador, así como con los demás instrumentos normativos internos. Establecer los principios y lineamientos que deberán guiar la elaboración de políticas, procedimientos e instructivos internos del Administrador en materia de protección de datos personales, asegurando su coherencia con la Regulación Aplicable.
c) Establecer normas de conducta para que el personal del Administrador, contratistas, proveedores y cualquier persona que acceda a datos personales bajo responsabilidad del Administrador, cumplan con la Regulación Aplicable y el código de ética institucional.
d) Definir los roles, responsabilidades y canales de reporte necesarios para asegurar la implementación efectiva de esta Política.
e) Promover una cultura organizacional orientada a la protección de datos personales, facilitando la identificación oportuna de riesgos y la implementación de medidas técnicas, organizativas y contractuales adecuadas para mitigarlos, así como el conocimiento general de las actividades de tratamiento realizadas por el Administrador, sus principales características y riesgos asociados, con el objeto de fortalecer su gestión, control y cumplimiento de la Regulación Aplicable.

2. ÁMBITO DE APLICACIÓN

Las disposiciones de la presente Política son de aplicación obligatoria para todas las personas y entidades que, en el marco de sus funciones o de una relación contractual, de prestación de servicios o de colaboración, accedan, traten, gestionen o resguarden datos personales bajo responsabilidad del Administrador, incluyendo:

- Los miembros del Consejo Directivo.
- El Director Ejecutivo.
- Los miembros del Comité Ejecutivo de Gobierno de Datos, Seguridad de la Información y Ciberseguridad.
- La totalidad de los funcionarios y personal del Administrador, independientemente de su condición contractual, incluyendo personal contratado bajo el Código del Trabajo y prestadores de servicios a honorarios.
    - Terceros y proveedores que, en virtud de una relación contractual o de cualquier otra índole, accedan o traten datos personales bajo responsabilidad del Administrador, incluyendo de manera enunciativa y no taxativa, los asesores, consultores y auditores externos; y al l personal de empresas proveedoras, contratistas o subcontratistas que presten servicios al Administrador.
- Entidades externas públicas o privadas, nacionales o internacionales, con las que exista intercambio de información, interoperabilidad o convenios de colaboración, en lo que resulte aplicable respecto de los protocolos de intercambio definidos por el Administrador.

El Administrador tratará datos personales, actuando como organismo público, con la finalidad de dar cumplimiento a sus funciones legales y asegurar el adecuado funcionamiento del financiamiento Seguro Social Previsional (Ley N° 21.735). Sus propósitos principales incluyen:

- Administrar las cotizaciones con rentabilidad protegida (CRP), emitir, registrar y pagar bonos previsionales y disponer los canales para que el titular acceda a su información.
- Gestionar el financiamiento del Seguro Social Previsional y realizar estudios técnicos y actuariales del Fondo para evaluar su sostenibilidad a largo plazo.
- Gestión del financiamiento del SIS, incluyendo las licitaciones para su correcta operación, la contratación de las aseguradoras y la evaluación constante de su viabilidad financiera.
- Intercambiar información para fines operativos y de estudios con organismos públicos y del sistema de pensiones (IPS, AFPs, Compañías de Seguros, Ministerios de Hacienda y Trabajo, Dipres).
- Proporcionar los antecedentes requeridos por la Superintendencia de Pensiones, la Contraloría General de la República y auditores externos en el ejercicio de las facultades regulatorias y de fiscalización de estas instituciones.

El tratamiento de datos personales solo podrá realizarse dentro del ámbito de competencias legales del Administrador, quedando prohibido cualquier tratamiento que exceda las atribuciones conferidas por la Ley N° 21.735 u otras normas habilitantes.

Se regirá por esta Política todo tratamiento de datos personales realizado por el Administrador, con independencia de que el soporte sea físico o digital, y de si el tratamiento es efectuado directamente por el Administrador o por terceros Mandatarios.

El alcance de esta Política comprende el tratamiento de datos personales de las siguientes categorías de titulares:

- Afiliados, beneficiarios y cotizantes del sistema de pensiones y del Seguro Social Previsional;
- Personal, postulantes y ex trabajadores del Administrador; y
- Proveedores, contratistas y otros terceros que se relacionen con el Administrador.

Las infracciones a esta Política y sus consecuencias se encuentran reguladas en este instrumento, en las demás políticas y normas internas del Administrador y en la legislación aplicable.

La presente Política se integra y coordina con los demás instrumentos normativos internos del Administrador que regulan materias relacionadas con la gestión, seguridad y tratamiento de la información.

3. MARCO NORMATIVO REFERENCIAL

El tratamiento de datos personales por parte del Administrador se rige por las siguientes disposiciones, leyes y documentos de referencia (en adelante, la “Regulación Aplicable”):

- La Ley N° 21.735, que crea un nuevo sistema mixto de pensiones y un Seguro Social en el Pilar Contributivo, mejora la Pensión Garantizada Universal y establece beneficios y modificaciones regulatorias.
- La Ley N° 19.628 sobre Protección de la vida privada.
- La Ley N° 21.719 que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, que entrará en vigencia a contar de diciembre de 2026.
- La Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, en lo relativo al principio de probidad administrativa.

- La Ley N° 20.285 sobre Acceso a la Información Pública.
- La Ley N° 21.663, Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información, y las directrices de la Agencia Nacional de Ciberseguridad (ANCI).
- Normativas de carácter general de la Superintendencia de Pensiones en materia de tratamiento de datos personales y demás atingentes, especialmente la NCG 278: Título XVIII. Referente a Sistema de gestión de seguridad y ciberseguridad.

Las instrucciones generales que emita la Agencia de Protección de Datos Personales y la Superintendencia de Pensiones serán incorporadas al marco normativo del Administrador conforme se dicten.

Asimismo, se considerarán las políticas internas vigentes, en especial la Política de Tratamiento y Uso de Información Reservada, la Política General de Seguridad de la Información y Ciberseguridad, la Política de Gestión y Gobierno de Datos, la Política de Riesgos de Terceros y Servicios Externalizados y el Código de Ética institucional.

3.1. Coordinación con Políticas Internas

La presente Política forma parte del marco institucional de políticas de aplicación general del Administrador y debe aplicarse de manera coordinada con los demás instrumentos normativos internos del Administrador, constituyendo un marco coherente de gestión de la información, especialmente con:

- Política de Tratamiento y Uso de Información Reservada
- Política General de Seguridad de la Información y Ciberseguridad
- Política de Gestión y Gobierno de Datos
- Política de Gestión de Riesgos de Terceros y Servicios Externalizados

En caso de conflicto entre esta Política y otras políticas o normativas internas, prevalecerá esta Política únicamente en lo relativo al tratamiento y protección de datos personales, sin perjuicio de la aplicación de la regulación legal vigente especiales en materia de tratamiento de información reservada, seguridad de la información, conservación de antecedentes, continuidad operacional y fiscalización sectorial.

4. DEFINICIONES

Para los efectos de esta Política, los siguientes términos tendrán el siguiente significado:

- Agencia: La Agencia de Protección de Datos Personales, creada en virtud de la Ley N° 21.719.
- Administrador: El Administrador del Fondo Autónomo de Protección Previsional, organismo público, técnico y autónomo, creado por la Ley N° 21.735.
- Anonimización: Tratamiento irreversible de Datos Personales que elimina definitivamente el nexo entre el Titular y la información resultante, de modo que esta deja de constituir Dato Personal.
- Aviso de Privacidad: Instrumento destinado a informar a los Titulares sobre las condiciones esenciales del Tratamiento de sus Datos Personales por parte del Administrador, de conformidad con la Regulación Aplicable.
- Base de Datos Personales: Conjunto organizado de Datos Personales, automatizado o no, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos.
- Comité Ejecutivo de Gobierno de Datos, Seguridad de la Información y Ciberseguridad: Comité creado en la Política Institucional de Gestión y Gobierno de Datos. Es presidido por el Director de Tecnología y Datos y compuesto por los Directores de Riesgos, Administración y Operaciones, Jurídica, Sostenibilidad Financiera, Inversiones, el Gerente de Datos y Analítica, Gerente de Tecnología y las Líderes de Gobierno de Datos y Ciberseguridad. Sesiona mensualmente para supervisar la estrategia, modelo operativo y estructura de Gobierno de Datos.
- Dato Caduco: El que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna.
- Dato Personal: Los datos relativos a cualquier información concerniente a personas naturales, identificadas o identificables. Los Datos Personales incluyen información que puede ser usada por sí misma, pero también en combinación con otra información para identificar a una persona. De esta manera, se distinguen tres elementos principales:
  a) Información: Comprende todo tipo de información, sea numérica, alfabética, gráfica, fotográfica, acústica, biométrica, etc.
  b) Debe tratarse de información relativa a una persona natural, siendo indiferente la naturaleza del dato, antecedente o hecho de que se trate. El Titular de Datos Personales sólo puede ser una persona natural.
  c) Debe tratarse de información que identifique o permita identificar al Titular. Para estos efectos se entiende por "identificable" toda persona cuya identidad pueda determinarse, directa o indirectamente, por ejemplo, mediante uno o más identificadores o varios elementos específicos característicos de su

identidad física, fisiológica, psíquica, económica, cultural o social (tales como: RUT o RUN, número de cuenta corriente bancaria, domicilio, número telefónico –fijo y móvil-, número de cliente etc.). En este último término el elemento determinante para considerar como identificable el dato será el tipo de esfuerzo que se realiza para lograr la identificación de una persona al momento del Tratamiento. De esta forma, no se considerará identificable si es necesario realizar actividades desproporcionadas o en plazos excesivos. Los datos pueden emanar de directamente del Titular de datos o de terceros, sin que ello afecte su naturaleza, pues, siempre estarán ligados a la persona a la cual conciernen.

- Datos Personales Biométricos o Datos Biométricos: Aquellos obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona que permitan o confirmen la identificación única de ella, tales como la huella digital, el iris, los rasgos de la mano o faciales y la voz.
- Datos Personales Sensibles: Aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, que revelen el origen étnico o racial, la afiliación política, sindical o gremial, situación socioeconómica, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los Datos Biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural.
- Delegado de Protección de Datos (DPO): La persona designada por el Administrador para supervisar el cumplimiento de la normativa de protección de Datos Personales, asesorar en el cumplimiento de sus obligaciones legales, monitorear las prácticas internas de Tratamiento, actuar como punto de contacto con la Agencia de Protección de Datos y atender consultas o solicitudes de los Titulares. Sus funciones incluyen:
  a) Asesorar al Administrador sobre sus obligaciones legales en materia de protección de datos.
  b) Supervisar el cumplimiento de esta Política y la Regulación Aplicable.
  c) Actuar como punto de contacto con la Agencia de Protección de Datos.
  d) Atender consultas y solicitudes de los Titulares.
  e) Desarrollar un plan anual de trabajo y rendir cuenta de sus resultados.
  f) Asistir en la identificación y gestión de riesgos asociados al Tratamiento de Datos Personales.

  El Delegado de Protección de Datos ejercerá sus funciones con independencia funcional y reportará al Comité Ejecutivo de Gobierno de Datos, Seguridad de la Información y Ciberseguridad, sin recibir instrucciones respecto del ejercicio de sus funciones técnicas.

En el desempeño de sus funciones, el Delegado de Protección de Datos actuará de manera coordinada con las funciones de gobierno de datos, seguridad de la información, gestión de riesgos, auditoría interna y asesoría jurídica, resguardando en todo caso su independencia. Asimismo, el Delegado de Protección de Datos no deberá desempeñar funciones que comprometan su independencia, en particular aquellas que impliquen la toma de decisiones sobre el Tratamiento de Datos Personales, salvo que existan resguardos adecuados para gestionar eventuales conflictos de interés.

- Derechos de los Titulares: Los derechos que la Regulación Aplicable reconoce a todo Titular para controlar el tratamiento de sus Datos Personales, incluyendo acceder a ellos, rectificarlos, suprimirlos, oponerse a su tratamiento, portarlos, y solicitar el bloqueo temporal.
- Elaboración de Perfiles: Toda forma de tratamiento automatizado de Datos Personales que consista en utilizar esos datos para evaluar, analizar o predecir aspectos relativos al rendimiento profesional, situación económica, de salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de una persona natural.
- Encargado o Mandatario: La persona natural o jurídica que trata Datos Personales por cuenta del Responsable de datos, siguiendo las instrucciones de este último.
- Evaluación de Impacto en Protección de Datos: Evaluación previa destinada a identificar y mitigar riesgos para los Derechos de los Titulares cuando un tratamiento pueda implicar un alto riesgo, en los términos definidos por la Regulación Aplicable.
- Fondo Autónomo de Protección Previsional o Fondo: El fondo creado por la Ley N° 21.735, cuyo objetivo es financiar las prestaciones del Seguro Social Previsional.
- Fuentes de Acceso Público: Todas aquellas bases de datos o conjuntos de Datos Personales cuyo acceso o consulta puede ser efectuada en forma lícita por cualquier persona, tales como el Diario Oficial, medios de comunicación o los registros públicos que disponga la ley.
- Órganos Públicos: Las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política de la República, y los comprendidos en el inciso segundo del artículo 1º de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado. Política: Esta Política de Protección de Datos Personales del Administrador.
- Regulación Aplicable: Normativa vigente en Chile relativa a protección y tratamiento de Datos Personales y que sea aplicable al Administrador, incluyendo leyes, decretos, tratados internacionales ratificados por Chile y que se encuentren vigentes, directivas, instrucciones, y cualquier otra normativa que tenga carácter

obligatorio *incluyendo específicamente la Ley N° 21.735, la normativa dictada por la Superintendencia de Pensiones y el DL N° 3.500 en lo que resulte aplicable*.

- Responsable del Tratamiento o Responsable: La persona natural o jurídica, pública o privada, a quien compete las decisiones sobre los fines y medios del tratamiento de los Datos Personales, independientemente de si los datos son tratados directamente por ella o a través de un Encargado.
- Seudonimización: Tratamiento de Datos Personales que impide que los datos puedan atribuirse a un Titular sin utilizar información adicional, siempre que dicha información adicional se mantenga por separado y sujeta a medidas técnicas y organizativas adecuadas.
- Titular: Las personas naturales, identificadas o identificables, a quien conciernen los Datos Personales. El Titular sólo puede ser una persona natural.
- Tratamiento de Datos o Tratamiento: Cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar Datos Personales, o utilizarlos en cualquier otra forma.

5. DISPOSICIONES GENERALES PARA EL TRATAMIENTO DE DATOS PERSONALES

5.1. Principios del Tratamiento de Datos Personales

Todo Tratamiento realizado por el Administrador deberá respetar los siguientes principios:

a) Principio de Licitud y Lealtad del Tratamiento: Los Datos Personales sólo pueden tratarse de manera lícita y leal. El Tratamiento deberá estar amparado en una base o fuente de licitud suficiente, esto es, en una justificación o hipótesis contemplada en la Regulación Aplicable que permite al Administrador tratar los Datos Personales. El Administrador debe ser capaz de acreditar la licitud del Tratamiento de Datos Personales que realiza y no realizarse a través de medios engañosos o fraudulentos para el Titular.

La lealtad y licitud del Tratamiento implica que éste no se realice mediante medios engañosos, no induzca a error al Titular y sea consistente con las finalidades informadas o legalmente habilitadas, respetando sus expectativas razonables. En consecuencia, las finalidades y demás elementos del Tratamiento deberán encontrarse debidamente definidos e informados conforme a los instrumentos definidos por el Administrador, asegurando adecuados niveles de información y transparencia hacia los Titulares.

b) Principio de Finalidad: Los Datos Personales deben ser recolectados con fines específicos, explícitos y lícitos, y su Tratamiento debe limitarse al cumplimiento de dichos fines. El Administrador sólo podrá utilizar los Datos Personales para los fines informados o para aquellos que autorice la Regulación Aplicable.

   En particular, las finalidades del Tratamiento por parte del Administrador comprenden aquellas funciones y actividades descritas en la Regulación Aplicable.

c) Principio de Proporcionalidad: Los Datos Personales que se recolecten y traten por el Administrador deberán ser adecuados, pertinentes y limitados a lo necesario en relación con los fines que justificaron su recolección. Previo a iniciar una nueva actividad de Tratamiento, deberá evaluarse si el objetivo puede alcanzarse mediante datos anonimizados, datos estadísticos o minimizando la cantidad y sensibilidad de datos utilizados.

   Asimismo, los Datos Personales deberán conservarse únicamente durante el tiempo necesario para cumplir los fines del Tratamiento, sin perjuicio de las obligaciones legales de conservación.

d) Principio de Calidad: Los Datos Personales deben ser exactos, completos, actuales y pertinentes en relación con su proveniencia y los fines del Tratamiento realizado por el Administrador. En este sentido, se deberán adoptar las medidas razonables para suprimir o rectificar, según sea necesario, los Datos Personales inexactos o desactualizados, y para permitir que los Titulares puedan ejercer sus derechos de rectificación y supresión.

e) Principio de Responsabilidad: El Administrador será responsable del cumplimiento de la Regulación Aplicable en materia de protección de Datos Personales y deberá adoptar las medidas necesarias para asegurar la observancia de los principios y obligaciones legales.

f) Principio de Seguridad: En el Tratamiento de los Datos Personales, el Administrador debe garantizar estándares adecuados de seguridad, protegiéndolos contra el Tratamiento no autorizado o ilícito, y contra su pérdida, filtración, daño accidental o destrucción. Las medidas de seguridad deben ser apropiadas y acordes con el Tratamiento que se vaya a efectuar y con la naturaleza de los datos.

g) Principio de Transparencia e Información: El Administrador debe entregar al Titular toda la información que sea necesaria para el ejercicio de los derechos que establece la ley, incluyendo las políticas y las prácticas sobre el Tratamiento de los Datos Personales, las que además deberán encontrarse permanentemente accesibles y a disposición de cualquier interesado de manera precisa, clara, inequívoca y gratuita.

h) Principio de Confidencialidad: El Administrador y quienes accedan a Datos Personales bajo su responsabilidad deberán guardar secreto o confidencialidad respecto de ellos, incluso después de terminada su relación con la institución.

5.2. Bases de Licitud del Tratamiento

Todo Tratamiento de Datos Personales realizado por el Administrador deberá fundarse en una base de licitud reconocida por la Regulación Aplicable. El Administrador deberá identificar, documentar y mantener actualizada la base de licitud aplicable a cada actividad de Tratamiento, ya sea ejecutada directamente o por medio de terceros bajo instrucciones del Administrador.

5.2.1. Bases de Licitud aplicables al Administrador en calidad de Órgano Público

El Administrador, en cuanto a organismo que forma parte de la Administración del Estado, puede tratar Datos Personales lícitamente cuando el Tratamiento se realiza para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias, de conformidad a las normas establecidas en la ley. En estas condiciones, el Administrador actúa como Responsable de datos y no requiere el consentimiento del Titular, específicamente y en virtud del mandato de la Ley 21.735, el Administrador trata datos sin requerir consentimiento para todas las funciones asociadas a: la gestión de financiamiento de beneficios previsionales, evaluación de sostenibilidad, inversiones e intercambio de información con organismos del Estado. Los activos de información asociados se registrarán conforme a la Política de Gestión y Gobierno de Datos del Administrador.

5.2.2. Otras Bases de Licitud

Sin perjuicio de lo anterior, en aquellos Tratamientos que no se vinculen directamente al ejercicio de competencias públicas o que requieran una habilitación adicional, el Administrador podrá fundarse en otras bases de licitud previstas en la Regulación Aplicable, según corresponda, tales como:

a) Consentimiento del Titular: Cuando el Titular otorgue su consentimiento libre, informado, específico e inequívoco. Si este fuera el caso el Administrador deberá implementar mecanismos tecnológicos y administrativos que permitan registrar de manera auditable la obtención del consentimiento, así como facilitar a los Titulares un mecanismo ágil, gratuito y expedito para la revocación de este en cualquier momento.
b) Cumplimiento de obligaciones legales: Cuando el Tratamiento sea necesario para el cumplimiento de una obligación legal.
c) Ejecución de un contrato: Cuando el Tratamiento sea necesario para la celebración

o ejecución de un contrato entre el Titular y el Administrador, si aplicare, o para la ejecución de medidas precontractuales adoptadas a solicitud del Titular.

d) Intereses legítimos: Cuando el Tratamiento sea necesario para la satisfacción de intereses legítimos del Administrador o de un tercero, siempre que no se afecten los Derechos del Titular. En estos casos, el DPO del Administrador deberá validar la utilización o justificación del Tratamiento en esta base de licitud.
e) Formulación, ejercicio o defensa de derechos: Cuando el Tratamiento sea necesario para la formulación, ejercicio o defensa de un derecho del Administrador o el Fondo ante tribunales de justicia u órganos públicos.
f) Tratamiento de datos relativos a obligaciones económicas: Cuando el Tratamiento esté referido a datos relativos a obligaciones de carácter económico, financiero, bancario o comercial y se realice de conformidad con las normas legales aplicables.

5.3. Tratamiento de Datos Personales por Órganos Públicos

En atención a su naturaleza institucional, el Tratamiento de Datos Personales realizado por el Administrador se regirá, además, por las normas especiales aplicables al Tratamiento por Órganos Públicos, en particular en lo relativo a competencias, deber de reserva, coordinación con otros órganos y limitaciones al ejercicio de derechos, en los términos previstos en esta Política y en la Regulación Aplicable.

5.3.1. Principios Específicos para Órganos Públicos

Además de los principios generales, el Administrador observará los principios de coordinación, eficiencia y probidad que rigen la actuación administrativa, procurando la interoperabilidad con otros Órganos Públicos y evitando requerimientos redundantes a los Titulares, conforme al artículo 21 de la Ley N° 21.719.

5.3.2. Información a Organismos Públicos

De acuerdo con el artículo 28 Nros. 5 y 12 de la Ley N° 21.735, el Administrador podrá solicitar a organismos públicos la información necesaria para el cumplimiento de sus funciones, dentro del ámbito de sus competencias y conforme a la Regulación Aplicable.

Lo anterior incluye el intercambio de información y suscripción de convenios con instituciones públicas y privadas, así como para la realización de estudios actuariales y demás funciones que correspondan por ley al Administrador.

La información proporcionada por organismos públicos al Administrador no contendrá datos de contactabilidad, tales como número telefónico, domicilio, correo electrónico u otros, conforme al artículo 28 N°12 de la Ley N° 21.735.

5.3.3. Prohibiciones Específicas

En conformidad con el artículo 28 N°12 de la Ley N° 21.735:

a) La información recibida por el Administrador de organismos públicos no podrá ser usada para fines comerciales ni para fines distintos a los relacionados con su deber de velar por la sostenibilidad financiera del Fondo Autónomo de Protección Previsional.
b) El personal del Administrador que acceda a información reservada o Datos Personales en el ejercicio de sus funciones queda sujeto a la obligación de reserva establecida en dicha norma. La infracción de dicha obligación será sancionada de conformidad con lo establecido en la Regulación Aplicable.

5.3.4. Deber de Reserva del Personal

El personal del Administrador deberá guardar reserva y secreto respecto de la información de la que tome conocimiento en el ejercicio de sus funciones, sin perjuicio de las certificaciones o comunicaciones que deban efectuarse conforme a la ley.

La infracción a este deber podrá dar lugar a responsabilidades administrativas, civiles o penales, según corresponda, y constituirá una contravención al principio de probidad administrativa.

El detalle del inventario de Datos Personales y sus finalidades será administrado a través de los instrumentos establecidos en la Política de Gestión y Gobierno de Datos vigente.

6. RECOLECCIÓN Y TRATAMIENTO DE DATOS PERSONALES

La recolección y cualquier otra forma de Tratamiento de Datos Personales se realizará en cumplimiento de los principios establecidos en esta Política y deberá encontrarse amparada en una base de licitud.

6.1. Reglas Generales

El Administrador recolectará Datos Personales únicamente cuando ello sea necesario para el cumplimiento de mandato y/o sus funciones legales.

6.2. Deber de Información

El Administrador debe mantener permanentemente a disposición del público las políticas, condiciones y elementos de información que exija la Regulación Aplicable, mediante Avisos de Privacidad.

Los Avisos deberán contener, al menos, la siguiente información:

a) La fecha y versión del Aviso.
b) La identificación del Administrador y, cuando corresponda, de su representante legal y del Delegado de Protección de Datos.
c) Los canales de contacto para el ejercicio de derechos.
d) Las bases de licitud del Tratamiento.
e) La descripción general de los Titulares a quienes se refiere el Aviso.
f) Las categorías de Datos Personales tratados y su fuente, indicando si provienen de Fuentes de Acceso Público.
g) Las finalidades del Tratamiento.
h) Los destinatarios o categorías de destinatarios a quienes se comunicarán o cederán los datos y la finalidad de dicha comunicación.
i) La eventual transferencia internacional de Datos Personales, cuando corresponda.
j) Los derechos que reconoce la ley a los Titulares y la forma de ejercerlos (Derechos ARSOP).
k) El plazo o criterio de conservación de los Datos Personales.
l) La existencia de decisiones automatizadas, incluida la Elaboración de Perfiles, cuando proceda, y la información relevante sobre su lógica general.

Asimismo, en conformidad con la siguiente tabla, se deberá entregar informacional adicional a los Titulares respecto del Tratamiento de los tipos de Datos Personales señalados, de resultar procedente:

Categoría de Dato Personal	Información adicional
Datos Biométricos	• La identificación del sistema biométrico usado;

	• La finalidad específica para la cual serán utilizados los datos recolectados por el sistema biométrico; • El período durante el cual serán utilizados los Datos Biométricos.
Datos de geolocalización	• El tipo de datos de geolocalización que serán tratados; • La finalidad y duración del Tratamiento; y • Si los datos se comunicarán o cederán a un tercero.

El Administrador deberá mantener actualizadas sus Avisos de Privacidad y establecer procesos determinados para que aquellos sean revisados en caso de modificaciones al contenido informado en ellas, al menos, una vez al año.

6.3. Tratamiento de Datos Personales Sensibles

El Administrador reconoce que, en el ejercicio de sus funciones, puede tratar Datos Personales Sensibles, los cuales requieren un nivel de protección reforzado, como, por ejemplo, datos de relacionados a la gestión y licitación del SIS y Datos Biométricos utilizados en validaciones de identidad en las instalaciones.

El Tratamiento de Datos Personales Sensibles sólo podrá realizarse cuando exista una habilitación legal o concurra alguna de las hipótesis previstas en la Regulación Aplicable.

6.3.1. Medidas Reforzadas de Seguridad

Cuando el Tratamiento involucre Datos Personales Sensibles, el Administrador deberá aplicar medidas de seguridad reforzadas y proporcionales al mayor nivel de riesgo asociado a esta categoría de datos.

Estas medidas deberán revisarse y evaluarse periódicamente, atendida la especial protección que la Regulación Aplicable otorga a los Datos Personales Sensibles y el impacto que podría generar para los Titulares una vulneración de seguridad.

Estas medidas se regirán por lo establecido en la Política de Tratamiento y Uso de

Información Reservada y en la política de seguridad de la información y ciberseguridad del Administrador.

6.4. Privacidad desde el Diseño y por Defecto

El Administrador deberá incorporar la protección de Datos Personales desde el diseño y por defecto en todo sistema, proceso, proyecto o iniciativa que implique Tratamiento de Datos Personales.

Cuando corresponda conforme a la Regulación Aplicable, el Administrador deberá efectuar una Evaluación de Impacto en Protección de Datos Personales. Para cumplir con esto el Fondo implementará un proceso de evaluación de privacidad para proyectos en coordinación con la Dirección de Tecnología y Datos, el Comité Ejecutivo de Proyectos de Tecnología y el Comité Ejecutivo de Gobierno de Datos, Seguridad de la información y Ciberseguridad.

Esto aplicará a nuevos proyectos tecnológicos o modificaciones sustanciales a los existentes.

6.5. Evaluación de Impacto en Protección de Datos Personales

Cuando un Tratamiento pueda implicar un alto riesgo para los Derechos de los Titulares, el Administrador realizará, previo a iniciar las actividades de Tratamiento, una Evaluación de Impacto en Protección de Datos Personales, que incluirá, al menos:

a) La descripción de las operaciones de Tratamiento.
b) La finalidad del Tratamiento.
c) La evaluación de la necesidad y proporcionalidad con respecto a su finalidad.
d) La evaluación de los riesgos para los Derechos de los Titulares.
e) Las medidas de mitigación previstas para abordar los riesgos.

La Dirección de Tecnología y Datos, en coordinación con el Delegado de Protección de Datos y el Comité Ejecutivo Integral de Riesgos, determinará los criterios para identificar Tratamientos de alto riesgo y el contenido de las evaluaciones de impacto, conforme a los lineamientos de la Agencia.

7. COMUNICACIÓN Y TRANSFERENCIA DE DATOS PERSONALES

7.1. Comunicación o Cesión a Órganos Públicos

El Administrador podrá comunicar Datos Personales a otros Órganos Públicos, cuando dicha comunicación resulte necesaria para el cumplimiento de funciones legales y ambos órganos actúen dentro del ámbito de sus respectivas competencias.

La comunicación deberá efectuarse para fines determinados y legítimos, y el órgano público receptor no podrá utilizar los datos para finalidades distintas de aquellas que justificaron su comunicación.

Con todo, el Administrador cumplirá con las condiciones, modalidades e instrumentos para la comunicación o cesión de Datos Personales entre organismos públicos, que se regularán a través de un reglamento expedido por el Ministerio Secretaría General de la Presidencia y suscrito por el Ministro de Hacienda y por el Ministro de Economía, Fomento y Turismo, previo informe de la Agencia una vez que dicho reglamento se encuentre vigente.

Mientras no se dicten o implementen íntegramente los referidos reglamentos o instrucciones, el Administrador deberá resguardar que dichas comunicaciones se encuentren debidamente fundadas, limitadas a los datos necesarios y sujetas a medidas de seguridad adecuadas, manteniendo un adecuado nivel de documentación y control conforme a sus instrumentos internos.

7.2. Comunicación a Personas o Entidades Privadas

La comunicación de Datos Personales a personas naturales o jurídicas de carácter privado requerirá contar con una base de licitud conforme a la Regulación Aplicable.

Cuando la comunicación no se encuentre amparada en una habilitación legal expresa, será necesario el consentimiento del Titular, salvo que la comunicación o cesión de datos sea necesaria para cumplir las funciones del Administrador en materia de cumplimiento de sus obligaciones previsionales u operativas legales en el ámbito de sus competencias.

En todo caso, la comunicación deberá limitarse a los datos estrictamente necesarios para la finalidad que la justifica.

Con todo, el Administrador cumplirá con las condiciones, modalidades e instrumentos para

la comunicación o cesión de Datos Personales entre organismos públicos y personas u organismos privados que se regularán a través de un reglamento expedido por el Ministerio Secretaría General de la Presidencia y suscrito por el Ministro de Hacienda y por el Ministro de Economía, Fomento y Turismo, previo informe de la Agencia.

7.3. Terceros Mandatarios

La contratación de terceros Mandatarios que, en virtud de la actividad o servicio a prestar al Administrador, pudieran tener acceso a Datos Personales, deberá encontrarse regulada debidamente en un mandato para el Tratamiento de Datos Personales que conste por escrito y que considere, al menos:

a) El objeto del encargo.
b) La duración del encargo.
c) La finalidad del Tratamiento de los Datos Personales.
d) El tipo de Datos Personales que serán tratados.
e) Las categorías de Titulares a quienes se refieren los Datos Personales.
f) Los derechos y obligaciones de las partes, incluyendo las facultades para subdelegar.
g) Obligaciones de confidencialidad.
h) Deber de adoptar medidas de seguridad a ser implementadas.
i) Regulación de ámbitos de responsabilidad.
j) La forma en que esta Política le será aplicable.
k) Los terceros estarán obligados a cooperar con el Administrador frente a fiscalizaciones de la Agencia, Superintendencia de Pensiones u otras autoridades, y en la respuesta a incidentes de seguridad.

7.4. Publicación de Convenios o Acuerdos de Intercambio de Información

El Administrador deberá publicar mensualmente en su sitio web institucional los convenios o acuerdos suscritos con otros Órganos Públicos o entidades privadas que contemplen la comunicación, cesión o transferencia de Datos Personales, resguardando la información cuya divulgación esté limitada por ley. Los contratos comerciales o de proveedores tecnológicos se rigen por la Ley de Compras y los mecanismos de la sección 7.3, sin necesidad de publicarse como "convenio mensual" de cesión pública.

El intercambio ocasional de datos amparado en requerimientos formales (oficios) de autoridades competentes no requerirá la publicación de un convenio.

7.5. Transferencia Internacional De Datos Personales

La comunicación o cesión de Datos Personales efectuada por el Administrador a un tercero en el extranjero deberá realizarse en cumplimiento con la Regulación Aplicable.
Son lícitas las transferencias internacionales de datos cuando:

a) Los países de destino que la Agencia de Protección de Datos califique oficialmente que proporcionan niveles adecuados de protección de Datos Personales.
a) Existan cláusulas contractuales, normas corporativas vinculantes, u otros instrumentos jurídicos que establezcan garantías adecuadas.
b) Se adopte un modelo de cumplimiento o mecanismo de certificación que establezca garantías adecuadas.

Las transferencias internacionales de Datos Personales deberán ser evaluadas previamente por el Administrador y sujetarse a medidas adecuadas de resguardo, conforme a la Regulación Aplicable y a sus instrumentos internos.

Mientras no se encuentren plenamente definidos los mecanismos o lineamientos aplicables, el Administrador deberá adoptar medidas reforzadas para asegurar un adecuado nivel de protección de los Datos Personales.

8. DERECHOS DE LOS TITULARES

En conformidad con la Regulación Aplicable, los Titulares podrán ejercer ante el Administrador los derechos que la ley les reconoce respecto de los Datos Personales que este trate en calidad de Responsable.

El ejercicio de estos derechos se efectuará en los términos, condiciones y limitaciones previstas en la Regulación Aplicable, considerando la naturaleza pública del Administrador y sus funciones legales. Asimismo, la procedencia y alcance de estos derechos será evaluada caso a caso, en atención a dichas circunstancias y a las obligaciones legales y regulatorias aplicables.

8.1. Derecho de Acceso

El Titular tiene derecho a solicitar y obtener del Administrador confirmación acerca de si está tratando sus datos y, en la afirmativa, acceder a información sobre:

a) Los Datos Personales relativos a su persona que el Administrador esté tratando.
b) Su procedencia y origen.
c) Los propósitos del Tratamiento.
d) Las categorías o individualización de los destinatarios a los cuales los datos son comunicados o cedidos.
e) El tiempo de conservación y Tratamiento de los datos.
f) La base de licitud del Tratamiento, cuando corresponda.
g) La información sobre la lógica aplicada para decisiones automatizadas que produzcan efectos jurídicos o afecten significativamente al Titular.

8.2. Derecho de Rectificación

El Titular tiene derecho a solicitar y obtener del Administrador la rectificación de sus Datos Personales cuando ellos sean erróneos, inexactos, desactualizados o incompletos. Si la inexactitud proviene de una fuente primaria externa (ej. Registro Civil, IPS, TGR o Administradores Privados), el Administrador derivará el requerimiento a la institución de origen para evitar inconsistencias sistémicas, notificando al Titular.

Cuando los datos provengan de fuentes externas, el Administrador podrá coordinar su rectificación con la entidad de origen o adoptar las medidas necesarias para resguardar la consistencia y trazabilidad de la información, conforme a sus instrumentos internos.

8.3. Derecho de Supresión

El Titular tiene derecho a solicitar y obtener del Administrador la eliminación de sus Datos Personales cuando:

a) Los datos no sean necesarios en relación con los fines del Tratamiento, conforme a los plazos legales y operación del Administrador.
b) El Titular revoque el consentimiento y no haya otro fundamento legal para conservarlos o tratarlos.
c) Los datos hayan sido obtenidos o tratados ilícitamente por el Administrador.
d) Los datos hayan caducado.
e) Los datos deban suprimirse para el cumplimiento de una sentencia judicial, de una resolución de la Agencia de Protección de Datos o de una obligación legal.
f) El Titular haya ejercido válidamente su derecho de oposición al Tratamiento y este haya sido acogido por el Administrador.

El derecho de supresión no procederá cuando los datos deban conservarse en virtud de una obligación legal o regulatoria, especialmente en el ámbito previsional y de seguridad social. Los plazos específicos relacionados a la conservación se definen según el Procedimiento de eliminación y conservaciones de datos del Administrador.

8.4. Derecho de Oposición

El Titular tiene derecho a oponerse al Tratamiento de sus Datos Personales cuando concurran las causales previstas en la Regulación Aplicable, tales como la afectación de sus derechos fundamentales.

El Administrador evaluará la procedencia de la oposición considerando la base de licitud invocada y las obligaciones legales que le resulten aplicables.

8.5. Derecho de Portabilidad

El Titular tiene derecho a solicitar y obtener del Administrador una copia de sus Datos Personales en un formato electrónico estructurado, genérico y de uso común, que permita ser operado por distintos sistemas, y poder comunicarlos o transferirlos a otro responsable de datos. El Titular tendrá derecho a que sus Datos Personales se transmitan directamente de Responsable a Responsable cuando sea técnicamente posible y procedente conforme a la Regulación Aplicable.

8.6. Derecho de Bloqueo

El Titular tiene derecho a solicitar la suspensión temporal del Tratamiento de sus Datos Personales, excepto por el almacenamiento, en los casos establecidos en la Regulación Aplicable.

8.7. Derecho Relativo a Decisiones Automatizadas

Cuando el Administrador adopte decisiones basadas exclusivamente en Tratamientos automatizados que produzcan efectos jurídicos o afecten significativamente al Titular, este tendrá derecho a:

a) Obtener información clara sobre los parámetros y lógica aplicada en el Tratamiento automatizado.

b) Solicitar la revisión humana de la decisión.
c) Impugnar la decisión automatizada cuando corresponda, en conformidad con la Regulación Aplicable.

8.8. Limitaciones

De conformidad con el artículo 23 de la Ley N° 19.628, el Administrador no acogerá las solicitudes de acceso, rectificación, oposición, supresión o bloqueo temporal de los Datos Personales en casos establecidos en la Regulación Aplicable. Toda denegación deberá ser fundada.

Dada la naturaleza de seguridad social del Administrador, se denegará la supresión, bloqueo u oposición cuando el Tratamiento sea imperativo para otorgar o mantener el financiamiento de los beneficios previsionales por mandato legal de la Ley N° 21.735. El derecho a la portabilidad se ejercerá sujeto a factibilidad técnica y conforme a las normas de interoperabilidad que defina la Superintendencia de Pensiones.

8.9. Procedimiento para el Ejercicio de Derechos

El Administrador dispondrá de mecanismos accesibles y gratuitos para el ejercicio de los Derechos de los Titulares. El Administrador priorizará los canales digitales (y convenios institucionales) para canalizar estas solicitudes, lo cual se estructurará en un procedimiento interno de atención de requerimientos.

Las solicitudes deberán ser respondidas dentro del plazo máximo de 30 días corridos, contado desde su recepción. Este plazo podrá prorrogarse por una sola vez y hasta por un período igual, cuando la complejidad o el volumen de las solicitudes lo justifiquen, lo que deberá ser informado oportunamente al Titular.

9. SEGURIDAD DE LOS DATOS PERSONALES

El Administrador adopta un enfoque de privacidad y seguridad por diseño y por defecto, proporcional al riesgo y alineado con la normativa aplicable.

9.1. Marco de Seguridad

El Administrador adopta un enfoque de privacidad y seguridad por diseño y por defecto. Las medidas técnicas y organizativas para la protección de Datos Personales se implementarán

conforme a la Política General de Seguridad de la Información y Ciberseguridad, la cual establece los controles específicos aplicables.

Cuando el Tratamiento involucre Datos Personales Sensibles, se aplicarán medidas de seguridad reforzadas (tales como cifrado de datos y Anonimización de la información) y proporcionales al mayor nivel de riesgo asociado.

9.2. Deber de Reportar Vulneraciones a las Medidas de Seguridad

En caso de producirse vulneraciones de seguridad que implique acceso no autorizado, pérdida, filtración, alteración o destrucción de Datos Personales, el Administrador deberá:

a) Notificar a la Agencia de Protección de Datos Personales dentro de las 72 horas siguientes a su detección, cuando exista riesgo razonable para los Derechos de los Titulares.
b) Comunicar a los Titulares afectados cuando el incidente pueda generar un riesgo significativo para sus derechos, en los términos establecidos por la ley.
c) Mantener un registro interno actualizado de los incidentes, incluyendo su descripción, evaluación, medidas adoptadas y acciones correctivas.
d) Notificar a la Agencia Nacional de Ciberseguridad (ANCI) y al CSIRT Nacional los incidentes de ciberseguridad que comprometan Datos Personales, a través del Líder de Ciberseguridad, conforme a la normativa vigente y los protocolos internos.
d) Notificar a la Superintendencia de Pensiones en el marco de la normativa vigente aplicable a incidentes operacionales.

La gestión, contención y erradicación de los incidentes de seguridad que afecten Datos Personales será coordinada internamente por quien ejerza el rol de Delegado de Ciberseguridad, en estrecha colaboración con quien ejerza el rol de Delegado de Protección de Datos, conforme a los protocolos establecidos en la Política General de Seguridad de la Información y Ciberseguridad. El personal deberá notificar inmediatamente y sin demoras indebidas cualquier sospecha de incidente de seguridad al Líder de Ciberseguridad o a quien haga las veces de Delegado de Ciberseguridad, para activar los protocolos de respuesta internos antes de que comience a correr el plazo legal de 72 horas.

10. SENSIBILIZACIÓN Y CAPACITACIÓN

El Administrador implementará programas de capacitación y/o sensibilización para promover una cultura organizacional orientada a la protección de Datos Personales,

dirigidos al personal, las que deberán ajustarse a las funciones, responsabilidades y niveles de riesgo asociados a los distintos roles dentro de la organización. Asimismo, cuando corresponda, a terceros que traten datos por cuenta del Administrador.

11. ROLES Y RESPONSABILIDADES

Los roles y responsabilidades específicas en materia de protección de Datos Personales se desarrollarán en el Programa de Cumplimiento correspondiente. Sin perjuicio de ello, se establecen las siguientes responsabilidades generales:

11.1. Consejo Directivo

Al Consejo Directivo le corresponde:

a) Aprobar esta Política y sus modificaciones.
b) Supervisar el cumplimiento de esta Política directamente o a través del Comité de Auditoría Interna, Riesgos y Cumplimiento, según corresponda.

11.2. Director Ejecutivo

Al Director Ejecutivo le corresponde:

a) Coordinar la implementación de medidas institucionales en materia de protección de datos.
b) Vía Comité de Gobierno de Datos, Seguridad de la información y Ciberseguridad:
    a. Designar al Delegado de Protección de Datos.
    b. Velar por la independencia funcional del Delegado y por la disponibilidad de recursos adecuados.
    c. Supervisar la implementación de la Política.

11.3. Delegado de Protección de Datos Personales (DPO)

Al Delegado de Protección de Datos Personales le corresponde:

a) Supervisar el cumplimiento de la Regulación Aplicable y toda la normativa del Administrador en materia de protección de Datos Personales.
b) Asesorar al Administrador sobre sus obligaciones en materia de protección de Datos Personales de acuerdo con la Regulación Aplicable.

c) Velar por la concientización y formación del personal que participa en las operaciones de Tratamiento de Datos Personales.
d) Compartir mejores prácticas sobre protección de Datos Personales.
e) Actuar como punto de contacto con la Agencia de Protección de Datos.
f) Coordinar, supervisar y resolver los procesos para atender y resolver solicitudes de ejercicio de derechos por parte de los Titulares de datos.
g) Colaborar en auditorías, inspecciones y procedimientos internos o promovidos por autoridades competentes.
h) Notificar a la Agencia sobre incidentes de seguridad que afecten Datos Personales.
i) Evaluar la necesidad de notificar a Titulares de Datos Personales.
j) Asesorar en las medidas de mitigación y prevención requeridas para resolver incidentes de seguridad.
k) Mantener un registro actualizado de actividades de Tratamiento y de riesgos asociados en un artefacto documental que permita mantener un inventario de los Tratamientos de Datos Personales del Administrador.
l) Reportar directamente al Comité de Gobierno de Datos, Seguridad de la información y Ciberseguridad.

11.4. Comité Ejecutivo de Gobierno de Datos, Seguridad de la Información y Ciberseguridad

Corresponde al 11.4. Comité Ejecutivo de Gobierno de Datos, Seguridad de la Información y Ciberseguridad, coordinar estratégicamente materias de gobierno y calidad de datos, seguridad de la información, ciberseguridad y gestión de riesgos asociados al Tratamiento de Datos Personales, de conformidad con lo establecido en el Estatuto.

11.5. Comité Ejecutivo Integral de Riesgos

Al Comité Ejecutivo Integral de Riesgos le corresponde:

a) Analizar y monitorear los riesgos y controles asociados a la protección de Datos Personales de afiliados y beneficiarios, integrándolos al Sistema de Gestión Integral de Riesgos del Administrador.
b) Actuar como instancia integradora de los aspectos relevantes en materia de privacidad y protección de datos presentados por la Gerencia de Datos y Analítica y la Gerencia de Tecnología, canalizando los reportes correspondientes al Consejo Directivo a través del Comité de Auditoría, Riesgos y Cumplimiento.

11.6. Dirección Jurídica de Administrador

Corresponde a la Dirección Jurídica asesorar en materias legales relativas a protección de datos, revisión contractual, transferencias internacionales y procedimientos ante autoridades competentes. Todo lo anterior, en estricta coordinación y coherencia con la Política de Gestión Integral de Riesgos y definiciones de Auditoría Interna del Administrador.

11.7. Todo el Personal del Administrador

Todo el personal del Administrador, sin distinción de su calidad contractual, tiene la obligación de:

a) Guardar reserva y secreto absolutos sobre los Datos Personales de los que tomen conocimiento en el ejercicio de sus labores.
b) Abstenerse de usar dicha información en beneficio propio o de terceros.
c) Informar a su superior jerárquico y al Delegado de Protección de Datos de cualquier incidente de seguridad que ponga en riesgo la confidencialidad de la información.
d) Participar en las capacitaciones obligatorias en materia de protección de Datos Personales.
e) Cumplir con las disposiciones de esta Política y normas asociadas.

12. INCUMPLIMIENTO

Los destinatarios de esta Política deben tener presente que su incumplimiento, así como el de la Regulación Aplicable, puede acarrear consecuencias significativas para los distintos actores involucrados en las operaciones de Tratamiento:

a) Para el Administrador: Infracciones legales, responsabilidad civil, fallos operacionales, incumplimiento de mandato y daño reputacional.
b) Para los funcionarios: Sanciones disciplinarias, responsabilidad administrativa y, en su caso, responsabilidad civil o penal.
c) Para los Titulares: Perjuicio moral y patrimonial.

12.1. Sanciones Administrativas

Las infracciones a la normativa de protección de Datos Personales cometidas por Órganos Públicos serán sancionadas conforme a lo establecido en la Regulación Aplicable.

12.2. Responsabilidad Individual de los Funcionarios

Sin perjuicio de la aplicación de los procedimientos disciplinarios y sanciones internas, si se determina que existen responsabilidades individuales de uno o más funcionarios del Administrador, la Contraloría General de la República, a petición de la Agencia de Protección de Datos, podrá iniciar una investigación sumaria.

Las infracciones gravísimas constituirán una contravención grave a la probidad administrativa.

La persona que infrinja la obligación de reserva establecida respecto de la información recibida de organismos públicos será sancionada con la pena de presidio menor en cualquiera de sus grados, sin perjuicio de la responsabilidad administrativa cuando proceda, conforme al artículo 28 N°12 de la Ley N° 21.735.

12.3. Sanciones al Personal Externo y Proveedores

En caso de incumplimiento por parte de Mandatarios, contratistas o proveedores que traten Datos Personales por cuenta del Administrador, se aplicarán las medidas contractuales correspondientes, sin perjuicio de las acciones legales que procedan.

Los contratos respectivos deberán contemplar cláusulas que permitan exigir responsabilidades, aplicar multas contractuales, exigir indemnización de perjuicios o poner término anticipado al contrato, según la gravedad del incumplimiento.

12.4. Modelo de Prevención de Infracciones

El Administrador podrá implementar un modelo de prevención de infracciones que cumpla con los requisitos establecidos por la Ley N° 19.628 (y sus modificaciones) y solicitar su certificación ante la Agencia.

13. CANAL DE INFORMACIÓN Y CONSULTAS

Esta Política estará permanentemente disponible y accesible al público en el sitio web institucional del Administrador. Asimismo, el Administrador mantendrá a disposición del público la individualización del Responsable, los datos de contacto del Delegado de Protección de Datos, las categorías de datos tratados, las bases de licitud y una descripción

general de las medidas de seguridad adoptadas.

Toda persona sujeta a esta Política que tome conocimiento de un eventual incumplimiento deberá informarlo al Delegado de Protección de Datos.

14. VIGENCIA

La presente Política entrará en vigencia a partir de su aprobación por el Consejo Directivo del Administrador del Fondo Autónomo de Protección Previsional, en la forma que se indica:

a) Estarán plenamente vigentes desde la aprobación de esta Política las disposiciones relativas a:

- Principios del Tratamiento.
- Seguridad y confidencialidad de los Datos Personales.
- Roles y responsabilidades (a excepción del DPO)
- Deber de reserva del personal.

c) Sin perjuicio de lo anterior, aquellas disposiciones cuya plena operatividad dependa de la entrada en vigor de la Ley N° 21.719, de su normativa complementaria o de su implementación interna, se aplicarán de manera progresiva conforme a un plan de implementación del Administrador. Particularmente, las disposiciones de esta Política que requieran implementación progresiva como: (i) el ejercicio íntegro de derechos ARSOP, (ii) la implementación del Modelo de Prevención de Infracciones, y (iii) las Evaluaciones de Impacto, entrarán en plena vigencia el día 1 de diciembre de 2026, conforme a la entrada en vigor de la Ley 21.719.

Esta Política será revisada anualmente o cuando existan cambios significativos en la Regulación Aplicable o en las operaciones del Administrador que lo ameriten.

Cuadro de versiones y cambios

N° de versión	Principales cambios	Responsable	Instancia de aprobación	Fecha
1.0	Primera Versión	Dirección de Tecnología y Datos	Consejo Directivo	17 Marzo 2026