Diciembre 2025

Política de **Tratamiento y Uso de Información Reservada**

FONDO AUTÓNOMO
PROTECCIÓN PREVISIONAL

ÍNDICE

Nombre del Documento:	Política de Tratamiento y Uso de Información Reservada
Versión:	1.0
Fecha de Aprobación:	Diciembre 2025
Órgano de Aprobación:	Consejo del Fondo Autónomo de Protección Previsional
Próxima Revisión:	Noviembre 2026
Responsable:	Dirección de Tecnología y Datos

Política de Tratamiento y Uso de Información Reservada 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 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 de largo plazo, velando en todo momento por su sostenibilidad financiera a través de generaciones.

El organismo es autónomo, dotado de personalidad jurídica y patrimonio propio, que se relacionará con el Presidente de la República a través del Ministerio de Hacienda. La organización, funciones y atribuciones del Administrador se rigen según lo establecido en la Ley N° 21.735. Asimismo, se encuentra sujeto a la supervisión de la Superintendencia de Pensiones y a la fiscalización de la Contraloría General de la República.

En cumplimiento de sus funciones establecidas por ley, el Administrador requiere acceder y gestionar un volumen significativo de información para el desarrollo de sus funciones y cumplimiento de su mandato legal. En ese contexto, el Administrador generará y accederá, en cumplimiento de su labor, a información reservada, la cual podrá contener datos personales, incluyendo datos que tengan el carácter de sensibles. El Administrador podrá acceder a esta información reservada proveniente de diversos organismos públicos y privados, incluyendo la que reciba en virtud de los diversos convenios de colaboración que suscriba con éstos.

Consciente de la importancia de resguardar la confidencialidad, integridad y disponibilidad de la información reservada, y en cumplimiento con el marco normativo vigente, el Consejo Directivo del Administrador del Fondo establece la presente **Política de Tratamiento y Uso de Información Reservada.**

Esta política tiene por finalidad regular los principios y lineamientos generales para el tratamiento y uso de información reservada, como parte de la gestión integral de seguridad de información del Administrador, y se fundamenta en los principios de probidad administrativa, responsabilidad y legalidad que rigen la función pública, así como en las disposiciones de la Ley N° 19.628 sobre Protección de la Vida Privada y en la Ley N° 21.719, que entrará en vigencia el 1 de diciembre de 2026 y que regula la protección y el

tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales.

Su objetivo es definir un marco normativo claro y riguroso para todos los integrantes del Administrador, garantizando que la gestión de la información, y en especial el uso de la información reservada, se restrinja estrictamente a los fines para los cuales fue solicitada y se gestione bajo los más altos estándares de protección.

Dado que el Administrador se encuentra en etapa de instalación institucional y, asimismo en el proceso de puesta en marcha de su infraestructura tecnológica y operativa, esta primera versión de la política establece los principios, lineamientos y requisitos mínimos que orientarán su implementación progresiva. Las medidas descritas se irán operacionalizando de forma gradual, en coherencia con el desarrollo de la arquitectura tecnológica, la contratación de servicios especializados y la consolidación del modelo de gobernanza institucional del Fondo.

CAPÍTULO I: DISPOSICIONES GENERALES

1. Objetivo

El objeto de esta política es establecer los principios, directrices y responsabilidades para la gestión segura de la información y el tratamiento adecuado de toda información calificada como reservada, manejada por los directivos, funcionarios y colaboradores del Administrador. Su finalidad es asegurar que el uso de dicha información sea exclusivamente para los fines institucionales y conformidad con la normativa sobre protección de datos.

La presente política se dicta en cumplimiento del mandato legal conferido por el artículo 44 N°1 de la Ley N° 21.735 en que se señala como función del Consejo el "*aprobar la normativa interna de funcionamiento y aspectos básicos de la organización, personal y funcionamiento del administrador del Fondo, para el cumplimiento eficaz y eficiente de todas las obligaciones encomendadas por esta u otras leyes*". En dicho sentido, el artículo 28, numeral 12, inciso penúltimo, de la Ley N° 21.735, establece expresamente como función del Consejo Directivo la obligación de "*implementar una política de tratamiento y uso de la información reservada*".

2. Ámbito de Aplicación

Las disposiciones de la presente política son de aplicación, cumplimiento estricto y obligatorio para los miembros del Consejo Directivo y la totalidad de los funcionarios y el personal del Administrador, cualquiera sea su calidad contractual (contrato indefinido, contrato fijo u otro), así como para toda persona, natural o jurídica, que en el ejercicio de sus funciones o en virtud de una relación contractual o de cualquier otra índole, acceda, trate,

gestione o use de cualquier forma información del Administrador.

Quedan comprendidos, de manera enunciativa y no taxativa:

- Los prestadores de servicios a honorarios, asesores, consultores y auditores externos.
- El personal de empresas proveedoras, contratistas o subcontratistas que presten servicios al Fondo.

La obligación de confidencialidad y el deber de cumplir con esta política para resguardar la confidencialidad, integridad y disponibilidad de toda la información del Administrador a la que tengan acceso subsistirán y se mantendrán vigentes aun después de finalizada la relación contractual, laboral o de cualquier otra naturaleza con el Administrador.

3. Marco Normativo Referencial

El tratamiento de la información reservada por parte del Administrador se rige por las siguientes disposiciones, leyes y documentos de referencia:

- 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 del 1 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.
- Normativas de carácter general de la Superintendencia de Pensiones:
- NCG 278: Título XVIII. Referente a Sistema de gestión de seguridad y ciberseguridad.
- El Código Penal, en lo referente a las sanciones por la violación de secretos.
- ISO 27001:2022 Sistemas de gestión de la seguridad de la información. Control A.5.31.

CAPÍTULO II: DE LA INFORMACIÓN RESERVADA

4. Definición de Información Reservada

Para efectos de esta política, se considerará información reservada todo dato, antecedente o documento que el Administrador genere por sí mismo, reciba de organismos privados o

de organismos públicos, tales como, entre otros, la Superintendencia de Pensiones, el Instituto de Previsión Social, el Servicio de Registro Civil e Identificación, el Instituto Nacional de Estadísticas, la Dirección de Presupuestos, la Tesorería General de la República, el Depósito Central de Valores, ya sea que la reciba de forma cotidiana o a través de la suscripción de convenios, y que no tenga el carácter de público. Esto incluye, pero no se limita a:

- Datos personales, incluyendo los datos de afiliados al sistema de pensiones: Esto abarca información vinculada o referida a personas naturales identificadas o identificables, como nombres completos, RUT, fechas de nacimiento, historial de cotizaciones, montos acumulados en cuentas de capitalización individual, beneficiarios, y cualquier otro dato que permita la identificación o se relacione con la situación previsional de una persona.
- 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, la 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.
- Información económica y financiera de las entidades del sistema previsional: Comprende datos estratégicos y de operación de las administradoras de fondos de pensiones, compañías de seguros y otras entidades que integran el ecosistema previsional con las cuales debe interactuar el Administrador, cuya divulgación podría afectar la estabilidad del mercado o la competencia.
- Estudios técnicos y actuariales elaborados con base en información no pública: Incluye análisis, proyecciones y modelos que se nutren de los datos reservados recibidos por el Administrador, así como elaboración propia que conduzca a informes o estudios que deba realizar el Administrador conforme a su mandato, incluyendo informes para evaluar la viabilidad y sostenibilidad financiera del Fondo.
- Información relativa a las reuniones que sostengan los consejeros y altos ejecutivos del Administrador relativas a materias propias de su objeto, con agentes de mercado, ministros de Estado, subsecretarios y quienes ejerzan cargos de elección popular. (Art. 46 inc. 4 Ley 21735)

5. Finalidad del Tratamiento

El Administrador tratará la información reservada, incluyendo los datos personales a los que tenga acceso con el objetivo de cumplir con las obligaciones y funciones que le encomienda la Ley N° 21.735, y dentro de su competencia y atribuciones, rigiéndose siempre por el

principio de finalidad y el principio de licitud, en virtud del cual tratará los datos conforme a las bases de legitimidad establecidas en la normativa vigente para protección de datos personales. Sin perjuicio de lo señalado, el Administrador tratará los datos personales, incluyendo los datos personales sensibles, en conformidad con su Política de Tratamiento y Protección de Datos Personales.

En términos generales, las finalidades del tratamiento de información reservada por parte del Administrador son el correcto financiamiento de los beneficios del Seguro Social Previsional y la eficiente administración de los procesos vinculados al mismo, la gestión e inversión de los recursos del Fondo, el análisis y realización de estudios técnicos y actuariales para velar por la sustentabilidad financiera del Fondo a lo largo del tiempo, así como la entrega de información correspondiente a los cotizantes y beneficiarios del Seguro Social Previsional y el cumplimiento de obligaciones contractuales y regulatorias. Esto incluye, entre otras actividades:

5.1 Realización de Estudios Actuariales y de Sostenibilidad

El Administrador tiene la obligación de realizar estudios técnicos y actuariales y evaluaciones periódicas para proyectar la sostenibilidad financiera del Fondo en el largo plazo. Para esto, acceder a información proporcionada por organismos públicos o privados, incluyendo a información reservada es fundamental, ya que contribuye al cumplimiento de las funciones del Administrador. A modo ejemplar:

- Proyecciones de flujos de beneficios en base a datos demográficos y de esperanza de vida: Utilizando datos anonimizados proporcionados por organismos públicos, el Administrador puede modelar la evolución de la población de cotizantes, pensionados y beneficiarios, anticipando futuras obligaciones de pago.
- Análisis de la densidad de cotizaciones: La información sobre la frecuencia y montos de las cotizaciones de los afiliados que puedan proporcionar organismos tales como la Superintendencia de Pensiones, el Instituto de Previsión Social, la Subsecretaria de Previsional Social, entre otros, permitirían estimar los flujos de ingresos futuros del Fondo.
- Modelamiento de escenarios económicos: Datos económicos y financieros proporcionados al Administrador por diversas entidades públicas y privadas serán utilizados para simular el comportamiento de las inversiones bajo distintas coyunturas económicas (inflación, crecimiento del PIB, tasas de interés), evaluando así riesgos y la rentabilidad esperada.

5.2 Evaluación de la sostenibilidad financiera del Fondo

La ley contempla que el Administrador gestione los recursos necesarios para financiar ciertos

beneficios del Seguro Social Previsional. En este ámbito, el acceso y tratamiento de información reservada es crucial para:

- Evaluar la sostenibilidad financiera del Fondo en el largo plazo: El Fondo requiere realizar estudios técnicos y actuariales basado en datos efectivos de ingreso de cotizaciones y pago de beneficios del Seguro Social, entre otras variables, para resguardar que se pueda solventar el pago de los beneficios sin comprometer su viabilidad a futuro.
- Los datos personales y previsionales: Permiten al Administrador identificar a los grupos de la población que cumplen los requisitos para acceder a determinados beneficios, como insumo relevante para la realización de proyecciones y simulación de escenarios que inciden en sostenibilidad financiera del Fondo, garantizando una correcta asignación de los recursos en conjunto con los organismos competentes en este sentido.

5.3 Monitoreo y Gestión de Riesgos Financieros

El acceso a información detallada del sistema previsional permite al Administrador realizar actividades como:

- Optimizar la política de inversiones: Conociendo en profundidad la composición e información previsional de los afiliados y potenciales beneficiarios del Seguro Social Previsional, el Administrador puede diseñar una estrategia de inversión del Fondo que se ajuste de mejor manera a sus obligaciones futuras, buscando maximizar la rentabilidad con un nivel de riesgo adecuado. Asimismo, para optimizar la política de inversiones y asegurar que la gestión de activos se ajuste a las obligaciones futuras, se requiere un monitoreo exhaustivo sobre los resultados de las carteras de inversión administrados por terceros que el Administrador seleccione mediante licitación. Esto implica conocer el detalle del cumplimiento de límites, la composición de activos y la rendición de cuentas sobre la adecuación de las inversiones. Dicha información es reservada, ya que revela la táctica financiera y las posiciones de mercado específicas, cuya divulgación podría afectar la efectividad de las estrategias de rentabilidad y riesgo implementadas.

6. Cumplimiento de la Normativa y Transparencia

Respecto de la información reservada que genere o a la que tenga acceso el Administrador, su tratamiento estará sujeto a una estricto resguardo y supervisión.

Respecto al uso de datos personales, el Administrador tomará las medidas necesarias para resguardar que el uso de los datos se ajuste a los fines para los que fueron recabados. Esto

se alinea con los principios de la normativa vigente de protección de datos personales, que exige que todo tratamiento de datos tenga una finalidad lícita y explícita.

7. Prohibiciones

El uso de la información reservada está estrictamente limitado al cumplimiento de los fines expuestos en la presente política y en el marco de las funciones legalmente asignadas al Administrador. Respecto al uso de datos personales, será necesario considerar las limitaciones y consideraciones establecidas en la Política de Protección y Tratamiento de Datos Personales, así como las finalidades de tratamiento de datos informadas en los Avisos de Privacidad dirigidos a los titulares de tales datos.

Todo el personal y las partes autorizadas que tengan acceso a dicha información deberán acatar las siguientes prohibiciones de manera irrestricta:

7.1 Prohibiciones Generales de Uso y Divulgación

- Uso para fines no autorizados: Queda terminantemente prohibido utilizar la información reservada para cualquier propósito ajeno a las funciones y objetivos del Administrador y el Fondo, lo que incluye, pero no se limita a, fines comerciales, de marketing o cualquier otra actividad no contemplada en la normativa interna de la institución.
- Divulgación a terceros no autorizados: Se prohíbe estrictamente divulgar, comunicar, ceder, compartir o transferir información reservada a terceros, tanto dentro como fuera de la institución. Sin perjuicio de lo anterior, esta restricción no aplica al intercambio de información realizado para fines de cumplimiento normativo, a la publicación de informes mandatados del Administrador, ni a la cesión de datos a terceros conforme a contratos o convenios con base legal y finalidad lícita.
- Beneficio propio o de terceros: Es ilícito el uso de la información reservada para obtener cualquier tipo de beneficio, ventaja o provecho personal o para terceros, ya sea de índole económico, académico, profesional o de cualquier otra naturaleza
- Acceso indebido: Ningún colaborador o persona autorizada podrá acceder a información reservada que no sea estrictamente necesaria para el desempeño de sus funciones específicas. La curiosidad o el interés personal no constituyen una justificación válida para acceder a dicha información.

7.2 Prohibiciones Específicas sobre el Manejo y la Seguridad de la Información Reservada

- Reproducción no autorizada: Se prohíbe la copia, reproducción o duplicación de la información reservada por cualquier medio (físico, digital o electrónico), a menos

que exista una autorización expresa y por escrito del director ejecutivo del Administrador, o del director de tecnología y datos, alternativamente, y se realice para fines estrictamente laborales.

- Sustracción de información: Queda prohibido sustraer o retirar de las instalaciones y/o servicios del Administrador, cualquier documento, archivo físico o dispositivo electrónico con información reservada, sin contar con la debida autorización y los controles de seguridad establecidos para tal fin.
- Uso de dispositivos personales: Se prohíbe el almacenamiento, transferencia o procesamiento de información reservada en dispositivos de almacenamiento personal no autorizados, tales como computadoras portátiles, tabletas, teléfonos móviles, unidades USB o servicios de almacenamiento en la nube ajenos a la institución.
- Alteración o destrucción: Está prohibido alterar, modificar, dañar o destruir información reservada, salvo que dichos actos se realicen en el marco de los procedimientos de actualización o eliminación de datos debidamente autorizados y documentados por el Administrador.
- Divulgación de medidas de seguridad: Se prohíbe revelar a personas no autorizadas las medidas de seguridad, contraseñas, claves de acceso o cualquier otro mecanismo implementado para la protección de la información reservada.
- Acceso y uso autorizado: Todo acceso, consulta, modificación o gestión de la información reservada está estrictamente limitado al personal que cuente con autorización expresa y documentada por parte del director ejecutivo del Administrador, o del director de tecnología y datos, alternativamente. Dicha autorización definirá el alcance y los fines específicos para los cuales se concede el acceso, y no podrá extenderse a otros propósitos.

CAPÍTULO III: DE LAS RESPONSABILIDADES

8. Del Consejo Directivo

Es responsabilidad del Consejo Directivo aprobar, implementar y revisar periódicamente la presente política, así como de adoptar las medidas necesarias para garantizar su efectividad.

9. Del Director Ejecutivo

Responsable de implementar la política y asignar recursos necesarios para garantizar su efectividad.

10. Del Personal del Administrador y el Principio de Probidad Administrativa

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

- Guardar reserva y secreto absolutos sobre la información reservada de la que tomen conocimiento en el ejercicio de sus labores.
- Abstenerse de usar dicha información en beneficio propio o de terceros.
- Informar a su superior jerárquico de cualquier incidente de seguridad que ponga en riesgo la confidencialidad de la información.

La contravención a las obligaciones de reserva y secreto por parte del personal del Administrador será considerada una falta grave al principio de probidad administrativa conforme al Código de Ética.

CAPÍTULO IV: DEL TRATAMIENTO Y RESGUARDO DE LA INFORMACIÓN

11. Sistema de Gestión de Seguridad y Ciberseguridad (SGSC)

11.1 Marco del Sistema

El Administrador del Fondo implementará un Sistema de Gestión de Seguridad y Ciberseguridad (SGSC) basado en el Título XVIII de la NCG 278 de la Superintendencia de Pensiones o la que la modifique o reemplace. El detalle del SGSC será abordado en la Política de Ciberseguridad y Seguridad de la Información, estableciendo una gestión resiliente que permita optimizar los procesos y garantizar la confidencialidad, integridad y disponibilidad de los activos, con especial énfasis en la información reservada

12. Administración de Riesgos y Declaración de Controles

12.1 Administración Continua de Riesgos

La administración del riesgo de seguridad de la información y ciberseguridad debe ser un proceso continuo e integral. Este proceso debe incluir la identificación, análisis y evaluación de riesgos, considerando el contexto interno y externo de forma permanente para prospectar los riesgos con un enfoque preventivo.

12.2 Evaluación y Reporte de Riesgos

Los dueños de los procesos deben identificar las amenazas, vulnerabilidades y activos de información que podrían ser afectados. Se deberá estimar el nivel de riesgo inherente y el nivel de riesgo residual. Los resultados de la evaluación de riesgos y las decisiones adoptadas respecto de su tratamiento deben ser comunicados oportunamente al Consejo Directivo.

12.3 Plan de Tratamiento de Riesgos (PTR)

Para los riesgos no tolerables, se elaborará un Plan de Tratamiento de Riesgos (PTR) para el tratamiento de información reservada, el cual debe ser planificado y presupuestado. Se

deberá comunicar oportunamente al director ejecutivo y al Consejo Directivo el avance de la implementación del PTR.

12.4 Clasificación de la Información

Toda la información manejada por el Administrador será clasificada según su nivel de sensibilidad y criticidad. Se establecerán, como mínimo, las siguientes categorías: "Uso Público", "Uso Interno", "Confidencial" y "Reservada". La información proveniente de los organismos públicos para la realización de estudios técnicos y actuariales será catalogada por defecto como "Reservada" y estará sujeta a los más altos niveles de protección; asimismo, calificarán como “Reservada” los datos personales, incluyendo datos personales sensibles, de los afiliados. Este proceso de clasificación permitirá priorizar los esfuerzos de seguridad.

Durante la fase inicial de operación, y mientras se completa la implementación de plataformas automatizadas, el inventario de información y su clasificación se mantendrá mediante un registro manual o semiautomatizado, consolidado por la Dirección de Tecnología y Datos. Dicho registro identificará la fuente de origen, el tipo de dato, el nivel de sensibilidad, el custodio responsable y los mecanismos de transferencia asociados autorizados.

12.5 Medidas de Seguridad Física

Se implementarán controles para proteger las instalaciones, los equipos y la información en formato físico contra amenazas que puedan comprometer su seguridad.

- Control de Acceso Físico: El acceso a las instalaciones del Administrador, y en particular a las áreas donde se almacena o procesa información reservada (como bases de datos), estará estrictamente controlado. Se utilizarán sistemas de control de acceso, como tarjetas de identificación o datos biométricos, para asegurar que solo el personal autorizado pueda ingresar a las dependencias.
- Vigilancia y Monitoreo: Las instalaciones contarán con sistemas de personal de seguridad las 24 horas del día, los 365 días del año.
- Gestión de Soportes Físicos: Para casos de fuerza mayor o solicitudes de autoridades en que se requiera almacenar información reservada en dispositivos de almacenamiento (discos duros, cintas de respaldo, etc.), estos serán almacenados en gabinetes o bóvedas seguras. Su transporte fuera de las instalaciones tanto física como en la nube deberá ser autorizado por el Director de Tecnología y Datos y registrado. La destrucción de estos soportes, una vez finalizado su ciclo de vida, se realizará mediante métodos seguros que garanticen la irrecuperabilidad de la información.

12.6 Medidas de Seguridad Técnicas (Ciberseguridad)

Se aplicarán controles lógicos para proteger la información en formato digital, tanto en reposo como en tránsito, como mínimo se establecen:

- Control de Acceso Lógico: El acceso a los sistemas de información, bases de datos y aplicaciones se gestionará bajo el principio de "menor privilegio", asegurando que los usuarios solo tengan acceso a la información estrictamente necesaria para el cumplimiento de sus funciones. Se implementarán protocolos de Control de Acceso Basado en Roles (RBAC).
- Autenticación Robusta: Se exigirá el uso de mecanismos de autenticación multifactor (MFA) para el acceso a sistemas y en particular para los que contengan información reservada. Las contraseñas deberán cumplir con políticas de complejidad, longitud y rotación periódica.
- Cifrado de la Información: La información reservada deberá ser cifrada tanto en reposo (en servidores y bases de datos) como en tránsito (a través de redes internas y externas). Se utilizarán algoritmos criptográficos robustos y actualizados. Se buscará implementar esta medida de seguridad siempre que la viabilidad técnica y operacional lo permita.
- Seguridad de Red: Se implementarán cortafuegos (firewalls), accesos remotos seguros (VPN), sistemas de detección y prevención de intrusiones (IDS/IPS) y otras tecnologías para proteger el perímetro de la red institucional y segmentar las redes internas, aislando los sistemas más críticos.
- Gestión de Vulnerabilidades y Actualizaciones: Se establecerá un programa de gestión de vulnerabilidades que incluirá análisis periódicos de los sistemas para identificar y mitigar debilidades de seguridad. Se aplicarán parches y actualizaciones de seguridad de manera oportuna en todo el software y hardware institucional.

12.7 Medidas de Seguridad Administrativas

Se establecerán políticas, procedimientos y controles organizacionales para orientar la gestión de la seguridad de la información.

- Acuerdos de Confidencialidad: Todo el personal y terceros (proveedores o consultores) con acceso a información reservada deberán suscribir acuerdos de confidencialidad y no divulgación (NDA) que detallen sus obligaciones y las consecuencias de su incumplimiento.
- Procedimiento de Respuesta a Incidentes: Se establece que el Plan de Respuesta a Incidentes, sus protocolos de actuación (detección a recuperación) y los mecanismos de comunicación a autoridades serán definidos en la *Política General*

de Seguridad de la Información y Ciberseguridad.

- Auditorías y Revisiones Periódicas: Se elaborará anualmente un plan de auditoría que abarque todos los riesgos de seguridad. La evaluación del cumplimiento de la presente política será realizada por auditores externos una vez al año. Se mantendrá un registro de los profesionales que auditaron la seguridad de la información. Los resultados de estas auditorías serán presentados al director ejecutivo y Consejo Directivo para propuestas de acciones correctivas.
- Continuidad del Negocio y Recuperación ante Desastres: Se elaborarán planes de continuidad del negocio (BCP) y de recuperación ante desastres (DRP) para asegurar que las funciones críticas del Administrador puedan restablecerse en un tiempo razonable tras un incidente disruptivo, garantizando la disponibilidad de la información esencial.

13. Seguridad en la Cadena de Suministro y Gestión de Terceros

El Administrador debe garantizar que todas las entidades y personas que accedan traten o gestionen información reservada, en virtud de una relación contractual o de cualquier otra índole (incluidos los prestadores de servicios y proveedores), cumplan con los más altos estándares de protección, en línea con los requisitos de seguridad establecidos por la normativa vigente y esta política.

Asimismo, respecto de terceros que actúen en calidad de encargados para el tratamiento de datos personales respecto de los cuales el Administrador es responsable, se deberá velar porque se firmen los encargos de tratamiento de datos exigidos por la regulación de protección de datos, conforme a lo establecido en la Política de Protección y Tratamiento de Datos Personales.

13.1 Lineamientos para las Relaciones con Proveedores

- Identificación y Evaluación del Riesgo: El Administrador deberá identificar y evaluar los riesgos de seguridad de la información y ciberseguridad asociados a los servicios provistos por terceros. Esta evaluación se realizará de forma continua, especialmente al diseñar o modificar procesos que dependan de servicios externalizados.
- Requisitos Contractuales: Los acuerdos con proveedores, contratistas o subcontratistas deben contener medidas apropiadas para cumplir con la presente Política y con la Política de seguridad de la información y ciberseguridad del Administrador. Esto incluye la gestión de riesgos de la cadena de suministro con todo proveedor que pueda acceder, procesar, almacenar, comunicar o proveer infraestructura tecnológica o información del Fondo.
- Evaluación y Verificación: Se debe realizar la evaluación periódica de los

proveedores para confirmar que cumplen con las obligaciones contractuales y los estándares de seguridad y ciberseguridad establecidos por el Administrador.

- Gestión de Cambios: El administrador debe gestionar y aprobar los cambios en los servicios prestados por los proveedores, asegurando que se realicen en cumplimiento con la política de seguridad de la información y ciberseguridad.
- Continuidad y Resiliencia en Terceros: Los planes de continuidad del negocio (BCP) y recuperación ante desastres (DRP) (mencionados en el Artículo 10.4) deben asegurar la disponibilidad de los servicios críticos, y deben ser probados periódicamente, incluyendo específicamente la verificación de los servicios externalizados.

13.2 Responsabilidades Post-Contractuales

La obligación de confidencialidad y el deber de cumplir con esta política subsistirán y se mantendrán vigentes aun después de finalizada la relación contractual, laboral o de cualquier otra naturaleza con el Administrador, debiendo asegurar la devolución de todos los activos del Administrador que estén en su posesión.

13.3 Trazabilidad y Monitoreo

Con el propósito fundamental de establecer la responsabilidad individual, facilitar auditorías de seguridad, investigar incidentes y disuadir el uso indebido de la información, el Administrador implementará un sistema integral y sistemático de registro y monitoreo (logging) de toda actividad relacionada con el acceso y uso de la información reservada. Este sistema deberá ser capaz de reconstruir la secuencia de eventos que afectan a un dato o sistema específico.

CAPÍTULO V: DE LAS INFRACCIONES Y SANCIONES

14. Responsabilidad Penal y Administrativa

La persona que infrinja las obligaciones de reserva de la información gestionada por el Administrador quedará sujeto a la responsabilidad dispuestas por el marco legal, pudiendo incluir sanciones civiles, administrativas y penales.

Asimismo, el incumplimiento de las disposiciones de esta política por parte del personal del Administrador dará lugar, sin perjuicio de lo mencionado en el párrafo precedente, a la responsabilidad administrativa y civil correspondiente, como señala expresamente el artículo 57 de la Ley N° 21.735.

15. Notificación de Incidentes

Gestión de las Comunicaciones. El Administrador establecerá una matriz de comunicaciones que defina cómo, cuándo y a quién se entrega la información de incidentes

de seguridad.

Se exige la **comunicación inmediata de incidentes de seguridad y ciberseguridad a la Superintendencia de Pensiones** cuando las consecuencias puedan comprometer los objetivos, la información de cotizantes o beneficiarios o la reputación del Administrador y/o el sistema de pensiones.

Asimismo, la matriz de comunicaciones deberá definir cómo y cuándo se notifican los incidentes de seguridad y ciberseguridad que puedan afectar datos personales a la Agencia de Protección de Datos Personales y a los titulares de datos, en conformidad con los criterios que establezca la Política de Protección y Tratamiento de Datos Personales.

CAPÍTULO VI: DISPOSICIONES FINALES

16. Difusión y conocimiento, capacitación

Esta Política debe estar disponible para todos los funcionarios del Administrador y para los terceros que presten servicios al mismo y tengan acceso a información. Su difusión se realizará a través de los medios de difusión establecidos por el Administrador para estos efectos. La Dirección de Tecnología y Datos será responsable de difundir esta Política.

El Administrador implementará un programa de capacitación anual y obligatoria para todo su personal sobre la presente política y las normativas vigentes en materia de protección de datos y probidad administrativa. El programa de capacitación deberá **identificar las necesidades de capacitación de cada rol** (incluyendo propietarios de riesgo, custodios y personal de proveedores de servicio.

Este proceso deberá también contemplar que el personal de los **proveedores de servicios cuente** con conocimientos básicos de seguridad de la información y ciberseguridad.

En esta primera fase de instalación institucional, la difusión de la política se realizará mediante sesiones de inducción y capacitación dirigidas a los funcionarios, asesores y prestadores de servicios, dejando constancia de su recepción y compromiso de cumplimiento. Una vez desplegada en la plataforma o repositorio institucional, las futuras versiones y materiales de apoyo estarán disponibles de forma digital para consulta permanente.

17. Revisión y Actualización

Esta política será **revisada y actualizada por el Consejo Directivo al menos una vez al año**. La política deberá ser actualizada siempre que ocurran cambios en los procesos del

Administrador que afecten o pudieran afectar la seguridad.

18. Vigencia

La presente política entrará en vigencia a partir de su aprobación por el Consejo Directivo del administrador del Fondo Autónomo de Protección Previsional.

CAPÍTULO VII: DISPOSICIONES TRANSITORIAS Y DE IMPLEMENTACIÓN PROGRESIVA

19. Objetivo Transitorio

Este capítulo tiene por objeto establecer las medidas y lineamientos aplicables durante la etapa inicial de implementación de la presente política, mientras el Administrador se encuentra en proceso de instalación institucional y previo a la operación completa de su infraestructura tecnológica.

20. Responsabilidad interina y gobernanza temporal

Hasta la conformación formal del Comité de Seguridad y Ciberseguridad y la designación del Oficial de Seguridad de la Información, la Dirección de Tecnología y Datos asumirá interinamente la responsabilidad de supervisar la aplicación de esta política, coordinando con la Dirección Ejecutiva y reportando al Consejo Directivo.

21. Plan de implementación inicial

La Dirección de Tecnología y Datos deberá presentar al Consejo Directivo un plan de implementación inicial que contemple como mínimo los siguientes hitos:

- Elaboración y aprobación de la Declaración Obligatoria de Controles (DOC).
- Levantamiento del inventario de fuentes de intercambio de información.
- Elaboración de convenios de transferencia y protocolos de interoperabilidad.
- Creación del Comité de Privacidad, Seguridad de la información y Ciberseguridad.
- Diseño del Plan de Continuidad del Negocio (BCP) y Plan de Recuperación ante Desastres (DRP) que abarca información de todas las categorías del fondo incluso la clasificada como reservada.
- Capacitación y sensibilización inicial de todo el personal.

Dicho plan deberá definir responsables, cronograma, recursos asociados y mecanismos de seguimiento trimestral.

22. Política marco y políticas y procedimientos conexos

La presente política constituye el marco rector normativo de seguridad de la información reservada del Administrador. Para su implementación se contará con procedimientos en materias como gestión de accesos, continuidad operativa, desarrollo seguro, gestión de incidentes, en complemento a otras políticas para Tratamiento de datos personales, Seguridad de información y Ciberseguridad.

Cuadro de versiones y cambios

N° de versión	Principales cambios	Responsable	Instancia de aprobación	Fecha
1	Primera Versión	Matías Morales Dirección de Tecnología y Datos	Consejo Directivo	30/12/2025
2				