Enero 2026

Política de **Gestión y Gobierno de Datos**

FONDO AUTÓNOMO
PROTECCIÓN PREVISIONAL

ÍNDICE

Política de Gestión y Gobierno de Datos

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 Administrador requiere acceder y gestionar un volumen significativo de información, por lo que una gestión de datos de excelencia es crítica para el desarrollo de sus funciones y cumplimiento de su mandato legal. Los datos constituyen el activo estratégico fundamental para la realización de las operaciones del Administrador y el Fondo Autónomo de Protección Previsional, cuyas finalidades de los tratamientos de información 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.

Consciente de que la integridad, calidad y disponibilidad de la información son pilares del cumplimiento del mandato legal y la función pública del Administrador, el Consejo Directivo establece la presente Política de Gestión y Gobierno de Datos, la cual define el marco normativo interno para asegurar que el tratamiento de la información, durante el ciclo de vida de los datos completo, sea gestionado bajo estándares de máxima rigurosidad técnica y responsabilidad en su tratamiento. Para su implementación se crea el Comité Ejecutivo de Gobierno de Datos, Seguridad de la información y Ciberseguridad para su implementación.

Capítulo I: Disposiciones Generales

1. OBJETIVO

El objeto de esta Política es establecer los principios, directrices y el modelo de responsabilidades para el gobierno de los datos en el Administrador, y garantizar la integridad, calidad, trazabilidad y seguridad de la información desde su origen hasta su disposición final y explotación, fomentando una cultura institucional de toma de decisiones basada en evidencia.

Lo anterior, mediante un modelo de gobierno que supervisa la estrategia y operación de los datos, velando por que todos los colaboradores del Administrador comprendan su rol y deberes de protección y gestión de este activo estratégico. A la vez, se fomenta una cultura institucional de resguardo de la privacidad, protección y tratamiento adecuado de los datos que gestione el Administrador en el cumplimiento de sus funciones. Asimismo, busca definir los roles y responsabilidad de cada una de las instancias e integrantes del Administrador, sobre los activos de información en cada parte de los procesos que este desarrolla.

El modelo de Gobierno de Datos, definido en la presente Política, tendrá carácter obligatorio y vinculante para todos los procesos, sistemas, proyectos y decisiones que involucren el uso, generación, transformación o explotación de datos bajo responsabilidad del Administrador.

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 o de colaboración, desarrollen, accedan, traten o gestionen datos u otros activos digitales bajo responsabilidad del Administrador, incluyendo:

- Los miembros del Consejo Directivo.
- 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.
- Terceros y proveedores que, en virtud de una relación contractual o de cualquier otra índole, desarrollen, accedan, traten gestionen datos u otros activos digitales

bajo responsabilidad 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.

- Entidades externas públicas y privadas, locales e internacionales, con las que exista intercambio de información o interoperabilidad y/o convenios de colaboración en lo que resulte aplicable en, y respecto de los protocolos de intercambio seguro definidos por el Administrador.

3. MARCO NORMATIVO REFERENCIAL

Se implementará el Gobierno de Datos y la presente Política como una buena práctica, por cuanto proveen un marco de metodológico estándar[1], donde la rigurosidad en la identificación y clasificación de activos de datos, linaje, definiciones, catálogos y marco de responsabilidades contribuye al cumplimiento de políticas y exigencias normativas.

En este contexto, y sin perjuicio de otras disposiciones y de las instrucciones vigentes de los organismos competentes, para efectos de esta Política se consideran especialmente relevantes:

- **Ley N° 21.735:** Reforma Previsional que crea al Administrador y define su mandato fiduciario.
- **Leyes N° 19.628 y N° 21.719:** Sobre la Protección de la Vida Privada y el tratamiento de datos personales.
- **Ley N° 21.663:** Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información.
- **Normativa Técnica aplicable:** Norma de Carácter General Nº 278 de la Superintendencia de Pensiones, e instrucciones de la Agencia Nacional de Ciberseguridad (ANCI).

Asimismo, se considerarán las políticas internas vigentes, en especial la Política de Tratamiento y Uso de Información Reservada y la Política General de Seguridad de la Información.

[1] Marco metodológico basado en DAMA-DMBOK2 (Data Management Body of Knowledge), estándar global de mejores prácticas para gestión de datos.

Capítulo II: De los Principios y el Ciclo de Vida del Dato

4. PRINCIPIOS DEL GOBIERNO DE DATOS

El Administrador adopta los siguientes principios rectores, de aplicación obligatoria, que guían el Gobierno de Datos a lo largo de su ciclo de vida y orientan la definición de responsabilidades, estándares y controles, en coherencia con las políticas institucionales vigentes:

a) **El dato como activo estratégico:** Los datos son recursos institucionales valiosos que deben ser gestionados con el mismo cuidado y responsabilidad que el resto de los activos de la organización, trascendiendo el enfoque puramente tecnológico para integrar personas, procesos y los sistemas que los soportan.
b) **Responsabilidad proactiva:** El Administrador adoptará en forma preventiva y oportuna las medidas orientadas a resguardar el cumplimiento de las normativas de protección de datos y seguridad de la información.
c) **Seguridad y privacidad por diseño:** La protección de datos personales y sensibles es inherente a cualquier proceso tecnológico o funcional, adoptándose los mecanismos de prevención y resguardo desde su concepción.
d) **Integridad y calidad:** Los datos utilizados por el Administrador para el cumplimiento de sus funciones deben retratar la realidad de la forma más integra, coherente y oportuna posible para la toma responsable de decisiones sobre el Fondo.
e) **Gobernanza de datos formal:** Todo dato debe tener un responsable claramente identificado y una definición única en el Catálogo de Datos que llevará el Administrador. Para ello, se define un modelo de propiedad de datos claro, asignando roles estratégicos, tácticos y operativos, para asegurar una toma de decisiones ágil promoviendo la responsabilidad institucional compartida sobre los activos de información.
f) **Minimización o sujeción del dato a lo estrictamente necesario:** Solo se recolectarán y procesarán los datos adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
g) **Propiedad intelectual y exclusividad:** Los datos, información, archivos y demás contenidos generados u obtenidos en el marco de las actividades encomendadas al Administrador (incluyendo proyectos de investigación), así como aquellos almacenados para su ejecución, se considerarán parte del patrimonio informacional institucional y estarán destinados al cumplimiento de su mandato. Lo anterior se entiende sin perjuicio de los derechos de terceros y de las condiciones contractuales

o licencias aplicables, y en el caso de datos personales, sujeto a la normativa vigente. Cuando corresponda, el Administrador podrá adoptar medidas de resguardo y protección sobre estos activos, conforme a la regulación aplicable y a las definiciones internas que se establezcan.

La aplicación obligatoria de los roles, estándares y controles de Gobierno de Datos basados en estos principios se activará prioritariamente para aquellos datos que cumplan, al menos, uno de los siguientes criterios:

a) Datos clasificados como Confidenciales o Reservados, conforme a los niveles de seguridad de la Política de Tratamiento y Uso de Información Reservada y las categorías de la Ley N° 19.628 y Ley N° 21.719[2].
b) Datos críticos para el cumplimiento de los objetivos estratégicos y obligaciones legales, regulatorias o de reporte institucional del Administrador.
c) Datos cuya finalidad y uso se encuentran directamente asociados al cumplimiento del mandato legal del Administrador, tales como el correcto financiamiento de los beneficios del Seguro Social Previsional y la eficiente administración de los procesos asociados; la gestión e inversión de los recursos del Fondo; el análisis y realización de estudios técnicos y actuariales orientados a velar por la sustentabilidad financiera del Fondo a lo largo del tiempo; y, la entrega de información correspondiente a los cotizantes y beneficiarios del Seguro Social Previsional y el cumplimiento de obligaciones contractuales y regulatorias.

Los demás activos de datos serán incorporados progresivamente conforme al plan de implementación del modelo de Gobierno de Datos.

5. CICLO DE VIDA DE LOS DATOS

El tratamiento de datos en el Administrador comprende todas las etapas en que el dato es registrado, almacenado, transferido y/o manipulado:

a) **Captura:** Recopilación desde fuentes internas (sistemas internos) o externas, en virtud de convenios, contratos protocolos con terceros.

[2] En vigencia en diciembre 2026.

b) **Integración:** Ingesta de datos recopilados en el repositorio institucional del Administrador. El almacenamiento de la Información se realizará exclusivamente en los repositorios autorizados por el Administrador, con el fin de resguardar la confidencialidad, integridad y disponibilidad según su clasificación, y de esta forma asegurar la aplicación de las medidas de protección correspondientes.
c) **Transformación:** Procesamiento, limpieza y aplicación de reglas de técnicas, funcionales respecto de datos recopilados en el repositorio institucional, según corresponda, incluyendo su preparación para usos específicos, tales como los modelos actuariales o de inversiones.
d) **Explotación y uso:** Utilización de los datos por parte de las personas usuarias de los datos para análisis, estudios, reportes financieros y regulatorios y toma de decisiones en general, conforme a los perfiles de acceso y a la clasificación de la información.
e) **Conservación/eliminación/archivo:** El Administrador mantendrá la información únicamente durante el tiempo estrictamente necesario para cumplir la finalidad para la cual fue recabada y para determinar las eventuales responsabilidades que pudieran derivarse de dicha finalidad y del tratamiento de los datos. Los plazos específicos de conservación se definirán progresivamente para cada tratamiento en el "Registro de actividades de tratamiento de datos personales" conforme a las obligaciones legales aplicables. Cumplida la finalidad o vencido el plazo legal, el Administrador dispondrá el bloqueo, archivo o la disposición segura de los datos, según corresponda al tipo de información y a su clasificación. En caso de eliminación, los procesos deberán garantizar la imposibilidad de reconstrucción y de posterior utilización de los datos, mediante mecanismos de destrucción segura/sanitización, aplicando estándares técnicos adecuados al tipo de soporte.

Capítulo III: Clasificación de información

6. CATEGORÍAS DE SENSIBILIDAD DE LOS DATOS

La información y los datos bajo responsabilidad del Administrador se clasificarán en función de su nivel de sensibilidad, usando como referencia la Matriz de Sensibilidad de la Información, con el propósito de asegurar una clasificación acorde con el nivel de protección necesario. Este proceso abarca toda la información gestionada, incluyendo aquella que se crea, genera o incorpora como novedad en los sistemas de la institución.

La clasificación es aplicable a toda información gestionada por el Administrador, con independencia de su formato o soporte, e incluye aquella que se origina, captura, integra, transforma o genera en el marco de los procesos institucionales, así como la información recibida de terceros en virtud de contratos, convenios o mecanismos de interoperabilidad. En caso de duda, se aplicará el criterio de mayor resguardo hasta que se determine formalmente su categoría.

En línea con lo establecido en la Política de Tratamiento y Uso de Información Reservada, se establecen las siguientes categorías:

- **Uso público o pública:** Información que no presenta restricciones para su divulgación ni requiere consideraciones especiales de seguridad o privacidad en su tratamiento. Esto incluye, sin limitarse a, información proveniente de fuentes de acceso público.
- **Uso interno o interna:** Información de carácter operativo o de gestión interna, creada o procesada por el Administrador para la gestión administrativa y el cumplimiento de su mandato. Su acceso se limita a personas usuarias autorizadas y su circulación debe mantenerse dentro del perímetro organizacional, salvo que exista habilitación expresa. La divulgación a terceros no autorizados se considera un incumplimiento de las directrices internas aplicables.
- **Confidencial o sensible:** ., Información protegida cuyo acceso se restringe a roles o perfiles específicos para fines operativos, por cuanto su exposición, modificación o pérdida puede generar impactos relevantes para el Administrador, el Fondo o los titulares de datos. Se considerará información confidencial o sensible, entre otras, la asociada a la gestión de datos previsionales individuales, datos personales de contacto (PII) e informes de auditoría interna. Su divulgación no autorizada puede derivar en incumplimientos normativos, sanciones y riesgo reputacional significativo.
- **Reservada o Altamente Sensible (IAS):** Activos de información críticos sujetos a reserva legal, o aquellos cuya divulgación genere un impacto severo para el Fondo, su Administrador o la estabilidad de los sistemas. Comprende, entre otros, las estrategias de inversión no públicas, microdatos suministrados por otras instituciones bajo convenios de interoperabilidad y/o traspasos de información, y datos personales sensibles.

En consecuencia, la custodia y tratamiento de información Reservada/IAS exige la aplicación obligatoria de los controles de seguridad, prohibiciones, restricciones de acceso y protocolos de resguardo definidos en la Política de Tratamiento y Uso de Información Reservada, así como de las medidas complementarias que establezca el marco normativo o institucional de seguridad de la información.

Capítulo IV: De las Responsabilidades y Estructura de Gobierno

7. ESTRUCTURA DE GOBIERNO DE DATOS

Con el propósito de asegurar una gestión consistente, trazable y segura de los datos a lo largo de su ciclo de vida, el modelo de Gobierno de Datos del Administrador define instancias y responsabilidades diferenciadas para dirigir, implementar y operar el marco de gobierno, facilitando la coordinación entre las áreas de negocio, tecnología y seguridad, y estableciendo mecanismos de escalamiento para la toma de decisiones y la resolución de controversias en materias de datos. Para ello, el modelo operativo se organiza en los siguientes niveles:

a) **Nivel Estratégico:** Se refiere al Comité Ejecutivo de Gobierno de Datos, Seguridad de la información y Ciberseguridad, como instancia superior de dirección, priorización y resolución en estas materias, conforme a lo establecido en su Estatuto.
b) **Nivel Táctico:** Se refiere a la Oficina de Gobierno de Datos, a que se refiere el numeral 9 de esta Política, como instancia responsable de conducir la implementación del programa de Gobierno de Datos. Para ello, articulará y convocará instancias de trabajo con los roles operativos y las áreas involucradas, definiendo mecanismos de coordinación, seguimiento y gestión de avances.
c) **Nivel Operativo:** Se refiere a los roles y equipos responsables del dato en los dominios definidos por el Administrador (incluyendo *Data Owners*, *Data Stewards*, *Data Custodians* y equipos de trabajo), quienes aplican los estándares, controles y prácticas de Gobierno de Datos en el ciclo de vida del dato, de acuerdo con lo establecido en esta Política y en la normativa interna aplicable.

8. DEL COMITÉ EJECUTIVO DE GOBIERNO DE DATOS, SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

El Comité Ejecutivo de Gobierno de Datos, Seguridad de la Información y Ciberseguridad constituye la máxima instancia de dirección, priorización y resolución en estas materias. Es presidido por el **Director de Tecnología y Datos**. Sus funciones principales, detalladas en su Estatuto, incluyen:

- Supervisar la estrategia, modelo operativo, marco metodológico y estructura de Gobierno de Datos.
- Validar y revisar periódicamente la Matriz de Sensibilidad de Datos y Riesgos relacionados en coordinación con la Dirección de Riesgo.
- Resolver, en última instancia, las discrepancias entre áreas sobre la propiedad o gestión de los datos.
- Seguimiento al cumplimiento de las políticas y procedimientos de manera sistemática y reporte al Consejo Directivo con periodicidad mínima anual a través del Comité de Riesgos, Auditoria y Cumplimiento.

El Comité ejercerá funciones de definición estratégica, priorización y resolución de controversias de impacto estratégico o normativo. El seguimiento operativo, ejecución de acuerdos y control periódico del cumplimiento de estándares será responsabilidad de la Oficina de Gobierno de Datos, quien informará periódicamente al Comité.

9. DE LA OFICINA DE GOBIERNOS DE DATOS

La Oficina de Gobierno de Datos es la instancia responsable de la implementación y operación del modelo de Gobierno de Datos. Dirigida por el Líder de Gobierno de Datos y dependiente de la Dirección de Tecnología y Datos, es responsable de:

- Gestionar modelo operativo de Gobierno de datos, proponer roles y liderar las mesas con los responsables operativos en todo el ciclo de vida del dato.
- Gestionar los artefactos de Gobierno de datos como el Catálogo de Datos y el Diccionario de Datos.
- Monitorear el cumplimiento procedimientos y controles de la presente Política.
- Definir y mantener los estándares de arquitectura y calidad de datos.

10. ROLES OPERATIVOS DEL GOBIERNO DE DATOS

Para materializar el Gobierno de Datos en el quehacer cotidiano, el Administrador define roles operativos con responsabilidades específicas y complementarias. Se establecen los siguientes roles para asegurar la custodia efectiva de los activos de datos bajo responsabilidad del Administrador:

- **Gerente de Datos y Analítica:** Responsable de dirigir el Gobierno de Datos de la institución. Diseña y participa de la ejecución la estrategia, estableciendo políticas y procedimientos para asegurar la adecuada gestión de datos, habilitando la toma de decisiones basadas en evidencia.
- **Líder de Gobierno de Datos:** Responsable de la aplicación de la estrategia de gobierno para de todos los proyectos, iniciativas y actividades asociadas.
- ***Data Owner* (Dueño del Dato):** Directores, Gerentes, jefaturas o cualquiera otra denominación referida a cargos que con autoridad sobre un dominio de datos. Define las reglas funcionales y aprueba quienes pueden acceder a que categoría de datos dentro de su ámbito conforme a la Matriz de Sensibilidad y a las políticas vigentes.
- ***Data Steward* (Gestor del Dato):** Especialista técnico/operativo que asegura que las reglas de calidad se cumplan en el día a día.
- ***Data Custodian* (Custodio del Dato):** Responsable técnico (TI) que garantiza el almacenamiento, respaldo y disponibilidad tecnológica del dato, y vela porque las integraciones funcionen correctamente.
- **Líder de Ciberseguridad:** Responsable técnico que implementa las soluciones tecnológicas relacionadas a la seguridad de la información acordadas en la Oficina de Gobierno.

En caso de discrepancia entre otros roles respecto a estándares de calidad, seguridad o uso de los datos, o a la aplicación de políticas, la controversia deberá ser elevada a la Oficina de Gobierno de Datos y, de persistir, al Comité Ejecutivo de Gobierno de Datos, Seguridad de la Información y Ciberseguridad para su resolución. En todo caso, la decisión deberá observar el orden de prelación normativa institucional y, tratándose de información clasificada como Reservada/IAS, aplicarán de manera preferente las restricciones y controles definidos en la Política de Tratamiento y Uso de Información Reservada.

11. DOMINIOS DE DATOS

Con el fin de ordenar la gestión, asignar responsabilidades claras y facilitar la estandarización de definiciones, el Administrador organizará sus datos en dominios lógicos para facilitar su gestión. A cada dominio se asignará un *Data Owner* perteneciente a algunas de las Direcciones técnicas comprendidas en el organigrama institucional del Administrador.

El *Data Owner* asignado a cada Dominio será propuesto por el Líder de Gobierno de Datos y ratificados en el Comité de Gobierno de Datos, Seguridad de la Información y Ciberseguridad. La designación de los encargados se realizará según el involucramiento en proyectos e iniciativas del Administrador con el objeto de asegurar idoneidad y cercanía a las problemáticas del uso de información.

12. GESTIÓN DE EXCEPCIONES

El modelo de Gobierno de Datos se basa en estándares y controles que deben aplicarse de forma consistente. No obstante, de manera excepcional, podrán autorizarse desviaciones específicas a los principios, estándares o roles definidos en la presente Política, cuando existan razones técnicas, operativas o normativas debidamente justificadas.

Toda excepción deberá ser solicitada formalmente por el encargado o responsable del proceso o sistema afectado, a través del director del área respectiva, indicando su alcance, riesgos asociados y un plazo máximo de vigencia. Dicha solicitud será evaluada y aprobada o rechazada por el Director de Tecnología y Datos, quien podrá definir un plazo máximo de vigencia distinto del solicitado, de estimarse necesario para la mitigación del riesgo asociado Las excepciones deberán ser informadas al Comité de Gobierno de Datos, Seguridad de la Información y Ciberseguridad.

Las excepciones autorizadas deberán ser registradas y monitoreadas mientras se encuentren vigentes, y no constituirán precedente para futuros casos.

Capítulo V: Del Cumplimiento, Calidad y Seguridad

13. ESTÁNDARES DE CALIDAD

La Oficina de Gobierno de Datos definirá métricas de calidad de datos que servirán de marco de acción para todos los proyectos tecnológicos, que creen, modifiquen, integren o consuman datos del Administrador. Su cumplimiento deberá ser validado previamente por la Oficina de Gobierno de Datos.

El seguimiento a la implementación de Calidad en los distintos proyectos tecnológicos del Administrador se realizará en el Comité de Gobierno de Datos, Seguridad de la Información y Ciberseguridad.

14. SEGURIDAD Y PRIVACIDAD

El Gobierno de Datos actuará de forma coordinada con los equipos del Administrador basándose en la Ley N° 19.628, sobre Protección de la Vida Privada, la Ley N° 21.735 y Ley N° 20.285, de Acceso a la Información Pública, y aplicando estrictamente la Política de Tratamiento y Uso de Información Reservada para la protección de los activos críticos y datos sensibles y Política de Seguridad de la Información y Ciberseguridad, según corresponda.

El acceso a los datos se regirá bajo el principio de menor privilegio, permitiendo el acceso solo a la información estrictamente necesaria para la función desempeñada. Para ello, se implementarán, al menos, las siguientes medidas técnicas:

- **Control de acceso:** Basado en el principio de "Menor Privilegio" Los accesos se otorgan según el rol y requieren aprobación del Data Owner.
- **Anonimización:** Los datos utilizados en ambientes de desarrollo o pruebas (No-Productivos) deben ser anonimizados, seudonimizados o enmascarados obligatoriamente.
- **Seguridad en la adquisición y desarrollo:** Todo nuevo proyecto tecnológico, ya sea desarrollo interno o adquisición de software de terceros, deberá someterse a una evaluación de cumplimiento de estándares de datos y seguridad antes de su contratación o paso a producción. No se autorizará la puesta en marcha de sistemas que no hayan sido sometidos a evaluación de estándares.

Para garantizar la adherencia a estos lineamientos, se han establecido protocolos de gestión que norman las medidas técnicas y operativas, especificando estrictamente los perfiles autorizados, los plazos de acceso y la matriz de responsabilidades correspondiente.

Capítulo VI: De las Infracciones y Sanciones

15. RESPONSABILIDAD ADMINISTRATIVA Y MEDIDAS APLICABLES

El incumplimiento de las directrices establecidas en la presente Política podrá dar lugar a la adopción de medidas y acciones disciplinarias, las que serán evaluadas por las áreas competentes del Administrador (incluyendo Recursos Humanos y la Dirección/áreas de Tecnología y Datos, según corresponda), de conformidad con la normativa aplicable —incluido lo dispuesto en el artículo 57 de la Ley N° 21.735— y con el Código de Ética Institucional, sin perjuicio de las responsabilidades civiles o penales que pudieren concurrir.

En particular, podrán constituir infracciones graves, según su naturaleza y circunstancias, entre otras, las siguientes conductas: (i) la manipulación, modificación o eliminación no autorizada de datos o metadatos; (ii) la negligencia en el resguardo de la integridad, calidad o disponibilidad de los datos bajo responsabilidad del rol correspondiente; y (iii) la vulneración o elusión de controles de acceso, el uso indebido de credenciales o el acceso a datos sin autorización o excediendo el rol asignado.

16. RESPONSABILIDAD INSTITUCIONAL COMPARTIDA

El Gobierno de Datos constituye una responsabilidad transversal del Administrador. Todas las áreas, niveles jerárquicos y roles definidos en la presente Política son responsables de incorporar sus principios y directrices en la gestión diaria de procesos, sistemas y decisiones que involucren datos, sin que dicha responsabilidad recaiga exclusivamente en la Oficina de Gobierno de Datos o en los roles técnicos asociados.

Capítulo VII: Disposiciones Finales

17. ORDEN DE PRELACIÓN NORMATIVA

En caso de contradicción entre la presente Política y los documentos internos que se desprendan de ésta (procedimientos, instructivos, estándares, guías u otros instrumentos

de carácter operativo, técnico o metodológico), prevalecerán las disposiciones de esta Política, salvo estipulación en contrario en la normativa legal y reglamentaria vigente.

Si la contradicción se produce entre políticas institucionales, la discrepancia deberá ser revisada y resuelta caso a caso por el Comité de Gobierno de Datos, Seguridad de la Información y Ciberseguridad, conforme al procedimiento que éste determine. Cuando ello además represente un riesgo para el Administrador, o se refiera a discrepancias con materias que excedan el ámbito de competencia del referido Comité, el asunto deberá ser escalado al Comité Ejecutivo Integral de Riesgo, y al Consejo a través de su Comité de Auditoría, Riesgos y Cumplimiento si no hubiere sido resuelto en las instancias anteriores.

18. REVISIÓN Y ACTUALIZACIÓN

La presente Política será revisada y actualizada al menos una vez al año por la Dirección de Tecnología y Datos o antes de este plazo a solicitud de Consejo Directivo, o el Comité de Gobierno de Datos, Seguridad de la Información y Ciberseguridad. Cualquier modificación deberá aprobarse por el mismo mecanismo aplicable a su versión inicial y quedar respaldada en el acto administrativo correspondiente.

Sin perjuicio de lo anterior, el Administrador podrá introducir ajustes a esta Política cuando resulte necesario para dar cumplimiento a exigencias legales o regulatorias, especialmente en materia previsional o de datos, o para reforzar la seguridad de los datos, debiendo en todo caso seguirse el proceso de aprobación y formalización señalado precedentemente.

19. DIFUSIÓN

La presente Política debe estar disponible para todo el personal del Administrador y para los terceros que presten servicios y tengan acceso a recursos tecnológicos o información institucional. Su difusión se realizará mediante los canales oficiales definidos por el Administrador, garantizando su accesibilidad y comprensión.

La Gerencia de Datos y Analítica será responsable de coordinar la difusión de esta Política con el área encargada de las comunicaciones internas.

20. VIGENCIA

Esta Política entrará en vigencia a partir de su aprobación por el Consejo Directivo del Administrador del Fondo Autónomo de Protección Previsional, sin necesidad de esperar la total tramitación del acto administrativo respectivo.

Disposiciones Transitorias

a) Implementación progresiva del modelo

La presente Política establece el estándar objetivo y permanente para la gestión de datos en el Administrador. No obstante, reconociendo la etapa de instalación institucional, la operacionalización de los roles, artefactos y controles específicos de Gobierno de Datos se realizará de manera progresiva, conforme a los planes de implementación de Gobierno de Datos que deberán ser aprobados en instancias del Comité Ejecutivo de Gobierno de Datos, Seguridad de la Información y Ciberseguridad.

b) Priorización y alcance inicial

Durante el periodo transitorio, la aplicación de controles exhaustivos se focalizará prioritariamente en los dominios de datos críticos, confidenciales y regulatorios. Los activos de datos restantes se incorporarán al modelo de gobierno según el cronograma establecido en el Plan de Implementación, sin que esto implique una exención de las normas generales de seguridad de la información.

c) Exigibilidad a terceros y proveedores de servicios

La gradualidad interna descrita en este capítulo no aplica a proveedores ni terceros. Los prestadores de servicios deberán dar cumplimiento íntegro e inmediato a los estándares de protección de datos, seguridad y confidencialidad establecidos en sus respectivos contratos y acuerdos de nivel de servicio, independientemente del nivel de madurez interno del Gobierno de Datos del Fondo.

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	30 Enero 2026

Anexo 1: Glosario y Conceptos Clave

- **Anonimizar:** Aplicar un tratamiento sobre un dato específico que pertenezca a una persona (ejemplo: salario) para que ya no se pueda ser vinculado a ella. Es un proceso irreversible.
- **Catálogo de datos:** Es el inventario inteligente y organizado de todos los activos de información de una organización. Es la herramienta central que permite saber qué datos tienes, dónde están, qué significan y quién es responsable de ellos.
- **Cifrado de datos:** Proceso de transformación de la información mediante algoritmos criptográficos con el fin de hacerla ininteligible para terceros no autorizados, garantizando su confidencialidad. Es un proceso reversible únicamente para quien posea la clave de descifrado correspondiente.
- ***Data Lake:*** Arquitectura de datos unificada que almacena información de múltiples fuentes en su formato original, sin necesidad de estructurarla previamente. Abarca desde bases de datos tradicionales hasta archivos no estructurados.
- ***Data Warehouse*:** Arquitectura de almacenamiento que consolida datos estructurados, integrados y depurados provenientes de diversas fuentes. A diferencia del *Data Lake*, aquí la información se almacena procesada bajo un modelo definido, estando optimizada específicamente para el análisis histórico, la generación de reportes y la explotación.
- **Data Lakehouse:** Arquitectura de datos que combina un *Data Lake* y un *Data Warehouse* permitiendo un almacenamiento para grandes volúmenes de datos del *Data Lake* con capacidades de gestión, calidad y rendimiento transaccional propias del *Data Warehouse*, permitiendo realizar explotación analítica, inteligencia de negocios y ciencia de datos.
- **Diccionario de datos:** Documento técnico que define la estructura, el significado y las restricciones de cada campo en una base de datos. Incluye información como nombres de columnas, descripciones, formatos, valores, entre otros.
- **Dominio de datos:** Conjunto de datos agrupados por su naturaleza o función de que requieren una gestión unificada. Se definen para asignar responsables y garantizar que su procesamiento, calidad y consumo cumplan con los estándares institucionales.
- **Enmascarar:** Tratamiento sobre un dato manteniendo una estructura similar, pero ocultando algunos de sus elementos. Ejemplo: mostrar los números de una tarjeta de crédito como: XXXX-XXXX-XXXX-1234.

- **Información reservada:** Información crítica que, por disposición legal, está sujeta a restricciones de acceso y divulgación. Debe ser tratada bajo los máximos estándares de seguridad y ciberseguridad del Administrador para prevenir riesgos, daño reputacional o incumplimiento normativo.
- **Ingesta:** Es el proceso de recopilar, importar y trasladar datos sin procesar desde diversas fuentes hacia un destino centralizado como un *Data Lake*, *Warehouse* o base de datos para su almacenamiento y análisis.
- **Principio de menor privilegio:** Práctica de seguridad de la información que establece que cualquier usuario, aplicación o sistema solo debe tener los permisos y accesos estrictamente necesarios para realizar sus funciones.
- **Registro de actividades de tratamiento de datos personales (RAT):** Registro detallado y actualizado que documenta el flujo de los datos personales en la organización. Especifica la naturaleza de los datos recolectados, la finalidad lícita de su uso, los destinatarios y los controles de seguridad implementados para su resguardo.
- **Seudonimizar:** La seudonimización es una técnica de protección y privacidad de datos que reemplaza los identificadores directos (como el RUT) por un seudónimo o código (como un código numérico o alias) para que los datos no puedan atribuirse a una persona sin información adicional, la cual se almacena por separado y con medidas de seguridad, siendo un proceso reversible y clave para el cumplimiento de normativas.
- **Repositorio institucional del Administrador:** Almacén de información del Administrador que agrupa datos estructurados y no estructurados provenientes de distintas fuentes o generados por el mismo Administrador, organizados en dominios de datos y resguardado con los más altos estándares de seguridad para ser explotados por la institución.