Enero 2026

Política **General de Seguridad de la Información y Ciberseguridad**

FONDO AUTÓNOMO
PROTECCIÓN PREVISIONAL

ÍNDICE

Nombre del Documento:	Política General de Seguridad de la Información y Ciberseguridad
Versión:	1.0
Fecha de Aprobación:	Enero 2026
Órgano de Aprobación:	Consejo del Fondo Autónomo de Protección Previsional
Próxima Revisión:	Diciembre 2026
Responsable:	Dirección de Tecnología y Datos

N° de versión	Principales cambios	Responsable	Instancia de aprobación	Fecha
1	Primera Versión	Matías Morales Director de Tecnología y Datos	Consejo Directivo	

Política General de Seguridad de la Información y Ciberseguridad del Administrador del Fondo Autónomo de Protección Previsional

1. 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, velando en todo momento por su sostenibilidad financiera a través de generaciones.

La información que genera, gestiona y resguarda el Administrador constituye un activo estratégico esencial para la operación institucional y el cumplimiento de su mandato legal y funciones principales. Entre estas funciones se incluyen el correcto financiamiento de los beneficios del Seguro Social Previsional, la eficiente administración de los procesos vinculados, la gestión e inversión de los recursos del Fondo y el análisis y realización de estudios técnicos y actuariales para velar por su sustentabilidad financiera a lo largo del tiempo. Asimismo, el Administrador debe asegurar la entrega de información correspondiente a los cotizantes y beneficiarios del Seguro Social Previsional, así como el cumplimiento de las obligaciones contractuales y regulatorias vigentes. En este contexto, la protección de la información y la gestión de la ciberseguridad son pilares fundamentales para resguardar la continuidad operativa, la resiliencia institucional, la confianza pública y el cumplimiento normativo.

En coherencia con la Política de Tratamiento y Uso de Información Reservada, las finalidades del tratamiento de información por parte del Administrador se orientan a permitir el adecuado cumplimiento de sus funciones, particularmente en lo relativo al financiamiento de los beneficios, la administración de los procesos asociados, la gestión de los recursos del Fondo y la realización de análisis técnicos y actuariales. Asimismo, incluyen la entrega de información a cotizantes y beneficiarios del Seguro Social Previsional y el cumplimiento de obligaciones contractuales y regulatorias.

Para ello, el Administrador se compromete a establecer, implementar y mantener un Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI/SGSC) conforme a la norma NCh-ISO/IEC 27001:2023, a la ISO/IEC 27002:2022 y a la normativa sectorial aplicable, asegurando niveles adecuados de confidencialidad, integridad, disponibilidad,

autenticidad, privacidad y auditabilidad. Asimismo, el Administrador ha incorporado estándares de la Ley N° 21.663 (Ley Marco de Ciberseguridad), alineando esta Política General de Seguridad de la Información y Ciberseguridad (en adelante, la "Política") con las obligaciones aplicables a Prestadores de Servicios Esenciales (PSE) y, como buena práctica, ha incorporado ciertas exigencias aplicables a los Operadores de Importancia Vital (OIV).

2. COMPROMISO INSTITUCIONAL

El Consejo Directivo es la autoridad responsable de aprobar esta Política, el apetito y los niveles de aceptación de riesgo en materia de seguridad de la información y ciberseguridad, así como de revisar periódicamente su eficacia y adecuación.

Corresponde a la Dirección Ejecutiva implementar esta Política y adoptar las medidas necesarias, asegurar la disponibilidad de recursos requeridos para garantizar su cumplimiento, y dictar, coordinar y actualizar las normas, procedimientos y estándares derivados de esta Política.

En ese marco, la Dirección Ejecutiva y las direcciones técnicas se comprometen a fortalecer la gobernanza de seguridad de la información y ciberseguridad, otorgándole independencia funcional y asegurando su adecuada articulación con las instancias de coordinación institucional. Asimismo, cuando corresponda o sea requerido, deberán participar en los comités pertinentes en la materia, asegurar la emisión, actualización y cumplimiento de las normas, procedimientos y estándares que deriven de esta Política, y garantizar el cumplimiento de la legislación y normativa aplicable.

Finalmente, se promoverá la mejora continua del SGSI/SGSC mediante auditorías, revisiones periódicas y métricas de desempeño/efectividad, disponiendo acciones correctivas y preventivas cuando corresponda, en coherencia con la gestión basada en riesgos definida por el Administrador.

Capítulo I. Disposiciones Generales

3. ÁMBITO DE APLICACIÓN Y ALCANCE

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, diseñen, desarrollen, operen, administren, accedan, traten, resguarden, transmitan o gestionen información, datos u otros activos de información y/o activos tecnológicos 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 o traten datos u otros activos digitales bajo responsabilidad del Administrador, incluidos —de manera enunciativa y no taxativa.
- Prestadores de servicios a honorarios, asesores, consultores y auditores externos.
- 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, según los protocolos de intercambio seguro definidos por el Administrador.

Asimismo, esta Política es aplicable a todos los activos de información del Administrador, así como a sus redes y sistemas informáticos, incluyendo procesos, activos físicos y digitales, infraestructuras tecnológicas y servicios que soportan la operación institucional, independientemente de su ubicación o medio de procesamiento, transmisión o respaldo.

4. OBJETIVO

El objetivo de esta Política es establecer el marco rector para la protección y gobernanza de los activos de información del Administrador y el adecuado manejo del ciclo de vida de la información, asegurando la gestión sistemática y proactiva de los riesgos que puedan afectar su confidencialidad, integridad, disponibilidad, autenticidad, privacidad y auditabilidad de

aquellos, así como para resguardar la resiliencia de las redes y sistemas informáticos que utiliza el Administrador.

Este objetivo se cumple mediante la implementación de controles, procesos y responsabilidades definidos en el Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI/SGSC), garantizando la alineación con los objetivos estratégicos institucionales, el cumplimiento normativo y regulatorio aplicable, y la adopción de principios de mejora continua para fortalecer la resiliencia frente a amenazas internas y externas.

El SGSI/SGSC y los controles que de él se desprenden tendrán carácter obligatorio y vinculante para todos los procesos, proyectos, sistemas y servicios del Administrador, debiendo ser incorporados de manera transversal en la operación institucional y en la toma de decisiones.

5. MARCO NORMATIVO REFERENCIAL

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

- NCh-ISO/IEC 27001:2023 – Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestión de la seguridad de la información - Requisitos.
- ISO/IEC 27002:2022 – Seguridad de información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información.
- Ley N° 21.663 – Ley Marco de Ciberseguridad.
- Ley N° 19.628 sobre Protección de la Vida Privada, en lo que resulte aplicable, y de la nueva 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 la modifica y entra en vigencia en diciembre de 2026.
- Normativa sectorial de la Superintendencia de Pensiones (Libro V, Título XVIII).
- Instrucciones de la Agencia Nacional de Ciberseguridad, si las hubiere.

Esta Política forma parte del SGSI/SGSC del Administrador y se complementa con políticas específicas, procedimientos y estándares. Todas las directrices son coherentes entre sí y se aplican bajo principios de mejora continua y cumplimiento regulatorio.

En caso de contradicción entre esta Política y una norma legal obligatoria, prevalecerá este última.

6. TÉRMINOS Y DEFINICIONES

En este apartado se presentan los principales vocablos utilizados en esta Política y que facilitan su comprensión por parte del personal del Administrador:

- **Activo de información:** Corresponde a todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información con valor estratégico para el Administrador. Incluye:
    - Información y datos en cualquiera de sus formatos (papel, digital, imagen, audio, video, texto, transmisión verbal).
    - Activos asociados que permiten su uso, tales como software, aplicaciones, bases de datos, hardware, redes, infraestructura tecnológica, documentación, modelos, algoritmos, propiedad intelectual, configuraciones y servicios tecnológicos.

De acuerdo con la Ley 21.663 (Ley Marco de Ciberseguridad), todos estos elementos se consideran activos de información en la medida en que su uso o protección impacte la seguridad o continuidad del servicio.

- **Auditabilidad:** Corresponde a un atributo de la seguridad de la información que permite identificar el origen y seguir el rastro de las transacciones realizadas en los activos de información.
- **Autenticidad:** Corresponde a un atributo de la seguridad de la información que permite demostrar la identidad de su emisor, certificando que los datos, o la información, provienen realmente de la fuente que señala.
- **Ciberataque:** Intento de destruir, exponer, alterar, deshabilitar, o exfiltrar u obtener acceso o hacer uso no autorizado de un activo informático.
- **Ciberseguridad:** Corresponde al conjunto de acciones para la prevención, mitigación, investigación y manejo de las amenazas e incidentes de ciberseguridad, así como para la reducción de los efectos de estos y del daño causado antes, durante y después de su ocurrencia.
- **Confidencialidad:** Corresponde a un atributo de la seguridad de la información que busca que la información sea revelada solamente a individuos, entidades o procesos autorizados. Implica preservar autorizaciones restringidas sobre acceso a

información y su desclasificación, incluyendo la protección de la información personal y la propiedad de la Información.

- **Datos personales:** Corresponde a cualquier información vinculada o referida a una persona natural identificada o identificable.
- **Disponibilidad:** Corresponde a un atributo de la seguridad de la información que busca que la información se encuentre accesible y utilizable de forma oportuna y confiable cuando sea requerida por una entidad, usuario o proceso autorizado.
- **IDS (Sistema de Detección de Intrusiones):** Corresponde a un sistema que detecta y alerta sobre actividades anómalas o maliciosas en la red o en los sistemas, sin bloquearlas.
- **Incidente:** Corresponde a todo evento que perjudique o comprometa la confidencialidad, integridad o autenticidad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos.
- **Integridad:** Corresponde a un atributo de la seguridad de la información que busca proteger la exactitud y estado completo (completitud) de la información, de manera tal que esta no sea alterada, modificada o destruida sin autorización.
- **IPS (Sistema de Prevención de Intrusiones):** Corresponde a un sistema que detecta y bloquea automáticamente actividades maliciosas para evitar que afecten los activos de información.
- **MFA (Autenticación Multifactor):** Corresponde a un mecanismo de autenticación que requiere dos o más factores independientes (contraseña, token, biometría) para validar la identidad de un usuario.
- **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.
- **Privacidad:** Corresponde a un atributo de la seguridad de la información que busca proteger aquellos datos personales que por normativa legal no deben ser divulgados a terceros.
- **Red y sistema informático:** Conjunto de dispositivos, cables, enlaces, enrutadores u otros equipos de comunicaciones o sistemas que almacenen, procesen o transmitan datos digitales.
- **Resiliencia:** Corresponde a la capacidad de las redes y sistemas informáticos para seguir operando luego de un incidente de ciberseguridad, aunque sea en un estado degradado, debilitado o segmentado, y la capacidad de las redes y sistemas informáticos para recuperar sus funciones después de un incidente de ciberseguridad.

- **Riesgo:** Corresponde a la estimación del grado de exposición de que una amenaza se materialice sobre uno o más activos de información causando daños o perjuicios al Administrador.
- **Seguridad de la Información:** Corresponde a la preservación de los atributos de confidencialidad, disponibilidad e integridad de la información contenida en un activo y de otros atributos como la autenticidad, trazabilidad y privacidad.
- **Titular de datos o titular:** Persona natural, identificada o identificable, a quien conciernen o se refieren los datos personales.

Capítulo II: De los Principios y los Roles Involucrados

7. PRINCIPIOS DE SISTEMA DE GESTIÓN DE SEGURIDAD Y CIBERSEGURIDAD

Atendiendo a los objetivos establecidos en esta Política, el tratamiento de los activos de información utilizados en los procesos del Administrador debe ser estructurado, seguro y coherente durante todo su ciclo de vida, evitando que cualquier vulneración comprometa la confianza institucional, la transparencia hacia la ciudadanía y el cumplimiento normativo.

Para ello, el Administrador deberá implementar y mantener un Sistema de Gestión de Seguridad y Ciberseguridad (SGSI/SGSC) conforme a las mejores prácticas internacionales y a la normativa aplicable (NCh-ISO/IEC 27001:2023), asegurando el cumplimiento de los siguientes principios y los controles aplicables a cada caso:

- **Seguridad y privacidad desde el diseño y por defecto:** Integrar controles de seguridad y protección de datos desde etapas tempranas de procesos y proyectos, aplicando el principio de minimización de datos personales.
    - Controles asociados: evaluación de impacto en protección de datos personales, cifrado por defecto, autenticación robusta, segregación de ambientes (Anexo A de la ISO/IEC 27001:2022 – A.5.8 Seguridad de la información en la gestión de proyectos; A.5.12 Clasificación de la información; A.5.13 Etiquetado de la información; A.5.34 Privacidad y protección de información personal (PII)).
- **Proporcionalidad y defensa en profundidad:** Aplicar controles adecuados al nivel de riesgo y múltiples capas de protección para reducir la probabilidad e impacto de incidentes.
    - Controles asociados: firewall, IDS/IPS, segmentación de redes, autenticación multifactor (MFA), monitoreo continuo (Anexo A – A.8.20 Seguridad de

redes; A.8.21 Segmentación de redes; A.8.22 Control de tráfico; A.5.16 Gestión de identidad; A.5.17 Información de autenticación; A.8.16 Monitoreo de actividades).

- **Responsabilidad compartida:** Establecer claramente obligaciones entre Administrador y sus proveedores bajo el modelo de responsabilidad compartida, especialmente en servicios de nube, de manera coherente con las políticas de Tecnología de la Información, de Gestión y Gobierno de Datos y de Tratamiento y Uso de Información Reservada. Asimismo, el Administrador gestionará a las terceras partes (personas y empresas) que tengan acceso a su información, estableciendo mecanismos de control y altos estándares de seguridad, proporcionalmente al nivel de sensibilidad de la información involucrada
    - Controles asociados: cláusulas contractuales (tales como cláusulas de confidencialidad y seguridad de la información, incluyendo obligación de reporte de incidentes, y cláusulas de seguridad específicas en materia de acceso y uso de datos personales), evidencias de cumplimiento, auditorías externas (Anexo A – A.5.19 Seguridad de la información en relaciones con proveedores; A.5.20 Seguridad en acuerdos con proveedores; A.5.21 Gestión de seguridad en la cadena TIC; A.5.22 Monitoreo, revisión y gestión de cambios en servicios de proveedores; A.5.23 Seguridad para uso de servicios en la nube).
- **Cadena de suministro y operación segura**: Exigir que los proveedores, contratistas y terceros que participen en la cadena de suministro y operación del Administrador, especialmente, que implementen controles de seguridad equivalentes a los definidos por el Administrador, asegurando la protección de la información a lo largo de toda la cadena operativa.
    - Controles asociados: cláusulas contractuales, gestión de accesos, protección y cifrado de la información, monitoreo y reporte de incidentes, cumplimiento normativo aplicable (por ejemplo, NCh-ISO/IEC 27001, Ley N° 21.663 y normativa de la Superintendencia de Pensiones), verificación mediante evidencias operativas y auditorías (Anexo A – A.5.19 Seguridad de la información en relaciones con proveedores; A.5.21 Gestión de seguridad en la cadena TIC; A.5.22 Monitoreo, revisión y gestión de cambios en servicios de proveedores).
- **Gestión integral de incidentes:** Establecer un proceso sistemático y oportuno de gestión de incidentes de seguridad de la información y ciberseguridad, que incluya detección, análisis, contención, erradicación, recuperación y aprendizaje continuo, basado en el análisis de riesgos y orientado a evitar recurrencias. En incidentes de

alto impacto que generen disrupción en procesos o afecten información crítica del Administrador, se activará la gestión de crisis como mecanismo institucional de toma de decisiones. Se prohíben las prácticas de contrataque informático (hack-back), priorizando medidas proporcionales de contención y remediación.

  - Controles asociados: plan de respuesta a incidentes, pruebas periódicas, comunicación segura con autoridades (Anexo A – A.5.24 Planificación y preparación para la gestión de incidentes; A.5.25 Evaluación y decisión sobre eventos de seguridad; A.5.26 Respuesta a incidentes de seguridad; A.5.27 Aprendizaje a partir de incidentes de seguridad).

- **Registro y auditabilidad:** Mantener trazabilidad de eventos y cambios relevantes para asegurar la rendición de cuentas y la detección temprana de anomalías.
  - Controles asociados: *logging* centralizado, retención segura de registros, monitoreo SIEM (Anexo A – A.8.15 Registro de eventos (Logging); A.8.16 Monitoreo de actividades; A.5.33 Protección de registros).
- **Actualización y mejora continua:** Mantener inventarios y clasificaciones de activos, y revisar periódicamente los controles conforme a riesgos y cambios regulatorios.
  - Controles asociados: revisiones anuales, auditorías internas/externas, actualización de políticas (Anexo A – A.5.9 Inventario de información y activos asociados; A.5.12 Clasificación de la información; A.5.13 Etiquetado de la información; A.5.35 Revisión independiente de la seguridad de la información; A.5.36 Cumplimiento con políticas, reglas y estándares de seguridad).
- **Inteligencia de amenazas:** Incorporar información externa e interna sobre amenazas para sustentar decisiones de riesgo y priorizar acciones de mitigación.
  - Controles asociados: suscripción a fuentes de threat intelligence, integración con análisis de riesgos (Anexo A – A.5.7 Inteligencia de Amenazas).
- **Seguridad en la cadena operativa:** Los proveedores deberán implementar controles de seguridad equivalentes a los establecidos en el Administrador, incluyendo gestión de accesos, protección de datos, monitoreo de incidentes y cumplimiento normativo aplicable (p. ej., NCh-ISO/IEC 27001, Ley 21.663, normativa SP). Estos requisitos se formalizarán en los contratos y se verificarán mediante evidencias operativas, como “Cuestionario Due Dilligence” y auditorías internas o independientes.
  - Controles asociados: gestión de accesos, cifrado de datos, monitoreo de incidentes, verificación contractual y auditorías (Anexo A – A.5.19 Seguridad de la información en relaciones con proveedores; A.5.20 Seguridad en

acuerdos con proveedores; A.5.22 Monitoreo, revisión y gestión de cambios en servicios de proveedores).

- **Seguridad de las comunicaciones:** Proteger la información durante su transmisión interna y externa, asegurando la confidencialidad, integridad y disponibilidad de los canales de comunicación utilizados por el Administrador, incluyendo redes, integraciones, interoperabilidad y mecanismos de intercambio seguro de datos.
    - Controles asociados: cifrado de comunicaciones, redes seguras, segmentación de redes, control de tráfico, autenticación robusta (Anexo A – A.8.20 Seguridad de redes; A.8.21 Segmentación de redes; A.8.22 Control de tráfico; A.5.17 Información de autenticación; A.5.34 Privacidad y protección de información personal).
- **Continuidad y resiliencia operativa:** Mantener capacidades que permitan la preparación, respuesta y recuperación ante interrupciones o disrupciones que afecten procesos, información o sistemas del Administrador, activando los mecanismos de continuidad operacional y de gestión de crisis cuando corresponda.
    - Controles asociados: planes de continuidad, estrategias de recuperación, pruebas periódicas, respaldos, redundancias críticas (Anexo A – A.5.29 Preparación para continuidad de la seguridad; A.5.30 Recuperación ante desastres; A.8.13 Copias de respaldo; A.5.31 Continuidad de la seguridad de la información).
- **Cumplimiento normativo y obligaciones internas:** Asegurar que la gestión de la seguridad de la información y la ciberseguridad cumpla íntegramente con la normativa legal y reglamentaria aplicable, así como con las políticas, normas, estándares y lineamientos internos del Administrador, durante todas las etapas del ciclo de vida de la información.
    - Controles asociados: revisiones y auditorías internas/externas, monitoreo regulatorio, verificación del cumplimiento, actualización normativa (Anexo A – A.5.35 Revisión independiente de la seguridad de la información; A.5.36 Cumplimiento con políticas, normas y estándares; A.5.33 Protección de registros; A.8.16 Monitoreo de actividades).

8. ROLES Y RESPONSABILIDADES

8.1. Responsabilidad Institucional Compartida

La seguridad de la información y la ciberseguridad constituyen una responsabilidad transversal del Administrador y se integran en todos los niveles de la organización. Cada rol deberá cumplir las funciones específicas establecidas en esta Política, en coherencia con las

responsabilidades definidas en el apartado de Compromiso Institucional y con lo dispuesto en las demás políticas del Administrador.

8.2. Consejo Directivo

Es responsabilidad del Consejo Directivo aprobar esta Política y sus actualizaciones, así como el apetito de riesgo y los niveles de aceptación de riesgo en materia de seguridad de la información y ciberseguridad. Será también responsable de revisar periódicamente su efectividad.

8.3. Director Ejecutivo

El Director Ejecutivo es la autoridad responsable de liderar y sostener un ambiente de control institucional en materia de seguridad de la información, ciberseguridad y gestión de datos. Para ello, ejerce la presidencia del Comité Ejecutivo de Gobierno de Datos, Seguridad de la Información y Ciberseguridad, órgano único y transversal encargado de la dirección estratégica, priorización y resolución en estas materias. En su calidad de presidente, el Director Ejecutivo actuará con la orientación de los mismos miembros del Comité Ejecutivo de Gobierno de Datos, Seguridad de la Información y Ciberseguridad, y deberá asegurar la disponibilidad de los recursos necesarios para la implementación y mejora continua del SGSI/SGSC y del modelo de Gobierno de Datos.

Asimismo, le corresponde aprobar los lineamientos que se deriven de esta Política, con la orientación de los miembros del Comité de Gobierno de Datos, Seguridad de la Información y Ciberseguridad, garantizando una gestión eficaz de la protección de los activos de información del Administrador, de acuerdo con su sensibilidad y criticidad para las operaciones, y en coherencia con los atributos de confidencialidad, disponibilidad e integridad.

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

Este comité corresponde al equipo multidisciplinario del Administrador, conformado según las funciones, cargos y requisitos establecidos en su respectivo Estatuto. Dentro de sus responsabilidades se incluyen:

- Entregar una opinión especializada al Director Ejecutivo en relación con los lineamientos de políticas específicas o secuencias de actividades descritas en procedimientos de seguridad de la información y ciberseguridad.

- Supervisar la implementación de procedimientos y estándares que se desprenden de las políticas específicas de seguridad de la información y ciberseguridad.
- Proponer estrategias y soluciones específicas para la implantación de los controles necesarios para materializar las políticas de seguridad de la información y ciberseguridad establecidas.
- Evaluar la implementación del SGSI/SGSC y la debida solución de las situaciones de riesgo detectadas.

8.5. Gerencia de Tecnologías de la Información

La Gerencia de Tecnologías de la Información es responsable de:

- Garantizar la disponibilidad, integridad, resiliencia y continuidad de la infraestructura tecnológica del Administrador, asegurando que los procesos tecnológicos se encuentren alineados con los objetivos estratégicos y las normativas vigentes.
- Proveer, o solicitar oportunamente, los recursos humanos y técnicos necesarios para implementar esta Política y las políticas específicas, procedimientos y estándares de seguridad y ciberseguridad definidos por el Administrador.
- Implementar y operar los controles técnicos, soluciones tecnológicas y medidas de protección definidos en las políticas específicas, en coordinación con el Líder de Ciberseguridad, asegurando su correcta integración en los proyectos tecnológicos y en la operación diaria.
- Asegurar la operación, monitoreo, mantenimiento y continuidad de las plataformas tecnológicas, redes y sistemas informáticos del Administrador, incluyendo respaldos, parches, actualizaciones y medidas de recuperación ante fallas.

8.6. Líder de Ciberseguridad

El Líder de Ciberseguridad -dependiente de la Gerencia de Tecnologías de la Información-, es responsable de la gestión integral del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI/SGSC). Su función principal consiste en diseñar, evaluar, supervisar y mantener las políticas, arquitecturas, lineamientos y controles de seguridad y ciberseguridad que garanticen la confidencialidad, integridad y disponibilidad de los activos de información del Administrador, así como la resiliencia de sus redes y sistemas informáticos.

El Líder de Ciberseguridad ejercerá su rol en coordinación con la Gerencia de Datos y Analítica, asegurando que las medidas de protección técnica y normativa se alineen con la clasificación y gobernanza de datos definida por la organización.

Designación como Delegado de Ciberseguridad: El Líder de Ciberseguridad se desempeñará, además, como Delegado de Ciberseguridad, de acuerdo con lo establecido en la Ley Marco de Ciberseguridad. En este rol, actúa como enlace oficial entre el Administrador y la Agencia Nacional de Ciberseguridad (ANCI), cumpliendo los deberes de coordinación, reporte y gestión establecidos por la normativa vigente.

El Líder de Ciberseguridad deberá:

a) En materia de gestión interna de seguridad y ciberseguridad:

- Diseñar, implementar, evaluar y mantener las políticas, normas, procedimientos y controles de seguridad y ciberseguridad del Administrador.
- Velar por la actualización permanente de las políticas de seguridad, conforme a cambios regulatorios, tecnológicos y mejores prácticas internacionales.
- Supervisar el cumplimiento de las políticas institucionales en todos los procesos, proyectos y áreas.
- Coordinar con las demás áreas del Administrador la integración efectiva de medidas de seguridad en la operación de los servicios.
- Mantener y actualizar la arquitectura de ciberseguridad, asegurando que responda a riesgos, capacidades institucionales y requerimientos regulatorios.
- Supervisar la correcta implementación de los controles técnicos ejecutados por la Gerencia de TI.
- Gestionar el proceso institucional de riesgos de seguridad de la información y ciberseguridad, en coordinación con las áreas competentes.
- Dirigir la gestión de vulnerabilidades, su priorización, mitigación y verificación de cierre.

b) Como punto de contacto y coordinación interinstitucional:

- Actuar como enlace con organismos públicos, privados, industria y actores del ecosistema de ciberseguridad.
- Mantener informado al Administrador respecto de tendencias, amenazas, vulnerabilidades emergentes, cambios regulatorios y buenas prácticas.
- Coordinar comunicaciones internas y externas en materia de ciberseguridad, según lineamientos institucionales.

c) En gestión de incidentes y respuesta:

- Coordinar el proceso completo de gestión de incidentes: análisis, clasificación, contención, mitigación, erradicación y recuperación.
- Liderar los procesos de notificación a autoridades competentes, incluyendo la Agencia Nacional de Ciberseguridad, cuando correspondan.
- Asegurar la activación de los planes de respuesta a incidentes, continuidad operacional y recuperación ante desastres.
- Liderar el proceso de lecciones aprendidas y mejora continua derivado de incidentes.

d) Responsabilidades específicas como Delegado de Ciberseguridad según la respectiva Ley Marco:

- Actuar como interlocutor oficial ante la ANCI y demás organismos competentes.
- Asegurar el envío íntegro y oportuno de notificaciones, reportes e información requerida.
- Coordinar la implementación de las medidas obligatorias establecidas por la ley, reglamentos y normas técnicas.
- Supervisar el cumplimiento de los requisitos de gestión de riesgos, controles mínimos, auditorías y capacidades de respuesta.
- Gestionar y coordinar simulacros, pruebas y ejercicios de ciberseguridad exigidos por la autoridad.
- Verificar que el Administrador mantenga capacidades para detectar, contener, mitigar y recuperarse de incidentes relevantes.
- Mantener comunicación permanente, cuando corresponda, con el Comité Ejecutivo de Gobierno de Datos, Seguridad de la Información y Ciberseguridad, respecto del estado de cumplimiento, riesgos significativos y brechas detectadas.

8.7. Propietario de los activos de información.

Persona o rol responsable de asegurar que el activo esté identificado, clasificado, protegido, mantenido y que los accesos sean autorizados en conformidad con las políticas de seguridad de la información durante todo su ciclo de vida.

- Para activos tecnológicos e infraestructura: el propietario es el gerente o responsable del área con autoridad funcional o presupuestaria sobre el proceso de negocio que utiliza el activo.
- Para activos de información y datos: el propietario es el área dueña del proceso que genera, utiliza o mantiene la información.

- Para propiedad intelectual (documentos, algoritmos, modelos, especificaciones): el propietario es el área que desarrolla, registra o utiliza el activo.

El propietario puede delegar tareas operativas, pero no la responsabilidad.

8.8. Custodios de los activos de información

Rol asignado al personal del Administrador con funciones de custodia y manejo adecuado de los activos de información, de acuerdo con lo determinado por la Dirección de Tecnología y Datos. Al igual que el propietario de los activos de información, será responsable de mantener un registro actualizado de los activos bajo su cargo y la relación de quienes acceden a estos.

8.9. Usuarios de los activos de información

Este rol recae en el personal del Administrador y/o personal externo a la Institución que, con la autorización del propietario o custodio del activo de información, puede consultar, ingresar, modificar o eliminar la información almacenada en los sistemas informáticos, aplicativos u otros medios de almacenamiento, respecto de Activos de Información (Datos); o en el caso de Activos Tecnológicos e Infraestructura, puede acceder o utilizar el activo informático respectivo.

Todos los usuarios son responsables del uso adecuado y protección de los activos a los que acceden o utilizan, del cumplimiento de esta Política y de las políticas específicas, procedimientos y estándares de seguridad y ciberseguridad definidos por el Administrador, incluyendo el deber de reportar incidentes o sospechas de incidentes según los canales establecidos.

Capítulo III: Gestión de Activos y Clasificación de la Información

9. CLASIFICACIÓN DE LA INFORMACIÓN

El Administrador reconoce que no toda la información tiene el mismo valor ni requiere los mismos niveles de protección. Para asegurar la aplicación eficiente de controles y el cumplimiento normativo que corresponda, todos los activos de información deben ser identificados, inventariados y clasificados para contar con un debido tratamiento y protección según su nivel de sensibilidad.

La clasificación de la información y su etiquetado se realizará conforme a la Política de Gestión y Gobierno de Datos, en la cual la Oficina de Gobierno de Datos se establece como la instancia responsable de la implementación y operación del modelo de Gobierno de Datos, dirigida por el Líder de Gobierno de Datos, dependiente de la Dirección de Tecnología y Datos. Esta Oficina definirá y mantendrá los lineamientos, estándares y mecanismos de etiquetado y clasificación aplicables.

Las categorías definidas, alineadas con la Política de Tratamiento y Uso de Información Reservada, son:

- **Uso Público o Pública:** Información que no presenta restricciones para su divulgación ni requiere consideraciones especiales de seguridad y privacidad en su tratamiento. Esto incluye, sin limitarse a, información proveniente de fuentes de acceso público (p. ej., memorias anuales públicas).
- **Uso Interno o Interna:** Información operativa creada o procesada por el Administrador para la gestión administrativa y el cumplimiento de sus mandatos. Su acceso está limitado exclusivamente a funcionarios y debe mantenerse dentro del perímetro de la organización, dado que su divulgación a terceros no está autorizada.
- **Confidencial o Sensible:** Información protegida cuyo acceso se restringe a roles específicos para fines operativos. Incluye, sin limitarse a, la gestión de datos previsionales individuales (tales como cotizaciones), datos personales de contacto (PII) e informes de auditoría interna. Su divulgación no autorizada generaría incumplimiento normativo, multas y riesgo reputacional significativo.
- **Reservada o Altamente Sensible (IAS):** Activos de información críticos sujetos a reserva legal. Incluye estrategias de inversión no públicas, microdatos suministrados por otras instituciones bajo convenios de interoperabilidad, y datos personales sensibles (ej. dictámenes de invalidez/salud). Su vulneración implica un impacto severo o catastrófico, sanciones legales y la posible inhabilitación operativa. Por consiguiente, su custodia y tratamiento exigen la aplicación obligatoria de los controles de seguridad, prohibiciones y protocolos de resguardo definidos en la Política de Tratamiento y Uso de Información Reservada.

Cada categoría establece requisitos específicos de acceso, uso, almacenamiento, transmisión, respaldo y eliminación conforme a la normativa vigente y a los controles definidos en el SGSI/SGSC. La clasificación deberá ser revisada periódicamente y actualizada cuando cambie la sensibilidad del activo, su uso, o el contexto regulatorio/operacional.

Capítulo IV: Gestión de Riesgos y Excepciones

10. PROCESO DE GESTIÓN DE RIESGO

El Administrador implementará un proceso sistemático e iterativo de gestión de riesgos en Seguridad de la Información y Ciberseguridad que incluya los siguientes elementos: establecimiento del contexto, evaluación, tratamiento (reducir, compartir/transferir, aceptar o evitar), comunicación y monitoreo/revisión.

La metodología será revisada y validada por las instancias competentes definidas en los estatutos respectivos, asegurando consistencia con el Sistema de Gestión de Riesgo institucional. La aceptación de riesgos residuales relevantes deberá ser aprobada por el Comité competente conforme a dichos estatutos.

11. GESTIÓN DE CIBERATAQUES E INCIDENTES Y REPORTE OBLIGATORIO

El Administrador deberá mantener procedimientos de detección, reporte, clasificación, contención, erradicación, recuperación y aprendizaje respecto de incidentes o ciberataques que puedan afectar al Fondo o su Administrador.

Todos los sujetos obligados por esta Política deberán reportar de inmediato la ocurrencia, o sospecha, de cualquier incidente o ciberataque del que tomen conocimiento, de acuerdo con el procedimiento de gestión de incidentes y ciberataques definido por el Administrador.

Además de los incidentes y ciberataques que puedan ocurrir dentro del Administrador, deberán tomarse medidas para detectar y gestionar aquellos incidentes que puedan afectar a proveedores u otros terceros que presten servicios o trabajen para el Administrador. Estas medidas serán coordinadas y tomadas por la Dirección de Tecnología y Datos, a través del Líder de Ciberseguridad, quienes deberán activar los procesos de monitoreo, análisis y gestión definidos en el SGSI/SGSC.

Para incidentes y ciberataques con efectos significativos, el Administrador, por medio del Líder de Ciberseguridad, reportará al Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT) según los plazos y procedimientos establecidos en la Ley N° 21.663 o cualesquiera posterior que modifique o reemplace. Asimismo, se informará a la

autoridad sectorial competente, esto es, la Superintendencia de Pensiones y la Agencia Nacional de Ciberseguridad, según lo exigido por la normativa aplicable.

Con la entrada en vigencia la Ley N° 21.719, los incidentes que afecten datos personales se reportarán también a la Agencia de Protección de Datos Personales y, cuando corresponda, a los titulares de datos personales.

El aviso al Consejo Directivo se realizará a través del Director Ejecutivo, quien canalizará la comunicación mediante la Secretaría del Consejo (minuta urgente y/o citación extraordinaria), con copia al Presidente del Comité de Gobierno de Datos, Seguridad de la Información y Ciberseguridad, a fin de resguardar trazabilidad y registro institucional.

Capítulo V: Contenidos específicos del SGSI/SGSC

12. INTELIGENCIA DE AMENAZAS

El Administrador establecerá un proceso para recolectar, analizar y difundir inteligencia de amenazas interna y externa, incluyendo fuentes gubernamentales, sectoriales y comerciales, integrando los hallazgos al análisis de riesgos, gestión de vulnerabilidades y respuesta a incidentes y ciberataques.

13. SEGURIDAD *CLOUD*

Todo proyecto, adquisición o uso de servicios *Cloud* deberá alinearse obligatoriamente con los principios, controles y procesos definidos en esta Política y en el SGSI/SGSC, siendo requisito previo para su aprobación la validación de los riesgos de seguridad y ciberseguridad asociados.

14. SEGURIDAD DE DATOS PERSONALES

Este capítulo regula las obligaciones específicas en materia de protección de datos personales y constituye un apartado independiente dentro de esta Política, complementario y no subordinado al Capítulo 13 relativo a Seguridad *Cloud*.

14.1. Deberes de seguridad aplicables al tratamiento de datos personales

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

Respecto de los datos personales bajo el control del Administrador, ya sea que estén alojados en bases propias o de terceros, se implementarán y mantendrán medidas técnicas y organizativas idóneas para resguardar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de tratamiento, e impedir el tratamiento o acceso no autorizado o ilícito, así como cualquier pérdida, filtración, daño o destrucción de datos personales.

Las medidas de seguridad deberán ser apropiadas y acordes con el estado de la técnica, considerando los costos de la implementación, la naturaleza del tratamiento que se vaya a realizar (naturaleza, alcance, contexto y propósitos), la naturaleza de los datos personales, y la probabilidad de los riesgos y la gravedad de sus efectos en relación con el tipo de datos tratados. La especificación técnica y operacional se realiza conforme a los principios establecidos en el Capítulo V de esta Política y el proceso de gestión de riesgos del Ítem 10.

En conformidad con el principio de actualización y mejora continua, se establecerán procesos continuos de verificación y evaluación para asegurar la eficacia de las medidas implementadas frente a posibles incidentes.

14.2. Gestión de incidentes

Los incidentes que afecten datos personales tratados por el Administrador, en calidad de responsable de datos, se gestionarán conforme al marco de incidentes del Numeral 11 de esta Política.

Cuando la normativa de protección de datos personales así lo exija, el Administrador reportará tales incidentes a la autoridad competente y, cuando corresponda, a los titulares de datos, siguiendo los plazos y requisitos legales aplicables.

15. DOCUMENTACIÓN ESPECÍFICA DEL SGSI/SGSC

Esta política se complementa con políticas específicas, procedimientos y estándares incluyendo, entre otros, los siguientes: Gestión de Accesos; Protección de Datos Personales y *Data Loss Prevention*; Gestión de Vulnerabilidades y Parcheo; Continuidad Operativa y Recuperación ante Desastres; Teletrabajo y Dispositivos; Gestión de Riesgo de Proveedores

y Servicios Externalizados; Desarrollo Seguro; Gestión de Cambios; Seguridad de la Información en Proyectos; Gestión de Criptografía.

Capítulo VI: Disposiciones Transitorias y de Implementación Progresiva

16. ALCANCE DE ESTAS DISPOSICIONES

Las disposiciones de este capítulo tienen por finalidad permitir una implementación gradual y ordenada de la presente Política durante la etapa de instalación institucional del Administrador, sin alterar el objetivo general ni el alcance permanente de la Política.

17. GRADUALIDAD DE IMPLEMENTACIÓN DEL SGSI/SGSC

Considerando que el Administrador se encuentra en una etapa de instalación institucional y maduración progresiva de sus capacidades, la implementación de los controles, procesos y medidas definidas en la presente política y en el SGSI/SGSC se realizará de manera gradual, conforme a la priorización de riesgos, criticidad de los activos de información y capacidades organizacionales disponibles.

La inexistencia temporal de un control específico no constituirá incumplimiento de esta política, siempre que exista un plan de implementación formal, aprobado por la Dirección competente, con responsables y plazos definidos.

18. DISPOSICIONES TRANSVERSALES DEL SGSI/SGSC

18.1. Gestión de Excepciones a Controles de Seguridad

El modelo del SGSI/SGSC se basa en estándares y controles que deben aplicarse de forma consistente. No obstante, de manera excepcional, podrán autorizarse desviaciones específicas a los controles definidos en esta Política o en los documentos del SGSI/SGSC, cuando existan razones técnicas, operativas o legales debidamente justificadas.

Toda excepción deberá:

- Ser solicitada formalmente por la jefatura o responsable del activo o proceso afectado, canalizada a través del Director o Directora del área respectiva, para efectos de formalidad y trazabilidad.
- Contar con la aprobación expresa del Líder de Ciberseguridad.

- Concluir una propuesta de justificación técnica u operativa; el alcance, riesgos asociados y plazo máximo de vigencia serán definidos por el aprobador, conforme a la evaluación de riesgos y al estándar institucional.

Gobernanza y aprobación:

- La resolución de excepciones operativas o técnicas será revisada por el Comité Ejecutivo de Gobierno de Datos, Seguridad de la Información y Ciberseguridad.
- La aceptación de riesgos residuales derivados de dichas excepciones será evaluada y aprobada por el Comité Integral de Riesgos, conforme a sus atribuciones estatutarias.

Las excepciones autorizadas deberán registrarse y monitorearse mientras se encuentren vigentes, y no constituirán precedente para futuros casos.

Capítulo VII: Disposiciones Finales

19. 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/área 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 caso de que una acción, omisión o negligencia provoque daño o desperfecto en un recurso tecnológico institucional, o ante la pérdida o robo de equipos, el usuario deberá notificar a la Gerencia de Tecnología de la Información a la brevedad.

20. 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 Dirección de Tecnología y Datos será responsable de coordinar la difusión de esta Política con el área encargada de las comunicaciones internas.

Adicionalmente, el Administrador implementará un programa de capacitación anual y obligatoria para todo su personal sobre la presente Política y las políticas específicas y procedimientos vigentes en materia de Seguridad de la Información y Ciberseguridad. El programa de capacitación deberá identificar las necesidades de capacitación de cada rol. Este proceso deberá también propender a que el personal de los proveedores de servicios cuente con conocimientos básicos de seguridad de la información y ciberseguridad y deberá considerar mecanismos de evaluación de efectividad.

21. REVISIÓN Y ACTUALIZACIÓN

Esta Política será revisada y actualizada al menos una vez al año por el Consejo Directivo, o antes de este plazo a solicitud del 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.

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.

22. 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.

23. 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 Directivo, a través de su Comité de Auditoría, Riesgos y Cumplimiento, si no hubiere sido resuelto en las instancias anteriores.