Enero 2026

Política **de Tecnología de la Información**

FONDO AUTÓNOMO
PROTECCIÓN PREVISIONAL

ÍNDICE

Nombre del Documento:	Política Tecnología de la Información
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	Dirección de Tecnología y Datos	Consejo Directivo	30 enero 2026
2				

Política de Tecnología de la Información del Administrador del Fondo Autónomo de Protección Previsional

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 sustentabilidad financiera a través de generaciones.

Los activos tecnológicos y la información que el Administrador genera, gestiona y resguarda constituyen un activo estratégico esencial para la operación institucional para el cumplimiento de su mandato legal y funciones principales, incluyendo 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, entre otros.

En este contexto, las Tecnologías de la Información (TI) son un pilar fundamental para el desarrollo organizacional del Administrador, proporcionando soporte a las actividades diarias del personal del Administrador y asegurando la continuidad operativa.

Esta Política tiene por finalidad regular el uso correcto de los recursos tecnológicos y la protección de los activos tecnológicos, salvaguardando la propiedad intelectual de los desarrollos, procesos y sistemas bajo la administración de la institución. Asimismo, establece un marco normativo claro y riguroso para todos los integrantes del Administrador, garantizando la adecuada gestión de los activos tecnológicos, su correcto tratamiento y los resguardos necesarios para asegurar la continuidad de las plataformas y servicios críticos.

Capítulo I. Disposiciones Generales

1. 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 o de colaboración, desarrollen, accedan, traten o gestionen los activos y recursos tecnológicos bajo responsabilidad del Administrador, incluyendo:

- Los miembros del Consejo Directivo.
- Director Ejecutivo.
- 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 índole, desarrollen, accedan, traten con activos y/o recursos tecnológicos del Administrador, 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.

Esta Política establece directrices para el uso de activos y recursos tecnológicos de la institución, los principios que rigen la gestión de los activos tecnológicos del Administrador, su operación y utilización para el desarrollo de las actividades propias de la institución. Se aplica al uso de todos los equipos informáticos utilizados por el Administrador, así como a las infraestructuras, sistemas y servicios tecnológicos que sirvan a sus funciones, independientemente de su ubicación geográfica o del tipo de soporte.

Este alcance incluye, pero no se limita a:

- **Activos de información:** Espacios físicos o lógicos donde se alojen los datos, tales como bases de datos, expedientes digitales y físicos, propiedad intelectual y código fuente.
- **Infraestructuras:** El alcance de esta Política comprende exclusivamente la infraestructura, plataformas y servicios tecnológicos provistos por terceros bajo modelos de Computación en la Nube (*Cloud Computing*), tales como Infraestructura

como Servicio (IaaS), Plataforma como Servicio (PaaS) y Software como Servicio (SaaS), necesarios para el desarrollo de las actividades del Administrador.

En concordancia con los lineamientos estratégicos del Fondo de no mantener infraestructura de procesamiento física propia, se declara expresamente que la institución no adquiere ni administra centros de datos ni *hardware* de procesamiento *On-Premise*. En consecuencia, la gestión de *hardware* físico de servidores queda fuera del alcance de esta Política, focalizándose los controles y directrices estrictamente en la gestión, configuración, seguridad y gobierno de los recursos en la nube.

- **Dispositivos móviles y remotos:** Cualquier dispositivo que permite el acceso a datos institucionales y/o de sistemas propios del Administrador para el desarrollo de sus actividades, sin importar la ubicación del dispositivo que accede, incluyendo soluciones de acceso remoto, tales como las utilizadas para la realización de teletrabajo.

Todos los recursos tecnológicos adquiridos por el Administrador, así como los datos generados o procesados con ellos, y la información y creación intelectual desarrollada por el personal del Administrador en cumplimiento de sus labores, son de propiedad exclusiva de la institución. Esto incluye la información creada o gestionada en equipos tecnológicos no pertenecientes al Administrador por personal interno o terceros con relación contractual, y aun cuando no exista contrato suscrito a la fecha de inicio del servicio, siempre que el desarrollo haya sido encomendado por el Administrador o que dichas actividades se encuentren comprendidas dentro de sus funciones.

De conformidad con la normativa y los contratos vigentes, los recursos tecnológicos utilizados, así como la información que contienen, podrán ser objeto de inspección, monitoreo y auditoría por parte de la Gerencia de Tecnología de la Información o de la Auditoría Interna del Administrador, exclusivamente para fines de seguridad de la información, continuidad operacional y control interno.

Estas medidas se ejercerán en forma proporcional, impersonal y previamente informada, respetando en todo momento la vida privada, la honra, la dignidad y la intimidad de las personas, y se encontrarán debidamente respaldadas en los contratos de trabajo, anexos contractuales u otros instrumentos que habiliten legalmente dichas facultades, conforme a la Ley N° 19.628 y al Código del Trabajo.

2. OBJETIVO DE ESTA POLÍTICA

Establecer el marco para la protección de los activos tecnológicos, asegurando la gestión sistemática y proactiva de los recursos que puedan afectar su confidencialidad, integridad, disponibilidad, autenticidad, privacidad y auditabilidad.

Este objetivo se cumple mediante la implementación de controles, procesos y responsabilidades por la Dirección de Tecnología y Datos; en particular, a través de la Gerencia de Tecnología de la Información, garantizando la alineación con los objetivos estratégicos institucionales, el cumplimiento normativo y regulatorio aplicable, y la adopción de principios asegurando la continuidad operativa, la seguridad de la información y el cumplimiento normativo.

Capítulo II: De los Principios y los Roles Involucrados

3. PRINCIPIOS

Los siguientes principios constituyen los pilares fundamentales que rigen la gestión, operación, desarrollo y seguridad de los activos tecnológicos. Estos principios son de carácter transversal y obligatorio, debiendo ser utilizados como base para la interpretación de esta política, la resolución de situaciones no previstas explícitamente y la toma de decisiones estratégicas.

a) Principio de Seguridad Integral

La seguridad en el Administrador se fundamenta en la gestión de los activos según su clasificación, asegurando un adecuado uso y altos estándares de protección de estos, incluyendo los activos tecnológicos e infraestructura. Para ello, la protección de la información se basa en la preservación de tres dimensiones:

- **Confidencialidad**: Garantizar que la información sea accesible únicamente por las personas, procesos o sistemas debidamente autorizados.
- **Integridad:** Salvaguardar la exactitud y completitud de la información y sus métodos de procesamiento, protegiéndola contra modificaciones no autorizadas, sean estas intencionales o accidentales.
- **Disponibilidad:** Asegurar que los usuarios autorizados tengan acceso a la información y a los recursos asociados cuando lo requieran para el desempeño de sus funciones.

b) Principio de mínimo privilegio

La gestión de seguridad del Administrador regula los accesos a la información con el objetivo de asegurar la identificación, autenticación y autorización de los usuarios, de acuerdo con su clasificación y nivel de sensibilidad, y considerando estrictamente la función que cada persona desempeña. Este control se aplica de manera integral sobre los accesos físicos, lógicos y/o tecnológicos, de modo que cada usuario cuente únicamente con los permisos indispensables para ejecutar sus tareas.

En consecuencia, a todo usuario se le asignarán exclusivamente los accesos mínimos necesarios para el cumplimiento de su trabajo, otorgándose acceso a información solo dentro de los límites definidos por su categorización y restringiéndolo a quienes mantengan una necesidad de acceso legítima vinculada al desempeño de sus funciones. Dichos permisos deberán revocarse de forma inmediata cuando esa necesidad cese.

c) Principio de segregación de funciones

Para reducir el riesgo de fraude, errores operativos y conflictos de interés, las funciones críticas deben ser ejecutadas por personas distintas. Ningún usuario debe tener la capacidad de completar un proceso de negocio crítico o modificar sistemas de producción de principio a fin sin la intervención o supervisión de un control compensatorio o un segundo actor.

d) Principio de seguridad desde el diseño

La seguridad de la información no es un componente adicional, sino un requisito funcional. Todo nuevo proyecto, adquisición de *software*, desarrollo interno o cambio en la infraestructura debe contemplar controles de seguridad y privacidad de datos desde sus etapas iniciales de concepción y diseño, y no como una medida correctiva posterior a la implementación.

e) Principio de trazabilidad y responsabilidad

Toda actividad realizada en los sistemas del Administrador debe quedar registrada de forma que sea inequívocamente atribuible a una persona natural identificada o a un sistema debidamente identificado y autorizado. En consecuencia, se prohíbe el uso de cuentas genéricas o compartidas para la ejecución de acciones administrativas o cualquier operación que pueda afectar la seguridad, integridad o disponibilidad de los sistemas y de la información.

Cada usuario será responsable directo de las acciones realizadas bajo su identidad digital, debiendo resguardar adecuadamente sus credenciales y mecanismos de autenticación. Para estos efectos, los registros de auditoría (*logs*) constituirán la evidencia formal de las actividades ejecutadas, permitiendo su verificación para fines de seguridad de la información, control interno y auditoría.

f) Principio de gestión basada en riesgos

La gestión de riesgos tecnológicos se aplicará de manera transversal a los procesos de adquisición, desarrollo, operación y mantenimiento de tecnologías, con el fin de asegurar que los sistemas de información y sus activos incorporen los estándares definidos por el Administrador. En este marco, dicha gestión se orienta a resguardar permanentemente la confidencialidad, integridad y disponibilidad de la información y de los servicios tecnológicos, priorizando la asignación de recursos y controles de protección sobre aquellos activos críticos para el cumplimiento del mandato y de los objetivos estratégicos de la institución.

Asimismo, esta gestión contempla un ciclo continuo de identificación, evaluación y tratamiento de los riesgos tecnológicos, con monitoreo permanente y medidas de mitigación proporcionales a su criticidad. En consecuencia, solo se aceptarán niveles de riesgo residual que resulten coherentes con la visión de riesgo y los umbrales de tolerancia definidos por la Dirección de Tecnología y Datos del Administrador, debiendo revisarse periódicamente su vigencia y adecuación frente a cambios tecnológicos, operacionales o regulatorios.

g) Principio de legalidad y ética digital

Los recursos y activos tecnológicos son bienes institucionales destinados exclusivamente al cumplimiento de los objetivos del Administrador, debiendo ser utilizados con austeridad, eficiencia y rectitud ética.

h) Principio de Seguridad en las Comunicaciones

El Administrador garantiza la seguridad de las redes y servicios de comunicaciones para permitir un uso adecuado, integro y oportuno de la información. La transmisión de información, así como la recepción debe ser a través de canales seguros y medios de comunicación oficiales del Administrador.

4. ROLES Y RESPONSABILIDADES

La seguridad de la información y la protección de los activos tecnológicos no son responsabilidad exclusiva del área técnica, sino un compromiso transversal de toda la organización. Esta sección define los roles y responsabilidades para garantizar la gobernanza efectiva de las Tecnologías de la Información.

a) Responsabilidad Compartida

La seguridad de la información y el uso adecuado de los recursos tecnológicos constituyen una responsabilidad institucional compartida. Ningún rol, cargo o nivel jerárquico queda exento del cumplimiento de la presente Política, siendo obligación de todas las áreas del Administrador incorporar sus lineamientos en la ejecución de procesos, toma de decisiones y definición de requerimientos.

b) Gerencia de Tecnología de la Información

Como custodio técnico de los componentes tecnológicos del Administrador, la Gerencia de Tecnología de la Información será responsable de:

- **Gestión operativa:** Administrar, mantener y actualizar la infraestructura de *hardware*, *software*, redes y telecomunicaciones del Administrador, asegurando su disponibilidad y rendimiento. El mismo quedará registrado en un inventario de activos de Tecnología.
- **Implementación de controles:** Configurar y mantener los parámetros de seguridad técnica (*firewalls*, antivirus, políticas de contraseñas).
- **Gestión de accesos:** Crear, modificar o dar de baja cuentas de usuario únicamente bajo solicitud formal de jefaturas autorizadas o de Recursos Humanos.
- **Monitoreo y auditoría:** Supervisar la red y los sistemas para detectar anomalías. La Gerencia de Tecnología de la Información tiene la facultad de inspeccionar y auditar cualquier equipo o cuenta institucional ante sospechas fundadas de mal uso o requerimientos de investigación.
- **Respaldo:** Garantizar la ejecución y validación de las copias de seguridad de la información de los sistemas que sean utilizados por el Administrador.

c) Direcciones, otras gerencias y jefaturas

Los Directores de las áreas técnicas del Administrador definidos en su organigrama institucional, así como cualquier otro cargo de gerencia, subgerencia o jefatura que sea

responsable de procesos de administración y operaciones, legales y asuntos institucionales, recursos humanos, inversiones, actuarial y sostenibilidad financiera, entre otras, que interactúan con plataformas del Administrador, serán responsables de gestionar y controlar los accesos asociados a sus respectivos equipos y procesos.

En particular, deberán definir los permisos requeridos conforme a las funciones y al principio de mínimo privilegio, y solicitar formalmente las altas, modificaciones y bajas de acceso, asegurando que dichas solicitudes queden debidamente registradas y autorizadas. Asimismo, les corresponderá supervisar el cumplimiento de la presente política en su ámbito de responsabilidad, informando oportunamente a las instancias correspondientes cualquier incidente, infracción o desviación detectada, y colaborando en las acciones correctivas que se determinen.

d) Usuarios

Toda persona natural con acceso autorizado a los sistemas de información o redes del Fondo y su Administrador, incluyendo el personal contratado directamente por este y cualquier otro proveedor externo, consultor y/o visita autorizada, será responsable de:

- Cumplir estrictamente las disposiciones de esta Política.
- Proteger credenciales y evitar prácticas que comprometan la seguridad.
- Reportar de inmediato cualquier incidente, pérdida, robo o desperfecto en los recursos tecnológicos.

e) Comité de Arquitectura Tecnológica

La implementación y el cumplimiento de la presente Política serán monitoreados por el Comité de Arquitectura Tecnológica, el cual sesionará a demanda, cuando el Administrador requiera evaluar nuevos proyectos o cambios y/o mejoras vinculadas a los activos tecnológicos del Administrador, en los contextos señalados en esta Política, conforme a su reglamento interno de funcionamiento.

El Comité de Arquitectura Tecnológica reportará al Comité de Riesgos siempre y cuando la información a revisar con el Comité mencionado, sean de impacto relacionado con la seguridad, estabilidad o reputación de la institución. La estructura de decisión se menciona en el apartado “8. Desarrollo, Mantenimiento y Adquisición de *Software*”.

Capítulo III: Tipos de Activos y Conceptos

5. ACTIVOS DE INFORMACIÓN Y RECURSOS TECNOLÓGICOS

Los activos de información y recursos tecnológicos del Administrador constituyen herramientas esenciales para el desarrollo de su operación y el cumplimiento de sus funciones, conforme a su mandato. La siguiente clasificación identifica los distintos activos y recursos comprendidos en el alcance de esta Política.

- **Activo de Información:** Cualquier dato, dispositivo o sistema que tenga valor para el Fondo y/o su Administrador. Incluye no solo el *hardware* y *software*, sino también la información en sí misma (bases de datos, archivos físicos, propiedad intelectual). Los activos mencionados se encuentran comprendidos, asimismo, en el ámbito de aplicación de la Política de Seguridad de la Información y Ciberseguridad y de la Política de Tratamiento de Datos, en lo que resulte pertinente.
- **Recursos Tecnológicos:** Conjunto de elementos de *hardware*, *software*, redes y servicios contratados (Nube) destinados al procesamiento y almacenamiento de datos del Administrador.
    - *Hardware*: Son los componentes físicos tangibles de la tecnología, tales como servidores, computadores de escritorio, notebooks, teléfonos móviles, impresoras y dispositivos de red.
    - *Software*: Son los programas informáticos desarrollados por el Administrador como por empresas externas, sistemas operativos e integraciones que permiten conectarnos con el ecosistema externo al organismo.

6. CONCEPTOS DE SEGURIDAD Y RIESGO

Los conceptos fundamentales detallados a continuación constituyen la base terminológica para la comprensión de esta política. Estos se encuentran alineados y deben interpretarse en estricta concordancia con el **marco normativo institucional vigente** en materias de seguridad de la información y protección de datos, asegurando una gestión de riesgos integral y coherente.

- **Confidencialidad:** Garantía de que la información sea accesible únicamente por las personas, entidades o procesos debidamente autorizados para ello.
- **Integridad:** Salvaguarda de la exactitud y completitud de los activos de información, asegurando que no han sido modificados o manipulados sin la debida autorización.

- **Disponibilidad:** Garantía de que la información, los sistemas y los recursos asociados estén accesibles y utilizables por los usuarios autorizados en el momento que lo requieran.
- **Incidente de seguridad:** Cualquier evento adverso, confirmado o bajo sospecha, que comprometa o amenace la confidencialidad, integridad o disponibilidad de un activo de información o la continuidad operativa del Administrador (ej. infección de *malware*, acceso no autorizado, filtración de datos).
- **Vulnerabilidad:** Debilidad intrínseca en un sistema, procedimiento o control interno que podría ser explotada por una amenaza para causar daño o violar la política de seguridad.
- **Amenaza:** Causa potencial (de origen interno o externo) de un incidente no deseado, que al explotar una vulnerabilidad puede provocar daños a un sistema o a la organización.

Capítulo IV: Lineamientos de Uso de los Recursos Tecnológicos

7. DIRECTRICES DE USO DE RECURSOS TECNOLÓGICOS

a) Uso general de los Recursos Tecnológicos

Se considera "Uso Aceptable" de los recursos tecnológicos del Administrador aquel que se realice conforme a las normas establecidas en el Código de Ética Institucional, y que esté alineado estrictamente con el mandato legal, funciones y objetivos estratégicos y principios de gobernanza de la Institución.

b) Uso Permitido y Obligaciones:

- **Finalidad laboral:** Los usuarios deberán utilizar los recursos tecnológicos institucionales exclusivamente para la gestión, administración y operación de la información del Administrador orientado a la realización de alguna actividad vinculada a sus funciones.
- **Identidad y acceso:** El uso de servidores, equipos de escritorio, portátiles y sistemas debe realizarse mediante la cuenta de usuario y contraseña asignadas por la Gerencia de Tecnología de la Información. El usuario se compromete a mantener dichas credenciales como personales, únicas e intransferibles.
- **Propiedad intelectual institucional:** 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.

- **Acceso de terceros:** El acceso a la red para usuarios externos se concederá únicamente bajo las siguientes condiciones copulativas: ○ La persona debe estar debidamente identificada.
    - Debe mantener una relación contractual vigente (contrato de servicios o honorarios).
    - Debe contar con la autorización expresa de la jefatura.
- **Envíos y recepción de información:** Toda transmisión de datos se realizará de acuerdo con su nivel de sensibilidad (clasificación) y exclusivamente a través de los canales de comunicación formales definidos por el Administrador, asegurando la protección de los datos en tránsito contra intercepciones o accesos no autorizados.

c) Prohibiciones Generales

La protección de los activos del Administrador es responsabilidad de cada miembro del organismo. En consecuencia, resulta necesario establecer con claridad las prohibiciones de actuación aplicables conforme a la presente Política, en línea con lo establecido en el Código de Ética del Administrador:

- Utilizar activos o recursos tecnológicos para acciones que contravengan la legislación o normativa vigente o normativa interna del Administrador.
- Utilizar recursos tecnológicos para fines personales, aunque no conlleven beneficio personal o beneficios económicos privados.
- Compartir información que vulnere el respeto y la convivencia laboral.
- Compartir cuenta laboral con su respectiva contraseña y/o registro del factor de autenticación.
- Utilizar, intentar obtener o compartir credenciales de acceso (usuario/contraseña) de terceros.
- Obtener, transmitir o distribuir material que infrinja derechos de propiedad intelectual.
- Instalar *software* sin licencia válida o utilizar programas para evadir controles de seguridad.

- Conectar equipos personales (PCs, discos externos, impresoras) a la red corporativa sin autorización previa de TI (*Shadow IT*).
- Generar intencionalmente interrupciones o deterioro en el servicio de otros usuarios.
- Realizar cambios físicos (conexión, desconexión, reubicación) de equipos institucionales sin autorización de TI.

d) Uso de Internet

El acceso a Internet se provee exclusivamente para facilitar la búsqueda y acceso a la información, investigación, desarrollo, operaciones administrativas, accesos a las plataformas de desarrollo, mantenimiento de infraestructuras y otras tareas encomendadas por el Administrador.

e) Restricciones y prohibiciones

Proteger los activos del Administrador es responsabilidad de cada miembro. Las prohibiciones listadas están en línea con el Código de Ética del Administrador por la cual no está permitido el uso de la conexión a Internet Institucional para:

- Compartir información confidencial del Fondo y su Administrador sin autorización (fuga de datos).
- Descargar o distribuir contenido protegido por derechos de autor sin licencia.
- Utilizar herramientas de *hacking* o *software* que altere la seguridad de la red.
- Generar congestión intencional o degradación del servicio.
- Acceder a redes sociales o servicios de *streaming* (audio/video), salvo que el perfil del cargo lo requiera y esté autorizado.
- Usar *software* P2P (*Peer-to-Peer*) o *torrents* para fines no autorizados.
- Acceder a material de connotación sexual, racista, discriminatorio, violento, ilegal u ofensivo.

f) Monitoreo

El Administrador, a través de la Gerencia de Tecnología de la Información, se reserva el derecho de monitorear, controlar y fiscalizar el tráfico y acceso a Internet para garantizar la seguridad y el cumplimiento de estas directrices.

g) Uso del correo electrónico Institucional

El correo electrónico es el medio oficial de comunicación del personal del Administración y constituye una herramienta de trabajo a utilizar para el desarrollo de sus funciones. Su uso se rige por lo establecido en la Circular Nº 260/19 de la Dirección del Trabajo respecto a la facultad del empleador de regular su uso. A su vez, la información que se comparta a través de este medio se encuentra sujeta a la Política de Tratamiento de Datos, según corresponda.

Normas de administración y uso:

- **Plataforma oficial**: El único sistema autorizado es Microsoft Outlook (Office 365). Se prohíbe el uso de gestores de correo externos o no homologados.
- **Privacidad:** Sin perjuicio de que el correo electrónico institucional debe ser empleado solamente para fines laborales, el Administrador no accederá al contenido de comunicaciones de carácter personal. Cualquier acceso excepcional a información asociada al correo institucional, por motivos de seguridad, continuidad o investigación de incumplimientos, se realizará de manera limitada, proporcional y debidamente fundada, conforme a la normativa aplicable y a las disposiciones internas vigentes.
- **Identidad corporativa:** Las cuentas deben estar personalizadas y contar con la firma corporativa estandarizada por el área de Comunicaciones en el pie de página.
- **Cuentas genéricas:** Las cuentas de servicio o genéricas solo se crearán para procesos automatizados. Excepcionalmente, se asignarán a un usuario responsable a quien lo solicite previa autorización de la Gerencia de Tecnología de la Información solo por tiempo limitado y para tareas u operaciones técnicas específicas.
- **Solicitudes:** Las solicitudes de nuevas cuentas, modificaciones o eliminaciones de cuentas debe ser solicitada exclusivamente por el Líder de Infraestructura. La solicitud debe ser articulada mediante el sistema de requerimientos, adjuntando los antecedentes del funcionario, indicado en el Procedimiento de Alta, Baja y Modificación de usuarios.
- **Desvinculación:** Al finalizar la relación laboral, el área de Recursos Humanos deberá informar a la Gerencia de Tecnología de la Información para que proceda a la suspensión inmediata y automática de la cuenta de correo electrónico institucional. Dicha suspensión representa una baja “lógica” donde su acceso permanece bloqueado pero sus datos se mantendrán por el tiempo indicado en el Procedimiento de Alta, Baja y Modificación de usuarios.

- **Almacenamiento:** El correo electrónico institucional no está destinado al almacenamiento permanente de archivos. En consecuencia, el almacenamiento oficial de documentación y respaldos deberá realizarse en la plataforma Microsoft Office 365, donde OneDrive se utiliza para mantener el respaldo de la información del personal del Administrador y *Sharepoint* para documentos que son de uso colaborativo dentro de un equipo.
- **Prohibiciones específicas en correo electrónico Institucional:** Se considerará falta grave y podrá conllevar el bloqueo de la cuenta y sanciones disciplinarias:
    - Utilización de cuentas de servicio para fines distintos a los objetivos del Fondo o su Administrador.
    - Envío de correos anónimos, con remitente falso o cabeceras manipuladas (*Spoofing*).
    - Envío de correos masivos (SPAM) comerciales, cadenas, esquemas piramidales o misceláneos no solicitados.
    - Difusión de información estratégica contraria a los intereses o ética del Administrador.
    - Ataques de denegación de servicio o bombardeo de correos. ○ Suplantación de identidad de otros funcionarios. ○ Acceso no autorizado a listas de distribución globales.
    - Nota**:** El envío de correos masivos legítimos debe contar con la autorización explícita del responsable del Director del área respectiva y dar aviso a la Gerencia de Tecnología para evitar posibles restricciones técnicas de la infraestructura de correos.

h) Uso de periféricos y dispositivos

- **Autorización:** Está prohibida la conexión de periféricos (impresoras, escáneres, discos duros, etc.) que no sean propiedad del Administrador sin autorización escrita de la Gerencia de Tecnología de la Información.
- **Soporte:** La Gerencia de Tecnología de la Información no brindará soporte técnico ni asumirá responsabilidad por daños en equipos personales del usuario.
- **Responsabilidad:** El usuario es custodio de los periféricos asignados (teclados, monitores, tokens). En caso de robo o pérdida, debe dejar constancia en Carabineros y, a su vez, notificar de inmediato a la Gerencia de Tecnología de la Información. El costo de reposición podrá ser imputado al usuario si se determina negligencia.
- **Exclusividad:** Los periféricos institucionales no deben usarse para fines personales.

i) Uso y protección de la información

El manejo de la información debe ser legal, ético y seguro, y el mismo está regido por el Código de Ética del Administrador. Estas normas aplican incluso si, excepcionalmente, se autoriza el uso de equipos personales para tareas laborales.

- **Autorización de procesamiento:** Prohibido procesar o distribuir información institucional sin autorización del dueño del dato o de la Gerencia de Tecnología de la Información.
- **Fines personales:** Prohibido usar la base de datos o conocimientos del Administrador para beneficio propio o de terceros.
- **Devolución de activos:** Al cesar sus funciones, el trabajador está obligado a devolver todo equipamiento y entregar toda la información (digital o física) relacionada con su cargo inmediatamente.
- **Faltas graves:** La retención, eliminación intencional o divulgación de información confidencial u operativa sin autorización será sancionada disciplinaria y legalmente.
- **Respaldo:** Es obligación de cada usuario mantener respaldada la información crítica de su gestión en los espacios de nube asignados. No se debe almacenar información crítica localmente en el escritorio del equipo asignado.

Capítulo V: Del *Software*

8. DESARROLLO, MANTENIMIENTO Y ADQUISICIÓN DE *SOFTWARE*

a) Propiedad intelectual y titularidad

El Administrador mantiene la titularidad o los derechos de uso necesarios, así como el control sobre los activos tecnológicos que desarrolle o adquiera para el cumplimiento de su mandato, sea directamente o a través de proveedores contratados al efecto. En particular, se procurará que los desarrollos de *software* realizados para el Administrador queden debidamente regulados en cuanto a su titularidad, licencias y entregables, de modo que el Administrador cuente con los derechos y accesos necesarios para su operación, mantención y evolución, evitando dependencias indebidas de proveedores o de personal respecto del código fuente y sus componentes. Del mismo modo, las licencias de *software* adquiridas deberán contemplar condiciones que permitan su uso conforme a las necesidades del Administrador y a la normativa aplicable.

b) Titularidad de activos

Todo desarrollo de *software*, incluyendo código fuente, código objeto, *scripts*, bases de datos incluyendo sus datos, interfaces como APIs o archivos para transferencia de información y documentación asociada, generado en el marco de las funciones del Administrador o financiado por este, es propiedad exclusiva y universal del Administrador.

c) Cláusula para terceros

En caso de contratación de fábricas de *software* o desarrolladores externos, los contratos deberán estipular explícitamente la cesión total de derechos de propiedad intelectual al Administrador, entregando el código fuente sin ofuscación ni restricciones de uso. Dicho código generado por el tercero deberá siempre estar en los repositorios propios del Administrador, manteniendo y cumpliendo las normas de seguridad implementadas para dicho fin.

d) Integridad y custodia

La Gerencia de Tecnología de la Información es el responsable técnico de garantizar la integridad, el almacenamiento seguro y la sostenibilidad de estos activos digitales con el fin de preservar la integridad del funcionamiento del Administrador, así como de la continuidad operativa desde la visión de los sistemas de éste.

e) Gestión de la demanda y viabilidad

El Administrador cuenta con una planificación rigurosa respecto de los componentes y sistemas que debe implementar, desarrollar y desplegar para cumplir su mandato legal y las funciones asignadas por la Ley N° 21.735 de Reforma Previsional de 2025. En este contexto, la gestión de las capacidades técnicas necesarias para el desarrollo y/o implementación de nuevas soluciones de *software* debe planificarse adecuadamente, a fin de asegurar el cumplimiento de los compromisos definidos por la Dirección de Tecnología y Datos del Administrador y las demás áreas participantes. Por lo anterior, resulta necesario establecer un proceso claro y exigente para el análisis y determinación de la viabilidad técnica y funcional, así como de la disponibilidad de capacidades, previo a iniciar el desarrollo y/o la implementación de nuevas soluciones de *software*.

- **Solicitud formal**: Todo requerimiento de nuevo *software* o modificación evolutiva que sea detectado por parte del personal del Administrador deberá ser canalizado a través del Director el área respectiva e informado por este formalmente a la Gerencia de Tecnología de la Información.

- **Informe de factibilidad**: Una vez recibida la solicitud por parte de los requirentes, la Gerencia de Tecnología de la Información procederá a realizar un análisis detallado para comprender su factibilidad, viabilidad y prioridad. Finalizado dicho análisis, la Gerencia de Tecnología de la Información emitirá una comunicación donde expondrá los puntos evaluados:
    - Alineación arquitectónica: Se expondrán los puntos analizados y en relación con las capacidades técnicas del *software* y/o pieza a construir informando si los mismos son compatibles con el ecosistema actual o futuro del Administrador.
    - Costos recurrentes (*Total Cost of Ownership*, en adelante "TCO"): Se evaluará y se presentará una estimación de costos de licenciamiento, infraestructura, horas requeridas por los distintos especialistas siendo esto para la implementación, el desarrollo en caso de que aplique, y el costo recurrente para el mantenimiento y soportes necesarios para brindar su correcto funcionamiento dentro del ecosistema del Administrador.
    - Infraestructura: Se informará la totalidad de recursos necesarios estimados correspondientes a la infraestructura necesaria para los distintos ambientes, siendo estos para el desarrollo, aseguramiento de la calidad, ambientes productivos y de contingencia.

9. ESTÁNDARES DE INGENIERÍA DE *SOFTWARE*

La ingeniería de *software* es una práctica fundamental para el desarrollo y evolución de soluciones dentro del ecosistema tecnológico del Administrador. En su aplicación, es necesario incorporar estándares y prácticas que aseguren la calidad, seguridad, mantenibilidad y trazabilidad de los componentes implementados. Estas prácticas resultan esenciales para resguardar la continuidad operacional del Administrador y para asegurar una adecuada experiencia de usuarios en el acceso y consulta de la información.

a) Lineamientos Técnicos

Todo desarrollo deberá cumplir en forma obligatoria los estándares de arquitecturas, lenguajes permitidos y patrones de diseño para el desarrollo de *software* descritos en el repositorio interno de documentos técnicos gestionado por la Dirección de Tecnología y Datos.

b) Seguridad desde el Diseño

Los desarrollos deberán adoptar el enfoque denominado Operación Segura del Desarrollo (en adelante, "DevSecOps"). En consecuencia, será obligatorio cumplir con los siguientes controles y estándares:

- **Controles de seguridad desde el diseño:** Los desarrollos deberán implementar controles de seguridad desde la fase de diseño. El Administrador, para estos efectos, cuenta con una plataforma de control de seguridad que facilita la implementación y verificación de dichos controles.
- **Mitigación de vulnerabilidades conocidas (OWASP Top 10):** Será obligatorio identificar y mitigar las vulnerabilidades conocidas descritas en el "OWASP Top 10" (lista de los 10 riesgos de seguridad críticos para desarrollo de *software*), utilizando, cuando corresponda, las capacidades de la plataforma de control de seguridad del Administrador.
- **Prohibición de credenciales en código:** Queda estrictamente prohibido incluir contraseñas, llaves de API o secretos en el código fuente (*Hardcoding*) dentro de las piezas creadas y/o en los repositorios de *software* del Administrador. Estas deberán administrarse mediante mecanismos seguros, tales como variables de entorno o en las bóvedas de seguridad implementadas por el Administrador.

c) Uso de librerías de terceros

El uso de librerías de terceros, sean de código abierto o adquiridas por el Administrador deberá ser validado previamente por la Gerencia de Tecnología de la Información para asegurar que no contengan vulnerabilidades conocidas (CVEs) y que su tipo de licencia sea compatible con el uso institucional.

d) Gestión del código fuente o repositorios de código

Los repositorios de código fuente del Administrador son uno de los activos tecnológicos principales dentro de la institución debido que guardan el funcionamiento de todas las piezas de software escritas por los equipos técnicos. En ese sentido, es necesario cumplir con los siguientes controles:

- **Repositorio centralizado:** El código fuente debe residir obligatoriamente en el gestor de código fuente institucional del Administrador, siguiendo los lineamientos técnicos definidos en el repositorio interno de documentos técnicos de la Dirección de Tecnología y Datos.

- **Control de versiones:** Se prohíbe almacenar versiones finales o productivas en equipos locales de desarrolladores, servidores de archivos compartidos y/o repositorios públicos no autorizados (por ejemplo, cuentas personales en plataformas de control de versiones).
- **Acceso y roles:** El equipo administrador de la infraestructura del Administrador es el único autorizado para crear repositorios y asignar, modificar o revocar permisos de acceso (sean ellos de lectura y/o escritura) según el principio del mínimo privilegio. Al término de un contrato o proyecto, los accesos de desarrolladores externos deberán ser revocados inmediatamente, de conformidad con el Procedimiento de Alta, Baja y Modificación de usuarios.

e) Documentación Técnica

Toda pieza de *software* debe tener un documento relacionado en la plataforma de documentos técnicos gestionada por la Dirección de Tecnología y Datos que explique su funcionalidad. Para ello es necesario que:

- **Requisito de inicio de construcción**: Previo a la construcción de cualquier pieza de *software*, debe existir documentos relacionados con la funcionalidad, su arquitectura y como ella se integra con el ecosistema del Administrador. Sus documentos relacionados deben estar alojados en el gestor documental técnico administrado por la Dirección de Tecnología y Datos del Administrador.
- **Requisitos de entrega:** Una vez finalizada la construcción de la pieza o del *software*, ésta deberá ser entregada junto con su documentación técnica, o bien con la validación y actualización de la documentación existente, de modo de asegurar que la funcionalidad implementada se ajusta a lo definido previamente. Para estos efectos, será obligatorio cumplir con lo siguiente:
    - Manual Técnico de Despliegue: Deberán documentarse las instrucciones técnicas necesarias para la instalación, configuración y despliegue de la pieza y/o el sistema.
    - Diagrama de arquitectura**:** Al término de la construcción, se debe contar con un mapa de los componentes, bases de datos e integraciones utilizadas/desarrolladas.
    - Documentos de API: En caso de aplicar, se debe entregar la especificación técnica basada en el estándar OpenAPI 3.0 o superior, incluyendo los parámetros de entrada, métodos y respuestas de la integración.

f) Aseguramiento de calidad y paso a producción

Dentro del ciclo de vida del desarrollo de *software*, asegurar la calidad previa a desplegar las piezas en los ambientes productivos es una tarea esencial para prevenir errores y fallas que puedan afectar la operación del Administrador. Este control final busca reducir la posibilidad de impacto en los ciclos operativos del Administrador, para lo cual deberán cumplirse los siguientes lineamientos:

- **Separación de ambientes**: Se debe cumplir la estricta segregación entre los ambientes de desarrollo, certificación (o QA) y producción. Los desarrolladores no tendrán permisos de modificación ni de lectura a los datos en el ambiente productivo.
- **Pruebas obligatorias**: Antes de llevar una pieza al ambiente productivo, esta debe superar:
    - Pruebas funcionales: automatizadas o manuales según corresponda, buscando asegurar el funcionamiento de la pieza según lo previsto y documentado.
    - Pruebas de seguridad: toda pieza, previo despliegue en el ambiente productivo, deberá cumplir el estándar de seguridad de código definido en la plataforma de calidad de código y seguridad del Administrador.

g) Ventanas de mantenimiento

Los despliegues en producción pueden generar impactos en la operación, según el tipo y alcance de pieza desplegada. Por ello, en función del impacto previamente evaluado y documentado, los despliegues deberán programarse en ventanas de mantenimiento que minimicen el impacto en la operación, las que deberán ser comunicadas oportunamente al personal del Administrador. Asimismo, todo despliegue deberá contar con un plan de vuelta atrás en caso de falla.

Capítulo VI: De las Vulnerabilidades y Excepciones

10. GESTIÓN DE VULNERABILIDADES

La gestión de vulnerabilidades es el proceso continuo y sistemático orientado a identificar, evaluar, priorizar y corregir debilidades en los sistemas, aplicaciones, infraestructura y servicios de tecnológicos del Administrador, para así reducir los riesgos de seguridad y garantizar la integridad, disponibilidad y confidencialidad de la información de la institución.

Para asegurar la detección temprana y mitigación de vulnerabilidades, se deberán cumplir los siguientes lineamientos:

- **Escaneo mensual de vulnerabilidades en aplicaciones:** Se ejecutará obligatoriamente un análisis técnico automatizado, que nos permitirá ver una evaluación detallada de componentes, arquitectura y seguridad para identificar vulnerabilidades, riesgos y oportunidades de mejora.
- **Bloqueo inmediato de *software* obsoleto o sin soporte:** Se prohíbe ejecutar cualquier programa, sistema operativo o aplicación que haya alcanzado su fin de vida útil (*end of Life* - EOL) o que no reciba las actualizaciones del fabricante. La Gerencia de Tecnología de la Información estará facultada para desinstalar o bloquear técnicamente estos recursos de forma inmediata para proteger la integridad de la red. Cualquier excepción deberá estar debidamente justificada y presentada al Comité de Arquitectura Tecnológica para su aprobación.
- **Implementación de pruebas de penetración a sistemas internos:** Se realizará, al menos una vez al año, un ejercicio de pruebas de penetración (*Pentesting*) sobre la infraestructura y sistemas internos del Administrador. Estas pruebas deberán ser realizadas por especialistas de ciberseguridad, internos o externos.
- **Parcheo rápido:** Como compromiso de respuesta ágil ante vulnerabilidades de alto impacto, el Administrador mantendrá una política de “parchado rápido”, conforme a la cual toda actualización de seguridad clasificada como “crítica” o “urgente” por ciberseguridad, deberá ser probada y aplicada en todos los sistemas afectados en un plazo máximo de 72 horas tras su liberación.

11. GESTIÓN DE EXCEPCIONES

Toda excepción relacionada a los solicitudes, controles y lineamientos 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 autorizadas deberán ser registradas y monitoreadas mientras se encuentren vigentes, y no constituirán precedente para futuros casos.

Capítulo VII: Disposiciones Finales

12. 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 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.

13. 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.

14. REVISIÓN Y ACTUALIZACIÓN

La presente Política será revisada y actualizada al menos una vez al año por la Gerencia de Tecnología de la Información, o antes de este plazo a solicitud del Comité Ejecutivo Integral de Riesgos o del Comité Ejecutivo 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.

Adicionalmente, se realizarán evaluaciones independientes internas o externas para verificar su vigencia y efectividad. Esta deberá actualizarse cuando se produzcan cambios relevantes en procesos, tecnologías o normativas que afecten la seguridad de los recursos tecnológicos.

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

15. 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 Tecnología de la Información será responsable de coordinar la difusión de esta Política con el área encargada de las comunicaciones internas.

16. VIGENCIA

Esta Política entrará en vigor 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 los activos y recursos tecnológicos en el Administrador. No obstante, reconociendo la etapa de instalación institucional, la operacionalización de los activos y controles específicos se realizará de manera progresiva, conforme a los planes de implementación de la Gerencia de Tecnología que deberán ser aprobados por la Dirección de Tecnología y Datos.

b) Priorización y alcance inicial

Mientras no concluyan los planes de implementación a que se refiere el numeral anterior, la aplicación de controles exhaustivos se focalizará prioritariamente en la implementación de políticas técnicas y controles sobre los activos y recursos de usuarios finales. Los activos restantes se incorporarán al modelo de gobierno según el cronograma establecido en el plan de implementación respectivo, sin que esto implique una exención del cumplimiento 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, con independencia del nivel de implementación interna del modelo de gobierno aplicable al Administrador.

Anexo I: Términos y Definiciones

- **Nube (*Cloud Computing*):** Modelo de prestación de servicios tecnológicos a través de Internet (ej. Microsoft 365, Azure, Google Cloud), donde la infraestructura física no reside en las dependencias del Administrador.
- **VPN (*Virtual Private Network*):** Es la tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como Internet, permitiendo que el tráfico de información entre una estación de trabajo y el sistema informático esté viajando a través de un canal seguro (ej. Teletrabajo).
- **MFA (Autenticación de Multifactor):** Mecanismo de seguridad que requiere más de una forma de verificación para validar la identidad de un usuario (ej. contraseña + código en el celular).
- ***Phishing*:** Técnica de engaño (ingeniería social) que busca, a través de correos o mensajes fraudulentos, inducir al usuario a revelar información confidencial o descargar software malicioso.
- ***Ransomware*:** Tipo de *software* malicioso (*malware*) que secuestra la información cifrándola, impidiendo el acceso a los usuarios legítimos y exigiendo un pago (rescate) para su liberación.
- ***Logs* (Registros de Auditoría):** Archivos que registran cronológicamente los eventos y acciones que ocurren en un sistema informático. Los Logs pueden representar una traza en la conexión de varios sistemas, como así también el comportamiento de un usuario y/o su interacción con los sistemas del Administrador.