ACTA SESIÓN ORDINARIA N° 71 DEL CONSEJO DIRECTIVO DEL ADMINISTRADOR DEL FONDO AUTÓNOMO DE PROTECCIÓN PREVISIONAL

En Santiago, a 27 de enero de 2026, siendo las 10:30 horas, se celebró la sesión ordinaria del Consejo Directivo (en adelante, el "Consejo") del Administrador del Fondo Autónomo de Protección Previsional (en adelante, el "Fondo Autónomo"), en dependencias de su sede ubicada en Av. Libertador Bernardo O'Higgins 1449, Torre 7, oficina 81 (Santiago Downtown).

Presidió la sesión don Enrique Marshall. Participaron, además, los consejeros doña Rosario Celedón, don Rodrigo Caputo y doña Soledad Huerta.

Participaron como invitados los señores Sergio Soto, director ejecutivo; Catalina Coddou, directora Jurídica y de Asuntos Institucionales, actuando como secretaria de actas y ministra de fe; y, Diego Pérez, abogado senior de la Dirección Jurídica y de Asuntos Institucionales.

Tabla.-

1. Convocatoria y quórum para sesionar.
2. Presentación Políticas de Gestión y Gobierno de Datos, Tecnología de la Información y Seguridad de la Información y Ciberseguridad.
   2.1. Política de Gestión y Gobierno de Datos.
   2.2. Política de Tecnología de la Información.
   2.3. Política de Seguridad de la Información y Ciberseguridad.

1. Convocatoria y quórum para sesionar.-

El presidente informó del cumplimiento de todos los procedimientos previos de convocatoria para la celebración de la presente sesión.

Habiendo quórum suficiente de los consejeros, se inició la sesión.

2. Presentación Políticas de Gestión y Gobierno de Datos, Tecnología de la Información y Seguridad de la Información y Ciberseguridad.-

Para las tres presentaciones en tabla para la sesión, se invitó a participar a representantes de la Dirección de Tecnología y Datos, en particular don Felipe Marambio, gerente de Datos y Analítica; don Gastón Aprile, gerente TI; doña María José Farfán, líder de Ciberseguridad; y doña Gabriela Lazo, líder de Gobierno y Gestión de Datos, quienes presentaron al Consejo un conjunto de

políticas institucionales destinadas a fortalecer el marco de gobernanza de datos, tecnologías de la información y seguridad/ciberseguridad, para su análisis y consideración.

2.1. Política de Gestión y Gobierno de Datos. -

En primer término, se presentó la Política de Gestión y Gobierno de Datos, señalándose que el Administrador opera bajo un marco regulatorio exigente en materia de datos y tratamiento de información, y que resulta esencial contar con un modelo de gobernanza claro, con roles y responsabilidades. Se indicó como marco referencial la Ley N° 21.735, la Ley N° 19.628, la Ley N° 21.719 (con vigencia informada para diciembre de 2026) y normativa de la Superintendencia de Pensiones, señalándose además su complementariedad con la Política de Tratamiento y Uso de Información Reservada del Administrador.

Se informó que el objeto de la política es establecer principios, controles y responsabilidades para el tratamiento de datos durante todo su ciclo de vida, promoviendo estándares de integridad, calidad, trazabilidad y seguridad. Se indicó que el marco metodológico se apoya en el estándar internacional DAMA-DMBOK2, y que su implementación considera herramientas tecnológicas de apoyo y monitoreo.

Se informó, además, que se constituyó el Comité Ejecutivo de Gobierno de Datos, Seguridad de la Información y Ciberseguridad, como instancia encargada de entregar opiniones especializadas al director ejecutivo en relación con lineamientos de políticas específicas o secuencias de actividades de los procedimientos de seguridad y ciberseguridad, además de supervisar la implementación de procedimientos y estándares que provengan de la política de Seguridad de la Información y Ciberseguridad, entre otras funciones.

Debate y lineamientos del Consejo. Durante la discusión, los consejeros valoraron la propuesta considerando la oportunidad que tiene el Administrador de definir desde el comienzo esquemas de gobernanza y protocolos de actuación robustos, destacando que atendida la sensibilidad de los datos que manejará el Administrador y el carácter crítico que tienen para el adecuado cumplimiento de sus funciones, resulta del todo pertinente establecer estándares altos y exigentes para la gestión propia del Administrador y de los proveedores y terceros con los que le corresponde relacionarse. En particular, formularon observaciones orientadas a asegurar que la política distinga con claridad (i) el alcance y contenido de la política ("qué" regula), (ii) las responsabilidades y roles involucrados en su aplicación ("quiénes" ejecutan y

controlan), y (iii) los mecanismos de implementación y mejora ("cómo" se operacionaliza, mide y ajusta). Asimismo, se enfatizó la necesidad de una implementación gradual y verificable, con mecanismos de reporte y escalamiento de riesgos conforme al modelo de comités definido por el Consejo.

2.2. Política de Tecnología de la Información. -

A continuación, se presentó la Política de Tecnología de la Información, señalándose la conveniencia de contar con un marco de gobernanza que asegure una administración controlada, segura y eficiente de los activos tecnológicos del Administrador, delimitando roles y responsabilidades para el uso y gestión de dichos activos. Se indicó como marco metodológico el *framework* COBIT 2019 y como estándares complementarios ISO 27001 y normativa de la Superintendencia de Pensiones, especialmente la NCG 278, señalándose que esta política se articula con otras políticas institucionales vigentes.

Se informó que la política establece principios de uso responsable, control de accesos y gestión de activos, aplicando criterios como mínimo privilegio y segregación de funciones. Asimismo, se señaló que se implementará un modelo operativo centralizado gestionado por la Dirección de Tecnología y Datos y que se creará un Comité de Arquitectura Tecnológica para evaluar proyectos y cambios tecnológicos, considerando criterios de eficiencia, seguridad y continuidad operacional.

Los consejeros destacaron la conveniencia de que la política, además de establecer principios y reglas generales, explicite de manera ordenada la separación entre definiciones de gobernanza (roles y responsabilidades), el marco metodológico aplicable ("cómo" se gestiona y controla), y la ejecución operativa, de modo de facilitar su cumplimiento por parte de las áreas y colaboradores. Se solicitó, además, resguardar que los controles se implementen de manera progresiva y con monitoreo de su impacto operativo, de forma de fortalecer el control sin afectar la continuidad de los procesos críticos.

2.3. Política de Seguridad de la Información y Ciberseguridad. -

Finalmente, se presentó la Política de Seguridad de la Información y Ciberseguridad, señalándose que su objetivo es establecer un marco transversal para proteger información y servicios críticos, minimizando riesgos operacionales, tecnológicos y reputacionales. Se indicó como marco de

referencia la Ley N° 21.663 (Marco de Ciberseguridad), la Ley N° 19.628 y el estándar NCh-ISO/IEC 27001:2023, señalándose además que la política fue revisada por el asesor externo BITLAW.

Se informó que la política define principios, controles y responsabilidades aplicables a procesos, plataformas y servicios del Administrador, promoviendo una gestión basada en riesgos y mejora continua, y que su coordinación se articulará mediante el Comité Ejecutivo de Gobierno de Datos, Seguridad de la Información y Ciberseguridad.

Ante consultas sobre implementación por parte de los consejeros, se indicó que la adopción será gradual, proyectándose una primera etapa de controles básicos en un plazo acotado y una implementación más completa dentro de un horizonte inferior a seis meses, incorporándose además exigencias y resguardos en el relacionamiento con proveedores mediante debida diligencia y cláusulas contractuales.

En el debate, el Consejo relevó la necesidad de que la política se entienda como parte de un ecosistema normativo que se complementa con otras políticas institucionales y con instrumentos de integridad y conducta, reforzando un enfoque preventivo y coherente frente a riesgos externos. Asimismo, se solicitó que el modelo operativo, la adopción gradual de controles y la debida diligencia de terceros queden adecuadamente reflejados en procedimientos y protocolos de implementación, con reportería periódica a las instancias formales de riesgos y cumplimiento del Consejo.

El Consejo tomó conocimiento de lo expuesto, formuló lineamientos para reforzar la claridad de roles, la trazabilidad de la implementación y la reportería periódica, y solicitó que las versiones finales consoliden las observaciones realizadas, resguardando la coherencia entre las políticas y su despliegue gradual.

No habiendo otros asuntos que tratar, se levanta la sesión a las 12:30 horas, firmando al pie los consejeros asistentes y la secretaria abogada del Consejo.

Enrique Ignacio
Marshall Rivera
5818543-4
emarshall@fapp.cl

Firmado electrónicamente según Ley 19799
el 16-03-2026 a las 18:39:54 con Firma Electrónica Avanzada
Código de Validación: 1773697194723
Validar en https://www5.esigner.cl/esignercryptofront/documento/verificar/

Enrique Marshall R.
Presidente

Rosario Celedon

Rosario Celedón Forster
13253137-4 rceledon@fapp.cl
Firmado electrónicamente según Ley 19799
el 16-03-2026 a las 10:09:11 con Firma Electrónica Avanzada
Código de Validación: 1773666551203
Validar en https://www5.esigner.cl/esignercryptofront/documento/verificar/

Rosario Celedón F.
Vicepresidenta

Rodrigo Ernesto
Caputo Galarce
11646501-9
rcaputo@fapp.cl

Firmado electrónicamente según Ley 19799
el 16-03-2026 a las 10:19:40 con Firma Electrónica Avanzada
Código de Validación: 1773667180953
Validar en https://www5.esigner.cl/esignercryptofront/documento/verificar/

Rodrigo Caputo G.
Consejero

Soledad DEL
CARMEN HUERTA CASAS
8011298-K
shuerta@fapp.cl

Firmado electrónicamente según Ley 19799
el 17-03-2026 a las 13:25:21 con Firma Electrónica Avanzada
Código de Validación: 1773764721053
Validar en https://www5.esigner.cl/esignercryptofront/documento/verificar/

Soledad Huerta C.
Consejera

Catalina Coddou Liendo
19296837-2 ccoddou@fapp.cl
Firmado electrónicamente según Ley 19799
el 16-03-2026 a las 11:39:07 con Firma Electrónica Avanzada
Código de Validación: 1773671947746
Validar en https://www5.esigner.cl/esignercryptofront/documento/verificar/

Catalina Coddou L.
Secretaria y ministra de fe