ACTA SESIÓN ORDINARIA N° 119 DEL CONSEJO DIRECTIVO DEL ADMINISTRADOR DEL FONDO AUTÓNOMO DE PROTECCIÓN PREVISIONAL

En Santiago, a 23 de junio de 2026, siendo las 11:00 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; Diego Kother, director Jurídico, actuando como secretario de actas y ministro de fe y Diego Pérez, abogado senior de la Dirección Jurídica y de Asuntos Institucionales.

Se deja constancia de que la sesión se celebró de manera híbrida, utilizando una plataforma de videoconferencia que garantizó la comunicación simultánea e interactiva entre los consejeros e invitados convocados, permitiéndoles deliberar y votar en tiempo real.

Tabla. -

1. Convocatoria y quórum para sesionar.
2. Marco regulatorio sobre Ciberseguridad para el Administrador del Fondo Autónomo– Bitlaw.
3. Aprobación Manual de Prevención de Lavado de Activos y Financiamiento del Terrorismo.
4. Aprobación de modificación Estatuto Comité de Auditoría, Riesgo y Cumplimiento.

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. Marco regulatorio sobre Ciberseguridad para el Administrador del Fondo Autónomo – Bitlaw. -

Concurrió a la sesión doña Paulina Silva, Socia del asesor externo Bitlaw, quien presentó al Consejo Directivo una exposición sobre el marco regulatorio de ciberseguridad aplicable al Administrador y los principales desafíos derivados de la entrada en vigor de la nueva normativa.

En primer término, explicó el contexto en que surge la regulación de ciberseguridad, como parte del ecosistema normativo digital a la luz de estándares internacionales, que busca establecer obligaciones de cuidado a las organizaciones que administran información o prestan servicios relevantes para la comunidad.

En ese sentido, indicó que el objetivo de la normativa era incentivar la adopción de medidas preventivas destinadas a reducir la ocurrencia y el impacto de incidentes de ciberseguridad, considerando que la persecución de los responsables de este tipo de conductas delictivas resultaba especialmente compleja. Agregando que este marco contempla un régimen de responsabilidades regulatorias que pudieran derivarse del incumplimiento de las obligaciones de prevención establecidas en la normativa.

Asimismo, señaló que este modelo respondía a un esquema de responsabilidad compartida, por cuanto las organizaciones administraban información perteneciente a terceros y prestaban servicios cuya continuidad resultaba relevante para el funcionamiento del país. En ese contexto, explicó que la regulación descansaba sobre dos obligaciones fundamentales: adoptar medidas destinadas a proteger los sistemas e información de la organización y reportar oportunamente los incidentes de ciberseguridad a las autoridades competentes, derivándose de estos dos deberes el resto de las obligaciones contempladas en la ley.

Ante preguntas formuladas por los Consejeros, destacó que uno de los conceptos centrales de la regulación era la "*ciber resiliencia*", indicando que el objetivo de la normativa no consistía únicamente en prevenir que las organizaciones fueran objeto de ataques informáticos (circunstancia que, en la práctica, resultaba imposible garantizar), sino en desarrollar capacidades para responder adecuadamente frente a dichos incidentes, minimizar sus efectos y restablecer oportunamente la continuidad operacional de los servicios. En ese sentido, explicó que la regulación buscaba fortalecer la capacidad de recuperación de las organizaciones frente a eventos de ciberseguridad.

Posteriormente, presentó acerca el marco regulatorio vigente en Chile, indicando que éste se encontraba conformado por un conjunto de normas de aplicación general y sectorial. En particular, se refirió a la Ley Marco de

Ciberseguridad N° 21.663 y a la nueva Ley de Protección de Datos Personales, cuya entrada en vigor se encontraba prevista para diciembre de 2026, señalando que ambas conformaban un sistema regulatorio complementario. Asimismo, indicó que el Administrador se encontraba sujeto a normativa sectorial contemplada en el Compendio de Normas del Sistemas de Pensiones y las facultades regulatorias y supervisoras de la Superintendencia de Pensiones, las cuales ya contemplaban obligaciones relacionadas con la gestión de incidentes de ciberseguridad y la seguridad de la información como parte de su marco de supervisión basada en riesgos.

Sobre este punto se abordaron preguntas de los Consejeros en cuanto a instancias de coordinación interinstitucional considerando que en ámbito financiero y previsional ya existe normativa sectorial sobre la materia como parte del marco de gestión de riesgo operacional y la obligación de reportar a la Superintendencia de Pensiones eventuales incidentes operacionales

Sobre esta materia, explicó que la Ley Marco de Ciberseguridad creó una institucionalidad especializada, que es la Agencia Nacional de Ciberseguridad (ANCI), que tiene un rol de coordinación con las distintas autoridades sectoriales y que establece para un universo amplio de sujetos obligados (tanto públicos como privados) el deber de reportarle incidentes de ciberseguridad. Con ello, se perseguiría principalmente generar inteligencia y fortalecer la respuesta coordinada frente a amenazas de ciberseguridad.

Luego, abordó las categorías de sujetos obligados contempladas en la Ley Marco de Ciberseguridad, distinguiendo entre proveedores de servicios esenciales (aquellos necesarios para el normal funcionamiento del país) y operadores de importancia vital (instituciones públicas o privadas que dependen de redes y sistemas informáticos, y que, en caso de ser afectados por un ciberataque, puedan poner en riesgo la seguridad y el orden público, la prestación continua y regular de un servicio esencial para la ciudadanía, o el normal funcionamiento del Estado), precisando que estos últimos se encontraban sujetos a un régimen de obligaciones más exigente. Informó que el Administrador había sido incorporado dentro de la categoría de operador de importancia vital, en su calidad de organismo público y por desarrollar funciones vinculadas a la administración de prestaciones de seguridad social, circunstancia que determinaba la aplicación de estándares reforzados en materia de ciberseguridad.

A continuación, explicó que la ANCI había comenzado a dictar instrucciones generales destinadas a desarrollar las obligaciones establecidas en la ley, precisando las medidas mínimas que debían implementar los sujetos

regulados. En este contexto, señaló que los operadores de importancia vital debían establecer sistemas de gestión de seguridad de la información, implementar planes de continuidad operacional y de ciberseguridad, desarrollar programas permanentes de capacitación, designar un delegado de ciberseguridad y adoptar medidas destinadas a reducir el impacto de eventuales incidentes, entre otras obligaciones.

Sobre la obligación de adopción de medidas ante eventuales incidentes de ciberseguridad, el Consejo consultó si las medidas destinadas a reducir el impacto de un incidente se encontraban expresamente determinadas por la normativa o si correspondían a obligaciones de carácter general. La expositora respondió que la regulación se encontraba orientada al cumplimiento de objetivos, otorgando cierto grado de flexibilidad a las organizaciones para definir las medidas específicas que permitieran alcanzar dichos fines.

Posteriormente, abordó el deber de reportar incidentes de ciberseguridad al CSIRT Nacional, indicando que la normativa establecía plazos breves para efectuar dichas comunicaciones. No obstante, señaló que, en la práctica, durante las primeras horas posteriores a un incidente normalmente no era posible determinar con precisión su origen, alcance o impacto efectivo, razón por la cual su implementación representaba uno de los principales desafíos para las organizaciones.

Finalmente, explicó que el adecuado cumplimiento de estas obligaciones resultaba fundamental para fortalecer la resiliencia institucional y asegurar la continuidad operacional del Administrador frente a eventuales amenazas de ciberseguridad.

Al respecto, los Consejeros consultaron por el grado de implementación de las exigencias aplicables a operadores de importancia vital por parte del Administrador, a lo cual el Director Ejecutivo ratificó que el plan de trabajo diseñado por la Dirección de Tecnología y Datos y la Dirección de Riesgos consideraba dichos estándares anticipando una eventual calificación, por lo que a la fecha los avances eran relevantes en cuanto a aprobación de Políticas de Seguridad de Información, Policita de tecnología de Información, Política de Gestión y Gobierno de Datos, Política de Continuidad Operaciones y Resiliencia, designación de delegado ciberseguridad, así como instancias de capacitación al personal. Asimismo, dio cuenta de inicio de un proceso de fiscalización por parte de la Superintendencia de Pensiones que busca identificar el grado de preparación del Administrador ante su calificación como OIV, por lo que, en una próxima sesión de Consejo se presentará un reporte más detallado sobre la materia.

3. Aprobación Manual de Prevención de Lavado de Activos y Financiamiento del Terrorismo. –

A continuación, concurrieron a la sesión don Andrés Cifuentes, director de Riegos y doña Marjorie García, Jefe de Cumplimiento, quienes presentaron al Consejo Directivo los ajustes incorporados a la propuesta de Manual de Prevención de Lavado de Activos y Financiamiento del Terrorismo, a la luz de preguntas y observaciones formuladas por los Consejeros, explicando las principales modificaciones incorporadas al documento respecto de la versión previamente revisada.

En ese sentido, el director de Riesgos señaló que los principales cambios atendieron a temas relativos a:

- Complementación y reordenamiento de objetivos y alcances.
- Descripción más detallada de las funciones de las 3 líneas de defensa.
- La Debida Diligencia fue extendida a todas las contrapartes del Administrador del Fondo Autónomo.
- Descripción de las señales de alerta y uso de documento paralelo para llevar el detalle.

Al efecto, los expositores revisaron el documento con los ajustes efectuados y atendieron las consultas formuladas por el Consejo.

ACUERDO N° 1

Los consejeros, por unanimidad, aprobaron el Manual de Prevención de Lavado de Activos y Financiamiento del Terrorismo, en los términos presentados.

4. Aprobación modificación Estatuto Comité de Auditoría, Riesgo y Cumplimiento. -

Luego, se presentó al Consejo las modificaciones propuestas al Estatuto del Comité de Auditoría, Riesgos y Cumplimiento, exponiendo el principal cambio incorporado al texto vigente, correspondiente a la periodicidad de las sesiones del mismo, modificándose de 4 a 6 veces al año, según el calendario definido por el Presidente del Comité en función del plan de trabajo del Consejo y del Administrador del Fondo Autónomo.

Los expositores explicaron el alcance de cada una de las modificaciones propuestas y respondieron las consultas formuladas por el Consejo Directivo.

ACUERDO N° 2

Los consejeros, por unanimidad, aprobaron las modificaciones al Estatuto del Comité de Auditoría, Riesgos y Cumplimiento, en los términos presentados.

Constancia. -

Se deja constancia de que la sesión se celebró de manera híbrida, utilizando una plataforma de videoconferencia que garantizó la comunicación simultánea e interactiva entre los consejeros e invitados convocados, permitiéndoles deliberar y votar en tiempo real.

No habiendo otros asuntos que tratar, se levanta la sesión a las 13:00 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 20-07-2026 a las 11:17:57 con Firma Electrónica Avanzada
Código de Validación: 178456067484
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 20-07-2026 a las 11:05:33 con Firma Electrónica Avanzada
Código de Validación: 178455933363
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 20-07-2026 a las 15:14:33 con Firma Electrónica Avanzada
Código de Validación: 178457487336 1
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 23-07-2026 a las 15:39:55 con Firma Electrónica Avanzada
Código de Validación: 178483559590 6
Validar en https://www5.esigner.cl/esignercryptofront/documento/verificar/

Soledad Huerta C.
Consejera

Diego Andrés
Kother Kraemer
17346767-2
diego.kother@fapp.cl

Firmado electrónicamente según Ley 19799
el 20-07-2026 a las 12:19:11 con Firma Electrónica Avanzada
Código de Validación: 178456435114 9
Validar en https://www5.esigner.cl/esignercryptofront/documento/verificar/

Diego Kother K.
Secretario y ministro de fe