BCU
SUPERINTENDENCIA
DE SERVICIOS FINANCIEROS

ESTÁNDARES MÍNIMOS DE GESTIÓN PARA ADMINISTRADORAS DE FONDOS DE AHORRO PREVISIONAL

Vigencia: 1 de Julio de 2017

BANCO CENTRAL DEL URUGUAY

INTRODUCCIÓN

Se hace saber a las Administradoras de Fondos de Ahorro Previsional que, en el marco de las facultades y cometidos asignados por las normas legales correspondientes, la Superintendencia de Servicios Financieros ha definido que el proceso de supervisión debe estar orientado a ser integral, proactivo, enfocado a riesgos y sobre una base consolidada.

Una de las herramientas con que cuenta la supervisión para cumplir con sus cometidos es el trabajo llevado a cabo in-situ en las instituciones, a través del cual se procederá a evaluar la calidad de la gestión de las entidades y de los fondos previsionales y en caso de detectar debilidades, evaluar el impacto sobre la capacidad de la entidad de mantener niveles prudenciales de solvencia, y sobre la seguridad, estabilidad y rendimientos de los fondos de pensión.

Para ello, los Supervisores analizarán:

- El Gobierno Corporativo, es decir, el sistema a través del cual las instituciones son dirigidas, monitoreadas y controladas, y los fondos de pensión son gestionados

- El Sistema de Gestión de Riesgos de la institución y la capacidad de la misma de identificar, controlar, medir y monitorear los siguientes riesgos en forma integral (tanto para la Administradora como para los Fondos de Pensión):

    - Riesgo de Crédito

    - Riesgo de Mercado

    - Riesgo de Liquidez

    - Riesgo Operacional

    - Riesgo de Reputación

    - Riesgo de Lavado de Activos y Financiamiento de Terrorismo

- La gestión de los riesgos tecnológicos y confiabilidad y eficacia de los sistemas de información como herramientas de la gestión.

De acuerdo a lo previsto en el artículo 30.3.1 de la Recopilación de Normas de Control de Fondos Previsionales, en aras de generar valor para los afiliados y de proveer orientación a las instituciones sobre qué se espera de ellas, se ha elaborado una serie de estándares mínimos de gestión asociados a los aspectos que se procederá a evaluar.

Desde el punto de vista del supervisor, se entiende que el no cumplimiento de un estándar constituye una debilidad que debe ser tratada con atención prioritaria por la entidad.

LOS ESTÁNDARES MÍNIMOS

Las instituciones adoptan diferentes esquemas y estructuras para llevar adelante su gestión, tomando en cuenta la naturaleza y complejidad del negocio previsional y el tamaño de los fondos administrados.

El supervisor lleva adelante sus procedimientos de supervisión y evaluación teniendo en cuenta estos elementos. Los estándares constituyen prácticas de gestión que el supervisor espera encontrar en las entidades supervisadas. El supervisor formula su juicio global sobre la entidad en base a procedimientos a distancia y a una serie de procedimientos in-situ. Se buscan evidencias de que los procesos y procedimientos, en general, son adecuados dadas las características de cada entidad y que las distintas estructuras de Gobierno Corporativo cumplen con sus roles y responsabilidades en forma adecuada.

Los hallazgos permiten a posteriori definir si existen o no apartamientos a los estándares que se definen seguidamente. El supervisor no certifica la adherencia estricta a los puntos específicos contenidos en estos estándares.

El caso de los Conglomerados Financieros o Grupos Financieros

Las prácticas de gestión deben aplicarse tanto a las entidades individualmente consideradas como al grupo financiero que integran. El hecho de pertenecer a un grupo genera una serie de riesgos (contagio, concentraciones, riesgos derivados de operaciones y exposiciones intra-grupo, múltiple uso del capital, etc.), por lo cual deben considerarse los riesgos incrementales que pueden generarse por pertenecer a un grupo financiero.

En el marco de este documento se estará refiriendo a este tipo de estructuras como "conglomerados financieros" o "grupos financieros" en forma indistinta.

Definiciones

Marco de gestión del riesgo: incluye las políticas, procesos, controles y sistemas a través de las cuales se establece, comunica y monitorea el apetito de riesgo. Incluye además la declaración del apetito de riesgo, los límites de riesgo y un resumen de los roles y responsabilidades de los que supervisan la implementación y el monitoreo del apetito de riesgo. El marco debe tomar en cuenta los principales riesgos que enfrenta la institución y estar alineado con su estrategia y su plan de negocios.

Apetito de riesgo: El apetito de riesgo es el nivel y el tipo riesgo que una institución está dispuesta a asumir, teniendo en cuenta los objetivos definidos y las obligaciones con los accionistas. El apetito de riesgo es generalmente expresado en términos cuantitativos y cualitativos y deben considerarse para definirlo la posibilidad de ocurrencia de condiciones y eventos extremos. El apetito de riesgo debe reflejar el potencial impacto en los resultados y el nivel de capital de la institución y en el Fondo de Ahorro Previsional

Declaración del apetito de riesgo: es el documento en el cual se establece el apetito de riesgo.

Límites de riesgo: Es la cantidad de riesgo aceptable relacionado a los riesgos específicos del negocio. Un sistema de límites puede incluir los límites de riesgo

que no deben ser superados, de acuerdo con las políticas y los indicadores de alerta definidos.

Perfil de riesgo: valoración en un momento dado de las exposiciones al riesgo brutas de la institución o si procede exposiciones al riesgo netas.

Deber de diligencia: Deber de los miembros del Directorio de decidir y actuar con conocimiento de causa y prudencia en los asuntos de la institución y del fondo previsional. Suele interpretarse como la obligación de los directores de tratar los asuntos de la entidad y del fondo previsional como lo haría una «persona prudente» con sus asuntos personales.

Deber de lealtad: Deber de los directores de actuar de buena fe en el interés de la institución y de los afiliados. El deber de lealtad debe impedir que cada director actúe en interés propio, o en el interés de otro individuo o grupo, a expensas de la institución, de los afiliados y de los accionistas.

Conglomerado Financiero: conjunto o grupo formado por dos o más entidades interconectadas bajo un control común, o influencia significativa, de forma directa o indirecta, donde al menos alguna de ellas opera en algún sector regulado por la Superintendencia de Servicios Financieros.

ESTÁNDARES DE GOBIERNO CORPORATIVO (C)

El Gobierno Corporativo es el sistema a través del cual las instituciones y los fondos previsionales son dirigidos, monitoreados y controlados e incluye a la Dirección, la Alta Gerencia, el Comité de Inversiones y a los distintos mecanismos de control como son la Auditoría Interna, la Auditoría Externa y el Comité de Auditoría.

Un Gobierno Corporativo eficaz se basa en los siguientes componentes fundamentales:

- Cultura corporativa apropiada, con normas establecidas para un comportamiento responsable y ético

- Marco de gestión del riesgo

- Responsabilidades bien definidas y comunicadas a toda la organización para la gestión de riesgos y controles, lo que se conoce como «las tres líneas de defensa»:

    - la línea de negocio;
    - una función de gestión del riesgo y de cumplimiento independientes de la primera línea de defensa; y
    - una función de auditoría interna independiente

  La línea de negocio – primera línea de defensa - es donde se generan primordialmente los riesgos y es responsable de su gestión continua.

  La Gestión del riesgo, -segunda línea de defensa-, es responsable de identificar, medir, controlar y monitorear el riesgo, en forma independiente de la primera línea de defensa. La función de cumplimiento es también parte de esta segunda línea; es responsable de realizar el seguimiento continuo del cumplimiento de la legislación, normas de gobierno corporativo, regulaciones, códigos y políticas a las que esté sujeta la institución.

  La función de Auditoría Interna es la tercera línea de defensa. La misma debe realizar auditorías y revisiones independientes de las dos líneas anteriores, para garantizar al Directorio que el marco de gobierno general, incluido el marco de gestión de riesgos, es eficaz y que existen y se aplican consistentemente las políticas y procesos definidos.

- Debe existir una clara definición de roles y responsabilidades dentro de la organización y una estructura que permita establecer sus objetivos, determinando los medios para alcanzarlos y cómo supervisar su cumplimiento. La estructura organizacional debe permitir a la Dirección implementar una estrategia eficiente y efectiva para la institución y el fondo previsional, para asegurar al mismo tiempo un fuerte control interno, un buen sistema de administración de riesgos, a través de sistemas de información que garanticen su integridad, confiabilidad, oportunidad y accesibilidad. El Directorio y la Alta Gerencia de la Institución deben ser integrados por personas con los conocimientos, experiencia y competencias necesarias para cumplir sus roles respectivos. Deben planificar y dirigir la gestión comercial y de riesgos y manejar eficazmente la solvencia de la entidad y del fondo que administran.

- Debe promoverse una cultura de riesgo adecuada en relación a la actividad de gestión de los fondos previsionales.

Se consideran en este capítulo los estándares mínimos que deben cumplir el Directorio, la Alta Gerencia, el Comité de Inversiones, el Comité de Auditoría, la Auditoría Interna y la Auditoría Externa para asegurar un adecuado funcionamiento del Gobierno Corporativo.

DIRECTORIO

En adelante, cuando se hace referencia al Directorio debe entenderse como el órgano que ejerce la administración efectiva de la entidad.

El Directorio es el responsable último de definir la estrategia de negocios y controlar su implementación, vigilar la solvencia financiera de la institución y del fondo previsional, tomar las decisiones sobre el personal clave, la organización interna y las prácticas de gobierno, fijar el apetito de riesgo y controlar la gestión del riesgo y el cumplimiento de las obligaciones legales y regulatorias. También es responsable de asegurar la implementación de un sistema de remuneración con los incentivos adecuados.

El cuidado, diligencia, habilidad y prudencia con la cual los integrantes del Directorio cumplen sus roles tiene una influencia crítica sobre la viabilidad, seguridad y solidez de la institución, así como sobre la adecuada gestión y solvencia de los fondos previsionales, sobre su capacidad de ejecutar la estrategia de negocio y cumplir los objetivos y sobre su capacidad de generar confianza por parte de los afiliados y beneficiarios, supervisores y otros actores.

LOS ESTÁNDARES MÍNIMOS QUE EL DIRECTORIO DEBE CUMPLIR SON LOS QUE SE DETALLAN A CONTINUACIÓN:

1. El Directorio debe mantener una estructura apropiada que permita una visión independiente de la influencia de la Alta Gerencia, de influencias políticas y/o de otros intereses externos.

Para ello:

1.1 El Directorio (3 miembros como mínimo) debe incluir personas con un buen balance de habilidades, experiencia y conocimientos, que de forma colectiva posean las aptitudes necesarias conforme al tamaño del fondo administrado,

1.2 Los Directores No Ejecutivos[1] no deben tener injerencia en las decisiones diarias de la gestión.

1.3 Los Directores Ejecutivos no deben ejercer una influencia dominante en el conjunto del Directorio.

[1] Si bien no existe desde el punto de vista jurídico el concepto de Director No Ejecutivo, debe entenderse por tal a aquellos Directores que no cumplen ninguna función ejecutiva, aunque mantienen sus responsabilidades en tanto Directores.

1.4 Los integrantes del Directorio deben tener un claro entendimiento de su rol dentro del Gobierno Corporativo y deben cumplir con el deber de lealtad y diligencia.

1.5 El Directorio debe poseer la capacidad de ejercer un juicio independiente sobre los asuntos de la institución. Ello no obsta a que el Directorio pueda participar en el proceso de aprobación de algunas operaciones o en algunas decisiones operativas de significativa magnitud para la entidad y para el fondo previsional.

1.6 El Directorio debe implementar una estructura de Comités de Dirección (que contemple como mínimo al Comité de Inversiones y al Comité de Auditoría) acorde con el volumen de las actividades de la entidad para asegurar la participación de los distintos sectores involucrados en las decisiones relevantes.

1.7 El Directorio y sus comités deben mantener documentadas sus deliberaciones y decisiones (por ejemplo, actas de reuniones o resúmenes de temas tratados, recomendaciones emitidas, decisiones adoptadas y reportes utilizados para la toma de decisiones).

2. El Directorio debe asegurar un adecuado relacionamiento con el accionista o con la entidad controlante y con las entidades vinculadas.

Para ello el Directorio debe asegurar que:

2.1 Existe una adecuada coordinación e integración entre las distintas estructuras de Gobierno Corporativo de la entidad y su controlante.

2.2 Existe un adecuado control y monitoreo sobre las actividades tercerizadas, cuando sean realizadas por empresas relacionadas.

2.3 Sus roles y responsabilidades y los de su controlante y vinculadas se encuentran claramente establecidos y delimitados.

2.4 Su independencia es respetada por parte de su controlante en lo que refiere a las responsabilidades que debe asumir el Directorio.

3. El Directorio debe aprobar los objetivos estratégicos de la institución y del Fondo Previsional y supervisar su implementación.

Para ello, el Directorio debe:

3.1 Aprobar un marco estratégico que defina claramente los objetivos de la entidad y del fondo previsional, y los resultados esperados en cada caso, de forma consistente con el nivel de riesgo definido. Este marco debe ser claramente plasmado en políticas escritas y comunicado a toda la institución.

3.2 Aprobar el Plan Estratégico que contemple los objetivos definidos.

3.3 Aprobar la Política de Inversiones para el Fondo de Ahorro Previsional

3.4 Evaluar regularmente los resultados contra el presupuesto aprobado.

3.5 Revisar por lo menos anualmente los objetivos estratégicos, las políticas de inversión, los planes y el apetito de riesgo para asegurar que siguen siendo válidos.

3.6 Asegurar la existencia de un sistema de información íntegro, confiable y oportuno que permita tomar sus decisiones y que asegure la efectividad de las mismas.

3.7 Aprobar una estrategia y políticas de Tecnología de la Información (TI), adecuadas a la estrategia general de la institución y del fondo previsional y asegurar que la Alta Gerencia implementa los procedimientos que las hacen aplicables, para lo cual debe asegurar que:

- La institución cuenta con una organización y con personal capacitado para una adecuada gestión de TI y de los riesgos asociados.

- El soporte de TI permite dar cumplimiento a los requerimientos legales, regulatorios, contractuales y operativos para el manejo de riesgos.

3.8 Aprobar una estrategia y políticas de Seguridad de la información adecuadas a la estrategia general de la institución y asegurar que la Alta Gerencia implemente los procedimientos que las hacen aplicables.

4. El Directorio debe seleccionar, monitorear y si es necesario reemplazar a la Alta Gerencia.

Para ello, el Directorio debe:

4.1 Aprobar los roles y responsabilidades de la Alta Gerencia

4.2 Evaluar regularmente la efectividad y prudencia de la Alta Gerencia en la gestión de las operaciones y de los riesgos.

4.3 Asegurar que la Alta Gerencia que se designe cumple con los criterios de capacidad e integridad y que sus actuaciones son coherentes con la estrategia y políticas aprobadas por el Directorio

4.4 Cuestionar y revisar de forma crítica las explicaciones e información facilitada por la Alta Gerencia.

4.5 Aprobar un plan de sucesión para el equipo gerencial.

5. El Directorio debe aprobar una estrategia de riesgos y políticas asociadas que permitan la identificación, medición, monitoreo y control de todos los riesgos que puedan afectar el cumplimiento de los objetivos de la entidad y del fondo administrado.

Para ello el Directorio debe:

5.1 Entender los riesgos que enfrenta la entidad y el fondo administrado, así como definir el nivel de exposición a cada tipo de riesgo.

5.2 Promover una cultura de riesgos en la organización.

5.3 Aprobar la estrategia de riesgos y revisarla al menos anualmente, la que debe incluir todos los riesgos que quiere asumir y la tolerancia a los mismos.

La estrategia de riesgos debe:

- Ser consistente con la estrategia general, el perfil general de riesgo y el Plan estratégico definido.
- Estar claramente definida por escrito y ser coherente con prácticas prudentes y con los requisitos regulatorios
- Evaluar y ajustar la estrategia periódicamente considerando factores internos y externos que afectan la entidad y el fondo previsional (situación macroeconómica y de los mercados, su posición en el mercado, las capacidades del personal, la tecnología, etc.).

5.4 Asegurar que la Alta Gerencia toma las medidas necesarias para implementar un sistema de gestión integral de riesgos que involucra a todo el personal.

5.5 Asegurar que existan políticas y procedimientos por escrito que constituyan una guía efectiva para asumir y gestionar los riesgos

5.6 Contar con programas de pruebas de tensión prospectivas, acordes con el perfil de riesgo como parte integral del proceso de gestión del riesgo.

5.7 Asegurar que existe una gestión de la seguridad de la información cuyos objetivos se encuentran alineados con los del negocio.

5.8 Asegurar que existe un sistema de Evaluación de Riesgos que garantiza el logro de los objetivos de TI y de seguridad de la información de la entidad y del fondo administrado y permita responder a las amenazas

5.9 Asegurar que los procesos relevantes (entre ellos TI e inversiones) se monitorean y son auditados regularmente por personas independientes.

5.10 Asegurar que la institución cuenta con un plan de continuidad del negocio adecuado al volumen de sus operaciones y que, en particular, incluya un plan de contingencia de TI.

6. El Directorio debe promover una cultura corporativa que exija y provea los incentivos adecuados para una conducta ética y que evite o administre los posibles conflictos de interés.

Para ello el Directorio debe:

6.1 Establecer y comunicar los estándares éticos a través de un Código de Ética que guíen el accionar de la institución.

6.2 Definir una política por escrito sobre conflictos de intereses y un procedimiento de cumplimiento para su aplicación.

6.3 Actuar como ejemplo del cumplimiento de los estándares éticos.

6.4 Asegurar que la Alta Gerencia implementa políticas y procedimientos adecuados para evitar o administrar los posibles conflictos de interés y confirmar que los empleados y la Alta Gerencia son conscientes de que se tomarán medidas disciplinarias u otras medidas apropiadas ante comportamientos inaceptables o infracciones.

6.5 Asegurar que existen políticas y procedimientos claramente definidos para el tratamiento de operaciones con partes relacionadas para que todas las transacciones se realicen en condiciones de equidad o mercado y se adopten códigos de gobierno corporativo adecuados. Estas políticas deberían incluir la aprobación por parte del Directorio de las operaciones más significativas.

6.6 Asegurar que las políticas de remuneración y compensación son transparentes y consistentes con la estrategia global de largo plazo de la institución y que existen mecanismos para verificar su cumplimiento.

6.7 Vigilar la integridad, independencia y eficacia de las políticas y procedimientos de denuncia de irregularidades de la institución.

7. El Directorio debe promover una cultura de control en la organización, verificando que la Alta Gerencia implementa las políticas y procedimientos necesarios para que todos entiendan su rol en el control interno y la gestión de riesgos.

Para ello, el Directorio debe:

7.1 Promover una cultura de riesgo y transmitir que todos los empleados son responsables de ayudar a la institución a operar dentro del grado de apetito de riesgo y las delimitaciones del riesgo establecidas

7.2 Aprobar la estructura organizativa acorde al tamaño del fondo administrado y volumen de las operaciones y al perfil de riesgos de la institución y el fondo previsional y asegurar que la misma es conocida por toda la organización.

Esta estructura debe asegurar:

- una clara separación y equilibrio de las funciones de gestión de afiliados e inversiones, de las funciones de monitoreo y control

- que existe una función de cumplimiento claramente definida e independiente de la gestión, contando con la suficiente autoridad, relevancia, recursos y acceso al Directorio.

- que existe una adecuada segregación de funciones que facilite los controles cruzados.

7.3 Asegurar que existen mecanismos de control interno efectivos.

7.4 Asegurar que existe una clara definición de deberes y responsabilidades que sea consistente con la estrategia definida y que permita una clara asignación de autoridad.

7.5 Controlar a la Alta Gerencia en la implementación de las estrategias y el cumplimiento de las políticas establecidas.

7.6 Asegurar que el nivel de control se mantiene aún en el caso de tareas tercerizadas.

7.7 Asegurar que el sistema de información sea oportuno, íntegro y confiable. En particular, el Comité de Auditoría o la Auditoría Interna deberán cerciorarse que la información utilizada para la toma de decisiones es adecuada.

8. El Directorio debe asegurar que el Comité de Auditoría cumple su cometido.

Para ello, el Directorio debe:

8.1 Aprobar un estatuto o misión que establezca el propósito del Comité, sus objetivos, organización, autoridad y responsabilidad, así como las características que debe tener el registro donde consten los temas tratados en cada reunión del Comité de Auditoría

8.2 Asegurar que la integración de este Comité de Dirección es acorde con el volumen de las operaciones y que permite cumplir su cometido con independencia. Para ello, la mayoría de los miembros no deben estar involucrados con la gestión diaria de la entidad.

8.3 Asegurar que la experiencia de todos sus miembros es compatible con sus obligaciones.

8.4 Proveer al Comité de Auditoría de apoyo y recursos para que pueda desempeñar sus funciones en forma independiente.

8.5 Asegurar que la periodicidad de las reuniones es suficiente para monitorear y evaluar el adecuado funcionamiento de los mecanismos de control interno

8.6 Tener comunicación regular con el Comité de Auditoría promoviendo la rápida resolución de debilidades encontradas.

9. El Directorio debe asegurar que el Comité de Inversiones cumple su cometido.

Para ello, el Directorio debe:

9.1 Aprobar un estatuto o misión que establezca el propósito y definir las funciones del Comité de Inversiones, sus objetivos, organización, autoridad y responsabilidad, así como las características que debe tener el registro donde consten los temas tratados en cada reunión del Comité de Inversiones y las resoluciones adoptadas.

9.2 Definir pautas de funcionamiento del Comité de Inversiones acordes con el volumen del fondo previsional y de las operaciones. Como mínimo estas pautas deben fijar la periodicidad de actuación de este Comité (al menos una sesión bimensual)

9.3 Asegurar que la integración de este Comité de Dirección es acorde con el tamaño del fondo previsional administrado y el volumen de las operaciones que realiza y que permite cumplir su cometido con independencia.

9.4 Asegurar que la experiencia de todos sus miembros es compatible con sus obligaciones.

9.5 Proveer al Comité de Inversiones de apoyo y recursos para que pueda desempeñar sus funciones en forma independiente.

10. El Directorio debe asegurar que la función de Auditoría Interna (propia o tercerizada) cumple su cometido.

Para ello el Directorio debe:

10.1 Asegurar que la Auditoría Interna es independiente de las actividades auditadas y que cuenta con la suficiente autoridad y jerarquía para poder actuar con objetividad e imparcialidad.

10.2 Asegurar que la línea de reporte es a sí mismo o al Comité de Auditoría.

10.3 Asegurar que la función de Auditoría Interna es llevada a cabo por personal independiente, competente y capacitado y que existen recursos suficientes para cumplir con los objetivos establecidos y el plan anual.

10.4 Asegurar, en forma directa o a través del Comité de Auditoría que el Auditor Interno cumple con sus cometidos con eficacia y eficiencia.

10.5 Asegurar el acceso de la Auditoría Interna a la información necesaria para ejercer su función con eficacia.

10.6 Asegurar que la Alta Gerencia actúa para resolver deficiencias o debilidades encontradas por la Auditoría Interna.

10.7 En el caso que dicha función se tercerice se deberá asegurar que se cumplan los estándares anteriormente detallados.

11. El Directorio debe asegurar que la Auditoría Externa cumple su cometido.

Para ello, el Directorio debe:

11.1 Reconocer y comunicar la importancia de la función de Auditoría Externa dentro de la organización.

11.2 Tomar las medidas necesarias para asegurar la independencia de la Auditoría Externa dentro de la organización.

11.3 Asegurar que la Alta Gerencia toma las medidas necesarias para corregir los problemas detectados oportunamente.

12. El Directorio debe implementar un proceso para definir el nivel del patrimonio y de la reserva especial suficientes para respaldar los riesgos asumidos y proveer seguridad a los afiliados y beneficiarios.

El Directorio debe asegurar que la institución cuenta con un nivel suficiente de patrimonio y de reserva especial para poder absorber pérdidas potenciales de la institución y del fondo que administra (cuando esto último sea exigido reglamentariamente).

Este patrimonio y esta reserva especial deberán ajustarse a lo que exigen los requisitos regulatorios.

Para ello, el Directorio debe:

12.1 Establecer políticas y procedimientos adecuados y prudentes para la gestión del patrimonio de la institución y para asegurar la suficiencia en todo momento de la reserva especial

12.2 Revisar por lo menos anualmente las políticas, para asegurar que el nivel de patrimonio y de la reserva especial es adecuado y prudente.

ALTA GERENCIA

Las responsabilidades de la Alta Gerencia se centran en la implementación de las políticas, procedimientos, procesos y controles necesarios para gestionar las operaciones y riesgos en forma prudente, para cumplir con los objetivos estratégicos y el apetito de riesgo fijados por el Directorio.

Asimismo, se centran en asegurar que el Directorio recibe información relevante, íntegra y oportuna tal que le permita evaluar la gestión y analizar si las responsabilidades delegadas a la Alta Gerencia se están cumpliendo efectivamente.

En general, debe entenderse como Alta Gerencia al equipo formado por la Gerencia General o similar y las líneas de reporte relevantes, quienes en su conjunto son los responsables de la ejecución de la estrategia de la institución.

LOS ESTÁNDARES MÍNIMOS QUE LA ALTA GERENCIA DEBE CUMPLIR SON LOS QUE SE DETALLAN A CONTINUACIÓN:

13. La Alta Gerencia como equipo y cada uno de sus integrantes deben poseer los conocimientos y habilidades para gestionar y supervisar la actividad de conformidad con la planificación estratégica y otras políticas aprobadas por el Directorio.

Para ello, la Alta Gerencia debe:

13.1 Estar integrada por personas con capacidad, experiencia e integridad necesarias para gestionar las actividades y el personal bajo su supervisión

13.2 Trabajar como equipo respetando los roles de los distintos integrantes y asegurar el cumplimiento de las directivas establecidas por el Directorio

13.3 Ejercer una adecuada vigilancia de sus subordinados y garantizar que las actividades de la institución son coherentes con la estrategia de negocio, apetito de riesgo y políticas aprobadas por el Directorio.

13.4 Tener acceso regular a capacitación para mantener y mejorar sus competencias y mantenerse al tanto de los desarrollos relevantes para sus áreas de responsabilidad

14. La Alta Gerencia debe establecer y seguir un proceso continuo y adecuado para la gestión estratégica de la entidad en función de los lineamientos del Directorio y rendir cuentas a éste de lo actuado.

Para ello, la Alta Gerencia debe:

14.1 Desarrollar y presentar al Directorio para su aprobación:

- El Plan de Negocios, en base a los lineamientos estratégicos y a la declaración de apetito de riesgo definidos por el Directorio, que considere las características del entorno económico y de negocios, la situación financiera y patrimonial de la institución y los riesgos en los cuales tiene o tendrá exposición.
- El Presupuesto anual.
- El plan de continuidad del negocio

14.2 Implementar la Estrategia, el Plan de negocios y el Plan de inversiones aprobado.

14.3 Asegurar que la estructura organizacional es consistente con los objetivos estratégicos y políticas aprobadas por el Directorio.

14.4 Monitorear periódicamente el cumplimiento con respecto al Presupuesto, al Plan de Negocios y al Plan de Inversiones, y analizar los desvíos.

14.5 Proveer al Directorio de información completa, relevante, oportuna y periódica, al menos sobre los siguientes temas:

- la implementación de la Estrategia y los planes
- cambios en la estrategia del negocio, en la estrategia de riesgo
- los resultados y condición financiera de la institución
- excepciones a los límites del riesgo y/o infracciones a las normas de cumplimiento
- deficiencias en los controles internos;
- inquietudes jurídicas o reguladoras;
- denuncia de irregularidades
- resultados de las pruebas del plan de continuidad

14.6 Poner en práctica las políticas de compensación fijadas por el Directorio.

15. La Alta Gerencia debe implementar un Sistema de Gestión Integral de Riesgos que contemple el apetito de riesgos, involucre a todo el personal y sea proactivo.

Para ello, la Alta Gerencia debe:

15.1 Implementar la estrategia de riesgos aprobada por el Directorio.

15.2 Asegurar que existe un responsable del manejo de cada uno de los riesgos y un sistema que permita obtener una visión integral de todos los riesgos que asume la entidad y el fondo de ahorro previsional

15.3 Desarrollar, poner en práctica y hacer cumplir los procesos y procedimientos que permitan identificar, medir, monitorear y controlar todos los riesgos que puedan afectar el cumplimiento de los objetivos de la institución y del fondo de ahorro previsional.

15.4 Asegurar que cuenta con los recursos suficientes para un manejo adecuado de acuerdo al marco de riesgos determinado por la Dirección

15.5 Asegurar que el personal involucrado en el proceso de Gestión de Riesgos tiene la capacidad técnica para comprender y analizar los riesgos asumidos. La descripción de funciones, cargos y responsabilidades del personal involucrado deberá incluir explícitamente el rol en el sistema de gestión integral de riesgos.

15.6 Implementar procedimientos sobre las políticas de seguridad de la información aprobadas por el Directorio.

15.7 Asegurar que existe un sistema de revisión independiente de los procesos y procedimientos de riesgos para identificar y resolver debilidades.

15.8 Implementar un proceso para la aprobación de nuevos instrumentos financieros para el Fondo de Ahorro Previsional que asegure un adecuado control y gestión de riesgos.

15.9 Evaluar y revisar periódicamente los riesgos a los que se enfrenta la institución y su perfil general de riesgo.

16. La Alta Gerencia debe promover una cultura de control en toda la organización.

Para ello, la Alta Gerencia debe:

16.1 Diseñar y mantener una estructura organizacional de acuerdo a los lineamientos aprobados por el Directorio, que asegure un adecuado sistema de control.

16.2 Diseñar un sistema de comunicación que asegure que todo el personal de la institución entiende y cumple su rol en el control interno.

16.3 Asegurar que existen comités y/u otros mecanismos efectivos que aseguren la coordinación y comunicación de actividades entre distintas áreas.

16.4 Asegurar que los comités mantengan adecuadamente documentadas sus deliberaciones y decisiones (por ejemplo, actas de reuniones o resúmenes de temas tratados, recomendaciones emitidas y decisiones adoptadas).

16.5 Demostrar en su actuación diaria un claro compromiso con el control.

16.6 Mantener un seguimiento estricto de los riesgos derivados de las actividades tercerizadas, asegurando la calidad del sistema de control de la institución.

16.7 Tomar las medidas necesarias para corregir los problemas detectados por el Auditor Interno, el Auditor Externo y el Supervisor

16.8 Facilitar el relacionamiento con el supervisor y proveer los elementos necesarios para que éste pueda cumplir su rol.

16.9 Proporcionar al Directorio la información que necesite para efectuar sus funciones de supervisión de la Alta Gerencia y evaluar la calidad de su desempeño.

17. La Alta Gerencia debe implementar las políticas aprobadas por el Directorio para evitar o administrar posibles conflictos de interés y establecer los procedimientos de control necesarios.

Para ello, la Alta Gerencia debe:

17.1 Implementar las políticas y procedimientos para identificar, evitar o administrar y explicitar adecuadamente los conflictos de intereses, en particular, en lo vinculado a las operaciones con entidades relacionadas.

18. La Alta Gerencia debe implementar un proceso íntegro de Gestión de la Tecnología de Información (TI) consistente con la estrategia.

Para ello se debe cumplir que:

18.1 Los roles del responsable del área de TI se encuentran claramente definidos.

18.2 Existen políticas de medición y mitigación de los riesgos en los procesos.

18.3 Se entiende y se comunica la necesidad de cumplir con los requerimientos del organismo supervisor.

18.4 La responsabilidad de TI está ubicada dentro de la estructura general de la organización de modo de garantizar la competencia técnica e independencia respecto de las áreas usuarias, para garantizar soluciones de tecnología de la información, útiles para la organización.

18.5 El área de TI tenga la habilidad de desarrollar, adquirir, instalar y mantener soluciones apropiadas y acordes a las necesidades de la entidad, en forma prudente y dentro de un ambiente controlado

18.6 Existen procedimientos de control de la gestión del área de TI. Los servicios a ser prestados por el área de TI deben ser monitoreados (indicadores clave del desempeño y/o factores críticos de éxito) por la Alta Gerencia y comparados con los niveles mínimos establecidos. La evaluación del desempeño del área de TI debe llevarse a cabo en forma continua.

18.7 se mida la satisfacción del cliente sobre los servicios prestados por el área de TI para identificar el déficit en los niveles de servicio y establecer objetivos de mejoras.

18.8 Los procesos que no alcancen las metas mínimas de desempeño establecidas, se seleccionan para ser incluidos en procesos de mejoras.

19. La Alta Gerencia debe definir e implementar un sistema de información adecuado para cuantificar, evaluar y notificar al Directorio el volumen, composición y calidad de las exposiciones de los riesgos que asume la entidad. La información debe ser confiable, oportuna, fácilmente accesible y provista en un formato consistente.

El sistema de información debe:

19.1 Cubrir todas las actividades significativas de la institución.

19.2 Estar integrado por información financiera, operativa y de cumplimiento, adecuada y completa.

19.3 Incluir información sobre eventos externos y condiciones relevantes a la toma de decisiones.

19.4 El proceso de generación de información debe ser seguro, estar independientemente monitoreado y respaldado con planes de contingencia adecuados

19.5 Cumplir con las características de:

- Oportunidad – El sistema debe proveer información actualizada en forma oportuna a los usuarios apropiados, de forma de facilitar la toma de decisiones.

- Precisión – El sistema de controles sobre el procesamiento de información debe ser efectivo.

- Consistencia – La información debe ser procesada y compilada en forma consistente y uniforme.

  Los cambios en los sistemas deben estar adecuadamente documentados y claramente comunicados a los usuarios de la información.

- Integridad – Los tomadores de decisiones deben contar con información completa y pertinente en forma sintetizada.

- Relevancia - La relevancia de la información está directamente relacionada con las necesidades de la Gerencia y la Dirección para el desarrollo de su trabajo.

19.6 Los informes remitidos al organismo supervisor y al Directorio deben proveer datos confiables, para lo cual se deben verificar previamente.

19.7 Cuando la institución utilice modelos para medir los riesgos, se debe realizar validaciones periódicas e independientes de los mismos.

COMITÉ DE AUDITORÍA

20. El Comité de Auditoría debe asegurar que el Sistema de Gestión Integral de Riesgos de la institución es adecuado y que se toman las medidas necesarias para su mantenimiento en forma continua.

Para ello, el Comité de Auditoría debe:

20.1 Estar conformado adecuadamente de forma de asegurar el cumplimiento de los objetivos fijados para esta estructura de control.

20.2 Tomar medidas para que la Alta Gerencia lleve a cabo las acciones correctivas necesarias para subsanar las observaciones de la Auditoría Interna y Externa de manera oportuna.

20.3 Proveer información al Directorio que le permita evaluar el desempeño del Comité de Auditoría y sus preocupaciones.

20.4 Asegurar que la Alta Gerencia establece y mantiene un adecuado y efectivo sistema de gestión integral de riesgos.

20.5 Implementar un proceso orientado a identificar áreas de riesgo donde se debe profundizar las tareas de Auditoría y documentar sus resultados por lo menos anualmente.

20.6 Aprobar el Estatuto del Auditor Interno en donde se establezca el propósito de la Auditoría Interna, sus objetivos, su autoridad y responsabilidades.

20.7 Analizar y aprobar el plan y cronograma anual de Auditoría Interna y monitorear su funcionamiento y desempeño en el cumplimiento de los planes de auditoría oportunamente aprobados.

20.8 Aprobar la contratación y honorarios de los auditores externos e informar al Directorio. Esta contratación también puede ser realizada por el propio Directorio.

20.9 Validar el plan de trabajo de la Auditoría Externa y efectuar un seguimiento de la independencia y eficacia del Auditor Externo, asegurando que otras tareas adicionales (por ejemplo, consultorías) son compatibles y no impactan negativamente su independencia.

20.10 Revisar los informes de la Auditoría Externa y de la Auditoría Interna

20.11 Establecer una comunicación eficaz con el Auditor Externo y exigirle que le informe sobre todos los asuntos pertinentes de forma que permita a dicho comité desempeñar sus responsabilidades de vigilancia y mejorar la calidad de la auditoría.

20.12 Mantener comunicación periódica con la Superintendencia de Servicios Financieros a fin de conocer sus inquietudes, los problemas detectados en la supervisión de la institución, así como el seguimiento llevado a cabo para su solución

20.13 Revisar las políticas establecidas en la institución relativas al cumplimiento de leyes y regulaciones, normas de ética, conflictos de intereses e investigaciones por faltas disciplinarias y fraude.

COMITÉ DE INVERSIONES

21. El Comité de Inversiones debe definir la estrategia de inversión de los Fondos Previsionales y supervisar el adecuado cumplimiento de la política de inversiones.

Para ello, el Comité de Inversiones debe:

21.1 Estar conformado adecuadamente de forma de asegurar el cumplimiento de su cometido.

21.2 Definir parámetros cuantitativos para la aprobación de inversiones según el riesgo asociado a cada tipo de instrumento. Los asuntos tratados y las resoluciones adoptadas deberán constar en Actas.

21.3 Establecer topes y condiciones que deben cumplir las distintas clases de activos y los emisores

21.4 Analizar las situaciones relativas a los potenciales conflictos de interés relacionados con el proceso de inversión y su tratamiento.

21.5 Tomar las medidas necesarias para que la Alta Gerencia implemente las políticas definidas y supervisar su cumplimiento

21.6 Revisar periódicamente los objetivos, las políticas y los procedimientos para la administración del riesgo de las inversiones del Fondo Previsional

21.7 Supervisar el adecuado cumplimiento de la política y la estrategia de inversiones

21.8 Proveer información al Directorio que le permita evaluar el desempeño del Comité de Inversiones, y el grado de cumplimiento de la política de inversiones

AUDITORÍA INTERNA

22. La función de Auditoría Interna debe proporcionar fiabilidad al Directorio y al Comité de Auditoría sobre la calidad y eficacia de los sistemas y procesos de control interno, sobre los procesos de gestión del riesgo, cumplimiento y gobierno corporativo de la institución, ayudando con ello al Directorio y al Comité de Auditoría a proteger su organización y reputación.

El Auditor Interno debe:

22.1 Tener un mandato claro, rendir cuentas al Directorio y al Comité de Auditoría, ser independiente de las actividades auditadas.

22.2 Elaborar y someter a la aprobación del Comité de Auditoría un Estatuto de Auditoría Interna en el cual se establezcan los objetivos, funciones, autoridad, responsabilidades políticas de la Auditoría Interna, el cual sea aplicable también en caso de tercerización de tareas de Auditoría Interna.

22.3 Contar con los conocimientos y experiencia adecuados en forma individual y colectiva.

22.4 Cumplir con los estándares y prácticas internacionales de auditoría interna y con el código de ética pertinente.

22.5 Implementar procesos que aseguren que las pruebas, hallazgos y acciones correctivas son documentados adecuadamente y realizar un seguimiento proactivo de las debilidades encontradas

22.6 Desarrollar y presentar al Comité de Auditoría un plan anual de Auditoría basado en riesgos. El plan anual debe contener las metas, cronogramas, recursos humanos necesarios y sistema de reportes.

22.7 El alcance debe ser determinado en base a riesgos y debe cubrir todas las actividades de la entidad (incluso las tercerizadas)

22.8 Deberá evaluar la efectividad y eficiencia, al menos del:

- sistema de gestión integral de riesgos

- diseño y eficacia del marco de apetito de riesgo definido por el Directorio y sistema de información gerencial y sus procesos.
- los procesos de TI y de gestión de seguridad de la información.
- los controles internos
- la precisión y confiabilidad de los registros contables y los informes financieros y de gestión
- los sistemas diseñados para asegurar el cumplimiento de los requisitos legales, normativos y contractuales, así como del código de ética.
- la comprobación de la fiabilidad y oportunidad de los informes exigidos por el supervisor

22.9 Implementar el plan aprobado e informar al Comité de Auditoría sobre la existencia de desvíos significativos y el impacto de dichos desvíos sobre el cumplimiento de los objetivos establecidos.

22.10 Presentar sus informes de actuación con sus conclusiones y recomendaciones al Comité de Auditoría.

22.11 Mantener estrecha coordinación con otras estructuras de control (Síndico, Comisión Fiscal, etc.) que aseguren la cobertura de todas las actividades de la entidad.

AUDITORÍA EXTERNA

23. La Auditoría Externa debe aportar una seguridad razonable de que los estados financieros en su conjunto están libres de incorrección material, debido a fraude o error, que permita al auditor expresar una opinión sobre si los estados financieros están preparados, en todos los aspectos materiales, de conformidad con un marco de información financiera aplicable.

Para ello, la institución debe asegurar que el Auditor externo:

23.1 Designa un equipo de Auditoría conformado por un número adecuado de personas competentes y con experiencia para la función y con conocimiento del negocio.

23.2 Comprende su responsabilidad hacia la institución y todas las partes interesadas, especialmente hacia los afiliados y beneficiarios.

23.3 Actúa con objetividad e independencia en la planificación de las actividades y en la ejecución de la auditoría.

23.4 Reporta todos los hallazgos significativos y conclusiones de su trabajo tanto a la Dirección como al supervisor.

ESTÁNDARES DE GESTIÓN DE RIESGOS (R)

EL SISTEMA DE GESTIÓN INTEGRAL DE RIESGOS

Una competencia clave de las administradoras de fondos de ahorro previsional es su capacidad de gestionar los riesgos que asume, para sí y para el Fondo que administra, en forma prudente y rentable.

La administradora debe por lo tanto implementar un Sistema de Gestión Integral de Riesgos, definido como el conjunto de políticas, procedimientos y mecanismos de control implementados por la Institución para propiciar una apropiada identificación, medición, control y monitoreo de los riesgos que asume.

Para aquellas entidades que formen parte de un conglomerado, no siendo estas la entidad controlante, dentro de su gestión de riesgos deberán considerar el potencial impacto del vínculo con otras entidades del grupo, especialmente aquel proveniente de operaciones y exposiciones intra- grupo, contagios, y problemas reputacionales entre otros.

RIESGO DE CRÉDITO

El riesgo de crédito se define como la posibilidad de que el Fondo de Ahorro Previsional (o eventualmente la Administradora) vean afectado su patrimonio debido a la incapacidad de las contrapartes de cumplir con los términos originalmente pactados.

Para los fondos previsionales, el riesgo de contraparte se concentra en las operaciones con derivados (cuando el fondo resulta con posición activa) o en la liquidación de operaciones que no se realicen tal como fueron pactadas.

24. El Directorio debe aprobar las políticas para la gestión del riesgo de crédito.

Para ello el Directorio debe:

24.1 Aprobar las políticas de gestión del riesgo de crédito y revisarlas periódicamente, las cuales deben considerar la selección de contrapartes.

24.2 Establecer límites a nivel de contrapartes individuales y de contrapartes relacionadas entre sí (conjuntos económicos) y asignar facultades de aprobación, las que deberán ser consistentes con la capacidad y experiencia de los designados

24.3 Estar permanentemente informado de las contrapartes relevantes con problemas o potencialmente problemáticas.

24.4 Asegurar que la Alta Gerencia implementa procedimientos adecuados para que los riesgos asumidos sean consistentes con las políticas aprobadas y el riesgo se mantiene dentro de los límites establecidos.

25. La Alta Gerencia debe implementar las políticas aprobadas por el Directorio para el riesgo de crédito y desarrollar procedimientos para su identificación, medición, monitoreo y control.

Para ello, la Alta Gerencia debe asegurarse que:

25.1 Las actividades de la Institución respecto a las contrapartes son consistentes con la política establecida, existen procedimientos escritos, implementados efectivamente y las responsabilidades de aprobación y revisión de contrapartes se asignan clara y adecuadamente.

25.2 Se monitorean las exposiciones actuales frente a los límites fijados y se tienen procedimientos para incrementar el monitoreo y tomar medidas adecuadas si se acercan a los límites.

25.3 Identificar y monitorear las contrapartes con problemas y las potencialmente problemáticas (alerta temprana).

26. La institución debe implementar un sistema para administrar el riesgo de crédito, el cual debe ser consistente con el tamaño y el volumen de transacciones que realiza a Institución

Para ello, la Institución debe:

26.1 Contar con un sistema de medición de riesgo de crédito que incorpore las exposiciones con las contrapartes y que capture toda fuente material de riesgo.

26.2 Desarrollar un sistema de información que permita:

- suministrar información sobre todas las exposiciones con contrapartes

- comparar la información sobre contrapartes con los límites de riesgo establecidos e informar sobre excepciones a los mismos de manera oportuna y adecuada.

26.3 Contar con mecanismos que aseguren que las excepciones sean reportadas rápidamente, estén claramente documentadas y reciban la atención de la Alta Gerencia en forma oportuna.

RIESGOS DE MERCADO

El riesgo de mercado se define como la posibilidad que el Fondo de Ahorro Previsional (y/o eventualmente la Administradora) puedan sufrir pérdidas debido a movimientos adversos de las variables de mercado. Se identifican como riesgos de mercado:

- Riesgo de tasa de interés
- Riesgo de tipo de cambio

- Riesgo de reajuste
- Otros riesgos de mercado

a. RIESGO DE TASA DE INTERES

El riesgo tasa de interés es el riesgo asociado a las eventuales pérdidas en el valor de mercado del portafolio de inversiones originadas por movimientos adversos en las tasas de interés. Este riesgo tiene dos componentes:

- Riesgo Específico: Deriva de movimientos adversos en el valor de mercado del portafolio de inversiones originados en factores relacionados con los emisores de los instrumentos.
- Riesgo General: Proviene de movimientos adversos de precios originados por variaciones en las tasas de interés de mercado libres de riesgo. Este riesgo general tiene, a su vez, tres componentes básicos: el riesgo direccional, que mide la sensibilidad del precio de cada una de las posiciones, el riesgo de base, que contempla posibles compensaciones provenientes de posiciones con signos opuestos en una misma banda temporal y el riesgo de movimientos no paralelos en la curva, que mide las posibles compensaciones entre posiciones situadas con distintos horizontes temporales.

b. RIESGO DE TIPO DE CAMBIO

El riesgo tipo de cambio se define como la posibilidad de que el Fondo de Ahorro Previsional o el patrimonio de la sociedad se vean adversamente afectados por movimientos desfavorables en las tasas de cambio entre divisas.

c. RIESGO DE REAJUSTE

El riesgo de reajuste es el riesgo de que el Fondo de Ahorro Previsional o el patrimonio de la sociedad se vean adversamente afectados por movimientos en los tipos de cambio de las unidades de cuenta en moneda nacional en un horizonte de largo plazo.

d. OTROS RIESGOS DE MERCADO

Los otros riesgos de mercado se definen como la posibilidad de que el Fondo de Ahorro Previsional o el patrimonio de la sociedad se vean adversamente afectados por movimientos adversos en el precio de acciones, y otros activos de la economía real asociados a rendimientos de instrumentos financieros.

27. El Directorio debe aprobar la estrategia y las políticas para la gestión de los riesgos de mercado, la cual debe reflejar el apetito de riesgo de la institución.

Para ello el Directorio debe:

27.1 Aprobar la estrategia y las políticas de gestión del riesgo de mercado asumido por la institución para el fondo que administra y para sí misma y revisarlas periódicamente. Estas políticas deben:

- ser consistentes con el volumen de las actividades.
- definir los tipos, niveles y límites de riesgos aceptables
- prever mecanismos de identificación y notificación de excepciones a las mismas

27.2 Asegurar que la institución cuenta con una estructura organizacional adecuada para la gestión del riesgo de mercado.

27.3 Identificar líneas de responsabilidad y autoridad en la gestión del riesgo de mercado.

27.4 Contar con información suficiente, detallada y oportuna sobre los riesgos de mercado, de forma que permita comprender los riesgos asumidos y evaluar el desempeño de la Alta Gerencia en el monitoreo y control de dichos riesgos

27.5 Asegurar que la Alta Gerencia implementa las políticas y procesos necesarios para que los riesgos asumidos sean consistentes con las políticas aprobadas y el riesgo se mantiene dentro de los límites establecidos.

28. La Alta Gerencia debe implementar la estrategia y las políticas aprobadas por el Directorio para la gestión del riesgo de mercado y desarrollar procedimientos para su identificación, medición, monitoreo y control.

Para ello, la Alta Gerencia debe:

28.1 Implementar las políticas y desarrollar procedimientos para gestionar los riesgos de mercado en el corto, mediano y largo plazo, de forma consistente con la estrategia y las políticas definidas.

28.2 Asignar claramente las funciones, responsabilidades y atribuciones en materia de identificación, aprobación, medición y control del riesgo de mercado.

28.3 Asignar los recursos necesarios en cantidad, calidad y competencia a efectos de un buen manejo del riesgo de mercado.

28.4 Asegurar que existan mecanismos efectivos de control y de corresponder, asegurar controles eficaces sobre los modelos utilizados para identificar y cuantificar los riesgos de mercado.

28.5 Implementar un sistema de límites que asegure que las exposiciones a los riesgos se mantienen dentro de las políticas aprobadas por el Directorio.

28.6 Implementar un sistema para asegurar la medición correcta de los riesgos.

28.7 Definir una metodología para valuar posiciones y medir el desempeño.

28.8 Revisar periódicamente las políticas y procedimientos para asegurar que siguen siendo adecuados y prudentes.

28.9 Desarrollar un sistema de información que permita una oportuna y correcta agregación y notificación al Directorio de las exposiciones al riesgo de mercado así como que permita evaluar la efectividad de gestión del riesgo.

28.10 Contar con un proceso para analizar nuevos instrumentos financieros, que asegure que los riesgos financieros asociados son comprendidos e incorporados al proceso de gestión de riesgos.

29. La institución debe tener un sistema de medición de riesgo de mercado que capture toda fuente material de riesgo tasa de interés, tipo de cambio, reajuste y otros riesgos de mercado y evaluar el impacto de los mismos sobre el Fondo Previsional y la institución. Los supuestos subyacentes en dichos sistemas deben ser comprendidos claramente por el Directorio y la Alta Gerencia.

El sistema debe:

29.1 Evaluar el impacto de los cambios en los resultados y en el valor económico de los activos que gestiona

29.2 Identificar excesos en límites establecidos.

29.3 Asegurar que los supuestos están claramente documentados y que pueden ser comprendidos por la Alta Gerencia. Dichos supuestos deben ser revisados por lo menos anualmente.

29.4 Utilizar conceptos financieros y técnicas de medición de riesgos de mercado generalmente aceptados.

29.5 Tener un grado de detalle y complejidad que sea consistente con el nivel de riesgo asumido.

30. La institución debe tener un sistema adecuado para el monitoreo y control de los riesgos de mercado

30.1 Para ello el sistema de monitoreo y control debe:

- Controlar los límites aprobados
- Incluir procedimientos y metodologías de control claramente establecidas y definidas.

Asimismo se deberá:

30.2 Asegurar que las posiciones que exceden los niveles predefinidos reciben la atención de la Alta Gerencia en forma oportuna.

31. La institución debe establecer y realizar controles para asegurar que las excepciones en las políticas, los procedimientos y límites son identificadas y reportadas oportunamente al nivel jerárquico apropiado

Para ello, la institución debe:

31.1 Contar con mecanismos de control interno que aseguren que la gestión del riesgo de mercado se realiza de acuerdo con las políticas y procedimientos definidos por el Directorio y Alta Gerencia.

31.2 Establecer procedimientos de identificación, monitoreo, documentación y notificación de excepciones a las políticas y límites establecidos.

31.3 Asegurar que las posiciones que exceden niveles predefinidos reciban la atención de la Alta Gerencia en forma oportuna.

32. La institución debe contar con un sistema de información gerencial que suministre información adecuada y oportuna sobre las exposiciones a los riesgos de mercado al Directorio y la Alta Gerencia

Un sistema informativo, fiel y oportuno es esencial para gestionar las exposiciones de riesgos de mercado y asegurar el cumplimiento con las políticas establecidas por el Directorio.

Para ello, el sistema debe:

32.1 emitir reportes en forma regular y comparar las exposiciones con los límites establecidos.

32.2 incluir una comparación de las proyecciones con los resultados reales para permitir la identificación de limitaciones o errores en los modelos.

32.3 prever que los reportes que emite sean revisados por el Directorio y la Alta Gerencia.

RIESGO DE LIQUIDEZ

El riesgo de liquidez es la posibilidad de que el Fondo de Ahorro Previsional o la Administradora no cuenten con suficientes activos líquidos para hacer frente a las obligaciones asumidas. El riesgo de liquidez depende de dos dimensiones definidas como el riesgo de liquidez de fondeo (Pasiva) y el riesgo de liquidez de mercado (Activa) y de la correlación existente entre las mismas.

- Riesgo de liquidez de fondeo - Incluye la incapacidad de la institución de gestionar bajas o cambios inesperados en los flujos de fondos. A menudo esto puede causar la liquidación prematura de parte de sus activos.

- Riesgo de liquidez de mercado - Proviene de las dificultades derivadas de los cambios en las condiciones de mercado que afecten la rápida liquidación de los activos con una mínima pérdida de valor.

Para las **AFAP** el riesgo de liquidez está asociado a los ciclos laborales de los afiliados (retiros), y a decisiones de los mismos (traspasos y desafiliaciones).

Por estos motivos, la dimensión más relevante es la de mercado, en cuanto la Administradora debe estructurarse de modo que tenga suficientes activos líquidos o de fácil realización como para cubrir sus obligaciones cuando son exigibles. La dimensión pasiva es de menor relevancia, sin embargo la Administradora debería tener una estructura de portafolio adecuada para hacer frente a flujos de salida inesperados.

33. El Directorio debe aprobar la estrategia y las políticas para la gestión del riesgo de liquidez del Fondo de Ahorro Previsional y de la Institución.

Para ello, el Directorio debe:

33.1 Aprobar la estrategia y las políticas de gestión del riesgo de liquidez y revisarlas periódicamente.

33.2 Aprobar y revisar periódicamente los planes de contingencia de la Institución para enfrentar eventuales problemas de liquidez.

33.3 Asegurar que la institución cuenta con una estructura organizacional adecuada para la gestión del riesgo de liquidez.

33.4 Identificar líneas de responsabilidad y autoridad en la gestión del riesgo de liquidez.

33.5 Contar con información suficiente, detallada y oportuna sobre el riesgo de liquidez de forma que permita comprender los riesgos asumidos y evaluar el desempeño de la Alta Gerencia en el monitoreo y control de dicho riesgo

33.6 Asegurar que la Alta Gerencia implementa las políticas y los procedimientos necesarios para que los riesgos asumidos sean consistentes con las estrategias y políticas aprobadas.

34. La Alta Gerencia debe implementar la estrategia y las políticas aprobadas por el Directorio para el riesgo de la liquidez y desarrollar procedimientos para su identificación, medición, monitoreo y control.

Para ello, la Alta Gerencia debe:

34.1 Implementar las políticas y desarrollar procedimientos específicos para la gestión de liquidez que tengan en cuenta el marco definido de gestión de activos y las proyecciones de egresos futuros de fondos.

34.2 Definir los responsables de la administración del riesgo de liquidez y el mecanismo a través del cual se implementa la política de liquidez y se revisan las decisiones tomadas sobre la posición de liquidez

34.3 Asignar los recursos necesarios en cantidad, calidad y competencia a efectos de un buen manejo del riesgo de liquidez.

34.4 Implementar un sistema de límites que asegure que la liquidez se mantiene dentro de las políticas aprobadas por el Directorio.

34.5 Desarrollar planes de contingencia para hacer frente a flujos de salida inesperados.

35. La institución debe establecer un sistema de medición y monitoreo continuo de los requerimientos netos de fondos.

Para ello el sistema debe:

35.1 Tener la capacidad de calcular las posiciones de liquidez a corto y mediano plazo y en situaciones de stress

35.2. Ser lo suficientemente flexible como para enfrentar variadas contingencias que puedan surgir.

36. La institución debe definir mecanismos de control que aseguren el cumplimiento de los límites de liquidez definidos y contar con un proceso adecuado para la identificación y tratamiento de las excepciones.

Para ello, la institución debe:

36.1 Contar con mecanismos de control interno que aseguren que el manejo del riesgo de liquidez se realiza de acuerdo con las políticas y procedimientos definidos por el Directorio y Alta Gerencia.

36.2 Establecer procedimientos de identificación, monitoreo, documentación y notificación de excepciones a las políticas y límites establecidos

36.3 Asegurar que las posiciones que exceden niveles predefinidos reciban la atención de la Alta Gerencia de forma oportuna.

37. La institución debe contar con sistemas de información adecuada y oportuna para monitorear, controlar e informar el riesgo de liquidez. Los informes deben entregarse periódicamente al Directorio y Alta Gerencia.

Para ello, el sistema debe:

37.1 Emitir información en forma regular que permita el control de exposiciones al riesgo de liquidez actuales en relación a los límites establecidos.

37.2 Permitir una evaluación del nivel de riesgo de liquidez del Fondo Previsional y de la Institución.

RIESGO OPERACIONAL

El riesgo operacional se define como la posibilidad de que el patrimonio del Fondo de Ahorro Previsional o de la Administradora se vea afectado por pérdidas resultantes de procesos, personal o sistemas internos inadecuados o defectuosos, o por eventos externos. Incluye además el riesgo de cumplimiento, es decir, la posibilidad de que una entidad se vea afectada por violaciones a las leyes, regulaciones, estándares y prácticas de la industria o estándares éticos. Este riesgo también aparece en situaciones en donde las leyes o regulaciones que rigen ciertos productos o actividades son ambiguas.

El riesgo operacional acompaña el desarrollo y evolución de los servicios y los procesos transaccionales, está vinculado al desarrollo de sistemas (en particular sistemas de computación) y guarda relación con la calidad del personal y el ambiente de control interno. Es un riesgo diferente a otros, como el riesgo de crédito o de mercado, ya que no se asume riesgo operacional con el objetivo de obtener un retorno, sino que surge de la actividad normal de la entidad y afecta el manejo integral de riesgos.

La entidad puede tener su propia definición del riesgo operacional, pero cualquiera sea ésta, es crítico que exista una comprensión del concepto por parte de la entidad para su manejo efectivo.

Sin perjuicio de ello, la institución debe asignar los recursos necesarios, definir claramente responsabilidades, tener independencia operativa para el ejercicio de la función y estar sujeta a revisiones periódicas por parte de la Auditoría Interna.

38. El Directorio debe aprobar los principios generales para el manejo del riesgo operacional, el apetito al riesgo y las políticas significativas de la institución, y revisarlos periódicamente. Asimismo, debe revisar regularmente la exposición al riesgo operacional y asegurar que los niveles de riesgos se encuentran dentro del marco establecido.

Para ello, el Directorio debe:

38.1 Aprobar las políticas en relación al riesgo operacional y revisarlas periódicamente. Estas políticas deben ser consistentes con el apetito de riesgo definido.

Las mismas deben:

- Reconocer el riesgo operacional, (el cual incluye el riesgo de cumplimiento) como un riesgo que la entidad debe manejar explícitamente.
- Constituir una guía clara en relación al control de este riesgo y asegurar que todo el personal está comprometido con dichas actividades de control.

- Asegurar que todo el personal está comprometido con dichas actividades de control

38.2 Promover una cultura de control adecuada en la organización y el cumplimiento de las leyes, regulaciones, prácticas de la industria y estándares éticos

38.3 Asegurar que la gestión del riesgo operacional se lleva a cabo en forma continua.

38.4 Revisar periódicamente la efectividad de la gestión del riesgo operacional.

38.5 Asegurar que se cuenta con una estructura organizacional adecuada para la gestión del riesgo operacional.

38.6 Identificar líneas de responsabilidad y autoridad en la gestión del riesgo operacional.

38.7 Aprobar las políticas en relación a seguridad de la información y revisar periódicamente la efectividad de su implementación.

Las mismas deben:

- Reconocer explícitamente los riesgos vinculados a la gestión de activos de información.
- Constituir una guía clara en relación a la gestión de seguridad de la información.
- Promover una adecuada cultura de seguridad de la información.

38.8 Contar con información suficiente, detallada y oportuna sobre el riesgo operacional de forma que le permita comprender los riesgos asumidos y evaluar el desempeño de la Alta Gerencia en el monitoreo y control de dicho riesgo.

38.9 Asegurar la realización de revisiones independientes para que en forma periódica se validen los procesos, las políticas, los procedimientos. Asegurar que se instrumenten las acciones apropiadas ante las debilidades o fallas significativas detectadas por el auditor interno, externo, supervisor o profesional independiente.

38.10 Asegurar que la Alta Gerencia implemente las políticas y los procesos necesarios para que los riesgos asumidos sean consistentes con las políticas aprobadas.

39. La Alta Gerencia debe implementar las políticas aprobadas por el Directorio y desarrollar procedimientos apropiados para su identificación, medición, monitoreo y control del riesgo operacional. Estas políticas y procedimientos deben considerar el riesgo operacional en todas las actividades de la institución.

Para ello, la Alta Gerencia debe:

39.1 Implementar las políticas y desarrollar procedimientos para gestionar el riesgo operacional, de forma consistente con las políticas definidas.

39.2 Asignar responsabilidades en forma explícita para el manejo del riesgo operacional, independientemente de la estructura organizacional que se defina. En particular, se asignan y definen roles y responsabilidades sobre la seguridad de la información.

39.3 Asignar los recursos necesarios en cantidad, calidad y competencia a efectos de un buen manejo del riesgo operacional.

39.4 Identificar adecuadamente las fuentes potenciales de riesgo operacional y en consecuencia establecer mecanismos que mitigan este riesgo.

39.5 Establecer que la función de seguridad de la información debe ser independiente funcional y presupuestalmente del área de TI.

39.6 Asegurar que en la revisión de procesos, se considera el riesgo operacional en forma explícita.

39.7 Revisar periódicamente las políticas y procedimientos para asegurar que siguen siendo adecuados y prudentes.

39.8 Desarrollar un sistema de información que permita una oportuna y correcta notificación al Directorio del riesgo operacional así como que permita evaluar la efectividad de gestión del riesgo.

40. La Alta Gerencia debe implementar las políticas y desarrollar procedimientos apropiados para la identificación, medición, monitoreo y control del riesgo de cumplimiento y reportar al Directorio sobre el manejo de este riesgo.

Para ello, la Alta Gerencia debe:

40.1 Asignar responsabilidades en forma explícita para el manejo del riesgo de cumplimiento, independientemente de la estructura organizacional que se defina.

40.2 Identificar adecuadamente las fuentes potenciales de riesgo de cumplimiento, y en consecuencia establecer mecanismos que mitigan este riesgo.

40.3 Asegurar que el Directorio reciba en forma periódica información sobre la efectividad de la función de cumplimiento y en particular, cualquier aspecto que represente un riesgo de cumplimiento significativo.

40.4 Asegurar que exista un proceso que asegure el cumplimiento con las leyes y las regulaciones bancocentralistas.

40.5 Revisar periódicamente las políticas y procedimientos para asegurar que siguen siendo adecuados y prudentes.

40.6 Desarrollar un sistema de información que permita una oportuna y correcta agregación y notificación al Directorio del riesgo operacional y de cumplimiento así como que permita evaluar la efectividad de gestión del riesgo.

41. La institución debe contar con procedimientos de identificación, medición y evaluación de las fuentes de riesgo operacional y definir los mecanismos para mitigar dichos riesgos

Para ello, la institución debe:

41.1 Realizar un mapeo de los distintos procesos y revisarlo periódicamente.

41.2 Establecer algún mecanismo de auto evaluación de riesgos a nivel de los distintos procesos operativos de la entidad y definir los controles orientados a mitigar dichos riesgos.

41.3 Involucrar al personal vinculado a los distintos procesos en este mecanismo de auto evaluación.

41.4 Llevar un registro de los eventos de riesgo operacional que permita su consolidación y análisis.

41.5 Llevar un registro de las incidencias generadas en el proceso de atención a los afiliados y beneficiarios.

41.6 Generar un sistema de indicadores que alerten sobre debilidades en los procesos.

41.7 Contar con procedimientos que permitan asegurar el cumplimiento con las leyes, normas e instrucciones emitidas por entes reguladores.

41.8 Informar los resultados de las distintas herramientas de gestión de riesgo operacional a la Auditoría Interna y al Comité de Auditoría y comunicarlas al personal involucrado.

42. La institución debe implementar procedimientos de control y monitoreo del riesgo operacional.

Para ello la institución debe:

42.1 Asegurar que exista un estrecho contacto entre las estructuras de control, y se intercambie información sobre el resultado de las actuaciones de cada una de ellas.

42.2 Asegurar que los procesos (o partes de ellos) que se encuentren tercerizados están adecuadamente controlados.

42.3 Asegurar que existan reportes periódicos al Directorio sobre la eficacia de las políticas implementadas.

43. El área de TI debe proporcionar los servicios en un ambiente seguro, que incluya no solamente las condiciones operativas del área de TI sino también factores tales como confiabilidad, confidencialidad, integridad y disponibilidad. Incluye además el soporte y la capacitación a los usuarios del servicio y la habilidad para manejar problemas e incidentes, operaciones, desempeño del sistema, planificación de la capacidad y administración de los datos e instalaciones.

Las prácticas de manejo de riesgos promoverán operaciones de TI efectivas, seguras y sólidas, que aseguren la continuidad de las operaciones y la confiabilidad y disponibilidad de la información. El manejo del riesgo operacional derivado de los sistemas debe comprender a toda la organización y proveedores externos.

Debe asegurar que se cumpla con los siguientes requerimientos:

43.1 Proporcionar un nivel de servicio que satisfaga las necesidades del negocio.

43.2 Establecer controles adecuados de los datos a nivel de la operación, entradas, proceso y salidas.

43.3 Asegurar la calidad de los procesos y/o los programas que monitorean la capacidad y el desempeño del servicio de TI.

43.4 Asegurar la calidad de la asistencia proporcionada a los usuarios, incluida la habilidad para manejar problemas.

43.5 Contar con adecuadas políticas operativas, procedimientos y manuales.

43.6 Contar con una arquitectura adecuada y asegurar las conexiones con redes de comunicación.

En el caso de servicios prestados por terceros, debe asegurar que:

43.7 Se han documentado adecuadamente a través de contratos, las condiciones y niveles mínimos de servicio a ser obtenidos del proveedor.

43.8 Se han establecido controles adecuados sobre los proveedores externos y que la institución es capaz de monitorear los mismos.

43.9 El servicio a los requerimientos de los usuarios es adecuado.

43.10 El proveedor es capaz de proveer y mantener el desempeño de los niveles de servicios adecuado a las necesidades de los usuarios.

44. La institución debe contar con un plan de contingencia y de continuidad de los negocios que permita operar ante la ocurrencia de eventos externos severos.

Para ello debe:

44.1 Contar con un Análisis de Impacto al Negocio con el cual se identifiquen las actividades críticas de la institución.

44.2 Establecer planes que ante distintos escenarios de desastre, aseguren la continuidad del negocio. Los mismos deben diseñarse para permitir la recuperación de las operaciones y para no interrumpir el servicio prestado por los centros de procesamiento de datos, redes y proveedores externos y en las áreas de trabajo.

44.3 Abarcar en sus planes la continuidad de los servicios tercerizados.

44.4 Establecer planes de respaldo de información que aseguren su recuperabilidad.

44.5 Revisar periódicamente la aplicabilidad de estos planes. Para esto, se debe realizar una prueba (paralela o completa) del plan por lo menos anualmente, debidamente documentada y analizada al culminarse.

45. La institución debe contar con una gestión integral e independiente de la seguridad de la información.

Para ello debe:

45.1 Mantener actualizada la clasificación de sus activos de información. Debe asignarse dueño y custodio a todo dato y software necesario para reconstruir las informaciones emitidas para el Banco Central del Uruguay, los registros contables y cada uno de los movimientos que dan origen a los mismos (hasta el grado de detalle establecido en la normativa vigente).

45.2 Implementar estándares, procedimientos y directrices que permitan preservar la confidencialidad, integridad y disponibilidad de la información, teniendo en cuenta aspectos de seguridad física y lógica.

45.3 Identificar, evaluar, tratar y monitorear los riesgos asociados a la gestión de sus activos de información, de manera que se incluya un análisis sobre las amenazas y vulnerabilidades presentes.

45.4 Contar con indicadores y medidas que contribuyan al monitoreo de la gestión de la seguridad de la información.

45.5 Generar concientización y asegurar una adecuada capacitación al personal que permita involucrar a todos en la gestión de los riesgos asociados a los activos de información.

45.6 Asegurar el cumplimiento de las políticas de seguridad de la información en el caso de actividades tercerizadas, y velar por la seguridad de los datos procesados externamente.

45.7 Contar con una política, procedimientos e indicadores de gestión de incidentes de seguridad, y llevar a cabo pruebas frecuentemente de manera de tener actualizados las actividades a realizar.

46. La función de cumplimiento debe contar con mecanismos para identificar, medir, controlar y monitorear el riesgo de cumplimiento asumido.

Para ello debe:

46.1 Asesorar al Directorio y a la Alta Gerencia del cumplimiento por parte de la institución de las leyes, normativas y estándares aplicables.

46.2 Contar con la suficiente autoridad, importancia, independencia, recursos y acceso al Directorio

46.3 Promover y participar activamente en la capacitación de todos los funcionarios en materia de cumplimiento, actuar de punto de contacto para preguntas sobre cumplimiento y guiar sobre la aplicación adecuada de las leyes, normas, estándares aplicables, políticas y procedimientos, códigos de ética y de buenas prácticas.

46.4 Implementar mecanismos para identificar y evaluar el riesgo de cumplimiento existente en las distintas actividades de la entidad, incluyendo los productos nuevos, las propuestas de nuevos tipos de negocios o cualquier cambio en las características del relacionamiento con los clientes.

46.5 Establecer mecanismos para medir el riesgo de cumplimiento y usar estas medidas para mejorar el manejo de este riesgo. Algunos indicadores pueden ser utilizados con el apoyo tecnológico respectivo, para identificar y medir potenciales problemas de cumplimiento.

46.6 Implementar mecanismos para monitorear la efectividad de las políticas mediante pruebas sobre el cumplimiento.

46.7 Reportar al Directorio sobre los resultados del monitoreo y en general, sobre el perfil general del riesgo de cumplimiento basado en los indicadores definidos.

47. La información suministrada al supervisor debe ser confiable y oportuna y debe existir un responsable en la organización por su elaboración y presentación.

La información suministrada por la entidad es un insumo básico para que el supervisor pueda cumplir con sus responsabilidades. Por tanto, la calidad de dicha información es fundamental y constituye un elemento esencial en la definición del alcance de las actividades que debe desarrollar.

Los sistemas de contabilidad y procedimientos utilizados son un elemento crítico en la evaluación del perfil de riesgos de una institución y de su condición financiera y patrimonial.

Para que el proceso de generación de información al supervisor sea confiable debe:

47.1 Tener políticas y procedimientos claros sobre el tratamiento contable consistente con los requisitos regulatorios y los estándares internacionales.

47.2 Asegurar que los procesos de contabilización son eficaces y controlados evitando el diferimiento en la contabilización de las operaciones.

47.3 Existir un proceso automatizado de generación de información, donde ésta fluya naturalmente desde las transacciones a los productos finales de información.

47.4 Estar dotado de un sistema de controles adecuados (separación de funciones, actividades de control, reportes, etc.).

47.5 Contar con recursos suficientes y capacitados para llevar adelante la tarea en tiempo y forma.

47.6 Estar sometido a revisiones independientes periódicas por parte de la Auditoría Interna.

47.7 Contar con un responsable por la generación de información hacia el exterior de la administradora (tanto para el supervisor como para cualquier usuario externo).

48. La institución debe establecer mecanismos de revisión independiente y periódica del proceso del riesgo operacional. Los resultados de las revisiones deben ser reportados directamente al Directorio y a la Alta Gerencia.

La revisión independiente debe incluir la evaluación de:

48.1 El sistema en su conjunto y su eficacia en el cumplimiento de los objetivos.

48.2 El cumplimiento efectivo de las políticas y procedimientos y la adecuada documentación de los procesos y las decisiones adoptadas.

48.3 La organización y la suficiencia de los recursos humanos en cuanto a número y competencia técnica para gestionar en forma correcta el riesgo.

48.4 La capacidad y eficacia del sistema para capturar todos los elementos materiales de riesgo.

48.5 La confiabilidad y corrección en el procesamiento, agregación y cotejo de los datos.

48.6 Los cambios significativos que puedan afectar la efectividad de los controles, como cambios en los mercados, recursos humanos, tecnología o estructuras de cumplimiento.

48.7 La calidad de las revisiones y si son llevadas a cabo por individuos independientes de las áreas sujetas a revisión y con la formación y experiencia suficientes y si existe un proceso de seguimiento y corrección de hallazgos significativos por parte de la Alta Dirección y el Directorio.

RIESGO DE LAVADO DE ACTIVOS Y FINANCIAMIENTO DEL TERRORISMO (LA/FT)

El riesgo de Lavado de Activos y Financiamiento del Terrorismo refiere a la posibilidad de pérdida o daño que puede sufrir un Fondo de Ahorro Previsional o la Administradora al ser utilizada directamente o a través de sus operaciones como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades.

A efectos de mitigar estos riesgos, las instituciones deberán instrumentar un sistema que abarque políticas, prácticas y procedimientos que le permitan prevenirse de ser utilizada como instrumento para el lavado de activos.

49. El Directorio debe aprobar las políticas en relación al riesgo de Lavado de Activos y Financiamiento del Terrorismo.

Para ello, el Directorio debe:

49.1 Aprobar políticas que:

- Promuevan la conciencia y el compromiso de todo su personal de evitar ser utilizados para el LA/FT mediante un Código de Ética.
- Permitan prevenir y detectar operaciones que puedan estar relacionadas con la legitimación de activos provenientes de actividades delictivas,
- Definir criterios para la notificación de las actividades sospechosas al supervisor
- Definan directivas claras en cuanto al relacionamiento con los afiliados y beneficiarios en función de su grado de riesgo
- Establezcan mecanismos de revisión periódicos sobre las mismas.

50. La Alta Gerencia debe implementar las políticas aprobadas por el Directorio en relación al riesgo de lavado de activos y financiamiento del terrorismo.

Para ello, la Alta Gerencia debe:

50.1 Implementar:

- procedimientos para la administración del riesgo LA/FT, que permitan identificar, medir, monitorear y controlar el riesgo como así también reportar las operaciones sospechosas o inusuales.
- procedimientos que permitan atender los requerimientos de información por parte de las autoridades competentes.

50.2 Revisar periódicamente los procedimientos de forma de asegurar que continúan siendo adecuados

50.3 Asegurar que el Código de Ética aprobado es conocido y aplicado por toda la organización y refleja el compromiso institucional con la prevención de su utilización para el lavado de activos,

50.4 Asegurar que el personal comprenda su rol en el sistema de prevención y esté en conocimiento de los procedimientos y controles internos diseñados de forma de mitigar el riesgo de LA/FT.

RIESGO DE REPUTACIÓN

El riesgo de reputación se define como el riesgo presente y futuro de que el patrimonio del Fondo de Ahorro Previsional o las ganancias o el patrimonio de la Administradora se vean afectados por una opinión pública negativa. Afecta la capacidad de la institución de establecer vínculos con nuevos cotizantes, o continuar sirviendo las relaciones ya existentes. Este riesgo puede exponer a la institución a juicios, pérdidas financieras o a una disminución de la base de afiliados. La exposición al riesgo de reputación incluye la responsabilidad de tener amplia precaución al tratar con los afiliados (reales o potenciales) y beneficiarios y con la comunidad.

El riesgo de reputación no es fácilmente cuantificable pero aparece en todas las relaciones con los afiliados (reales o potenciales) y beneficiarios, en particular aquellas que aparejan asesoramiento y manejo de información confidencial de los mismos.

51. El Directorio debe aprobar y revisar periódicamente las políticas vinculadas al manejo de las relaciones con los afiliados y beneficiarios vinculados a la Administradora, que incluyan formalmente el manejo de la información de los mismos, una gestión adecuada de las actividades de asesoramiento y la atención de los mismos.

Para ello, el Directorio debe:

51.1 Aprobar las políticas en relación al riesgo de reputación. Estas políticas deben reconocer el riesgo de reputación que subyace en el relacionamiento con los afiliados y beneficiarios como un riesgo que la entidad debe manejar explícitamente.

51.2 Establecer políticas claras con relación a los afiliados y beneficiarios que incluyan:

- el trato a los mismos de forma justa procurándoles información oportuna y relevante sobre sus cuentas de ahorro individual, sus derechos, y las proyecciones de su futura renta vitalicia.

- el establecimiento de un proceso formal para reclamaciones, en particular para los casos de afiliaciones viciadas, que impliquen una rápida solución al afiliado afectado y las medidas

pertinentes respecto al promotor interviniente, así como la investigación de la cartera de afiliaciones del mismo.

51.3 Establecer políticas claras de relacionamiento con terceros (proveedores más relevantes incluyendo tercerizaciones)

51.4 Asegurar el cumplimiento de las políticas definidas en relación al riesgo de reputación.

51.5 Revisar periódicamente la efectividad de estas políticas.

52. La Alta Gerencia debe implementar y comunicar las políticas definidas, asegurar que las mismas se cumplen y reportar al Directorio sobre el manejo de este riesgo.

Para ello la Alta Gerencia debe asegurar que:

52.1 Se identifican adecuadamente las fuentes potenciales de riesgo de reputación y en consecuencia, se establecen mecanismos que mitigan o eliminan este riesgo.

52.2 Se diseñan procedimientos para el adecuado asesoramiento a los afiliados y beneficiarios y la atención de reclamos.

52.3 Existe un responsable del funcionamiento del servicio de atención de reclamos de clientes, que cuenta con los recursos necesarios y se provee entrenamiento continuo al personal relevante en esta tarea.

52.4 Existen mecanismos de evaluación independientes de la efectividad de las políticas definidas en torno al relacionamiento con los clientes. La Auditoría Interna deberá incluir entre sus actividades la evaluación del funcionamiento del servicio de atención al cliente, en particular, la adhesión a las políticas y procedimientos definidos, la naturaleza y cantidad de reclamos recibidos y las operativas o servicios que puedan presentar problemas extendidos de malas prácticas.

52.5 Se manejan los riesgos derivados del manejo de información sensible o confidencial por parte de los proveedores de servicios tercerizados, cuando existen.

52.6 Se aplican efectivamente los procedimientos de atención de reclamos establecidos.

52.7 Existe una adecuada difusión del servicio de atención al cliente en las oficinas de la institución, en la documentación y en el sitio de Internet de la entidad.

52.8 Existen reportes al Directorio en forma periódica sobre cualquier aspecto que represente un riesgo de reputación significativo, en particular en lo que refiere a los resultados de la gestión del servicio de atención al cliente.

ESTANDARES DE TECNOLOGIA (T)

Los estándares para la evaluación de las áreas de Tecnología de Información (TI) tienen como base el conjunto de principios conocido como CobiT, en particular los vinculados al dominio de Adquisición e Implementación. Los restantes dominios han sido contemplados en los estándares de Gobierno Corporativo y de Riesgo Operacional.

53. La Gerencia o el Responsable de TI debe tener la habilidad para identificar las necesidades y para desarrollar, adquirir, instalar y mantener soluciones de TI apropiadas de acuerdo a las necesidades de la entidad.

Para ello debe:

53.1 Tener procesos para identificar necesidades e implementar, controlar y mantener soluciones de TI adecuadas. Esto incluye compras de hardware o software realizadas por el proveedor interno o externo de TI, desarrollo y programación realizado por la institución o un proveedor externo, compra de servicios a vendedores independientes, centros de procesamiento de datos vinculados a la institución o una combinación de estas actividades.

53.2 Implementar una metodología de desarrollo de sistemas de la institución que incluye un análisis y gestión adecuada de los riesgos tecnológicos asociados.

53.3 Implementar procesos que aseguren que se mejoran y reemplazan componentes de TI en forma prudente y dentro de un ambiente controlado. El comportamiento en el desarrollo, adquisición y en el manejo de los riesgos asociados debe basarse en la evaluación de factores como:

- El nivel y calidad de la supervisión y soporte al desarrollo y adquisición de sistemas por parte de la dirección.
- La adecuación de las estructuras organizacionales y gerenciales para establecer conocimiento y responsabilidad por las iniciativas en materia de sistemas y tecnologías de TI.
- El volumen, naturaleza y extensión de la exposición al riesgo de la institución en el área del desarrollo y adquisición de sistemas.
- La adecuación de los estándares de desarrollo, ciclo de vida y programación de los sistemas de la institución.
- La calidad de las prácticas de administración de proyectos que son seguidos por los desarrolladores, operadores, nivel gerencial/propietario (entendiendo por propietario al usuario final dueño de la aplicación), vendedores independientes o proveedores vinculados (entendiéndose por proveedor vinculado a una empresa externa vinculada al grupo) de servicios de TI y los usuarios finales.
- La independencia de la función de aseguramiento de calidad y la adecuación de los controles sobre los cambios de programas.

- La calidad y exactitud de la documentación de los sistemas.
- La integridad y seguridad del software de red, de base y aplicaciones.
- El desarrollo de soluciones de TI que satisfagan las necesidades de los usuarios finales.
- El grado de compromiso del usuario final en el proceso de desarrollo de los sistemas.

53.4 Tener un proceso que comprende todas las fases necesarias para implementar un cambio de sistemas incluyendo investigación de las alternativas disponibles, selección de la opción más adecuada para la organización como un todo, conversión a un nuevo sistema o integración de un nuevo sistema con los existentes.

53.5 Evaluar en los proveedores externos de servicios de TI los aspectos vinculados a la calidad de las entregas de software y documentación, y a la adecuación de la capacitación proporcionada a los clientes.