Superintendencia de Pensiones

S P DDN
N° 246
Recepcionado Of. Partes
1 de Julio de 2019

NORMA DE CARÁCTER GENERAL N°

REF.: MODIFICA EL LIBRO V, SOBRE ASPECTOS ADMINISTRATIVOS Y OPERACIONALES DE LAS ADMINISTRADORAS DE FONDOS DE PENSIONES Y DEL INSTITUTO DE PREVISIÓN SOCIAL, DEL COMPENDIO DE NORMAS DEL SISTEMA DE PENSIONES.

Santiago,

En uso de las facultades legales que confiere la ley a esta Superintendencia, en particular, el artículo 47 N° 6 de la Ley N° 20.255, se introducen las modificaciones contenidas en la presente Norma de Carácter General, al Libro V del Compendio de Normas del Sistema de Pensiones.

I. Agrégase el siguiente Título XVII nuevo, en el Libro V del Compendio de Normas del Sistema de Pensiones:

"Título XVII. Instrucciones sobre Administración de Riesgo en el Instituto de Previsión Social

Capítulo I. Introducción

En el presente Título, la Superintendencia de Pensiones establece los principios y lineamientos generales que en términos de buenas prácticas se espera que el Instituto de Previsión Social, en adelante "el IPS", adopte en la gestión de sus riesgos, sin perjuicio de los lineamientos emanados del Consejo de Auditoría Interna General de Gobierno (CAIGG). El propósito es que el IPS identifique desafíos y se adapte para enfrentarlos, para lo cual debe conocer y documentar las oportunidades y riesgos que enfrenta, y administrarlos adecuadamente a través de la implementación de un modelo de gestión de riesgos que integre la gobernanza, la gestión del desempeño y prácticas de control interno, incentivando de esta manera una cultura de gestión de riesgos acorde a su particular naturaleza y contexto.

En relación con la cultura de Gestión de Riesgos, el Director Nacional tiene la responsabilidad principal de la supervisión y la mejora continua de la gestión del riesgo, siendo esencial que esta gestión se integre en el plan estratégico. A su vez, el

Director Nacional debe mantenerse informado sobre aquellos asuntos relevantes que afecten y puedan impactar en el logro de la estrategia y los objetivos del IPS.

Estas disposiciones se enmarcan en el Modelo de Supervisión Basada en Riesgos de la Superintendencia de Pensiones, contenido en la Resolución N° 102 de fecha 26 de diciembre de 2017, y particularmente en las categorías de riesgos inherentes consideradas en el citado modelo para el IPS.

Capítulo II. Componentes del Sistema de Gestión de Riesgos

En el presente Capítulo se presentan los elementos del sistema de gestión de riesgos que, al menos, deberá considerar el IPS para su funcionamiento.

II.1. Documentación sobre la Gestión de Riesgos

Se espera que las directrices de Gestión de Riesgos sean establecidas formalmente por el Director del Instituto, sean operativizadas mediante procedimientos que deben estar contenidos en Manuales de funcionamiento del sistema de gestión de riesgos implementado y alineado con el marco de referencia adoptado. El modelo de gestión de riesgos implementado debe estar basado en un marco de referencia reconocido internacionalmente, debe estar debidamente documentado y debe considerar la integración y alineación de las tres líneas de defensa, la estructura organizacional, la asignación de autoridad y responsabilidad en la Entidad, como asimismo las limitaciones del sistema de gestión de riesgos implementado.

La revisión de las directrices y procedimientos relacionados con la gestión de riesgos, se debe efectuar a lo menos una vez al año y cada vez que exista un cambio significativo en los procesos de la entidad.

Las directrices de Gestión de Riesgos y el manual de procedimientos que se defina a partir de ellas, deben ser conocidos por todos los funcionarios de la entidad, de manera tal que todas sus actividades se realicen de acuerdo a lo contemplado en dichos documentos.

En el manual de procedimientos de gestión de riesgos deberán quedar claramente definidas las asignaciones de autoridad, roles y responsabilidades de cada funcionario en relación con la gestión de riesgos. Asimismo, deberá quedar establecida la identificación de usuarios de reportes y sus roles, la emisión periódica de reportes de riesgos al Director Nacional, incluido el reporte de indicadores clave.

II.2. Principios o lineamientos éticos de la entidad

El Director Nacional debe aprobar los principios o lineamientos éticos de la institución, los que afectarán la actividad y decisiones tanto de los propios directivos y ejecutivos superiores, como del resto del personal del IPS. Se espera como buena práctica que las desviaciones de los estándares de conducta sean abordadas de manera oportuna y constante, y que sean comunicadas oportunamente a la Dirección Superior del IPS a través de canales expeditos.

Las normas éticas deben constar por escrito, por ejemplo, a través de un código de ética, siendo recomendable que tales normas sean ampliamente divulgadas a través de canales formales, con el fin de que sean conocidas y aplicadas por todo el personal en su trabajo cotidiano.

Constituye una buena práctica de administración tener procedimientos que permitan que los funcionarios entiendan que la entidad debe cumplir estrictamente con las obligaciones que imponen las leyes y las regulaciones, y que las conductas que lleven a infracciones al marco normativo son contrarias al mejor interés del IPS y de los imponentes/beneficiarios.

Se considera una buena práctica que el IPS exija permanentemente la estricta observación y apego a los principios éticos que lo rigen y aplicar medidas disciplinarias o correctivas cuando se detectan incumplimientos.

II.3. Aspectos organizacionales de Gestión de Riesgos

Una buena gestión de riesgos en el IPS se manifiesta en el establecimiento de una estructura operativa y el diseño de líneas de reporte que permitan el compromiso de los funcionarios con el desarrollo e implementación de prácticas para administrar todos los riesgos pertinentes derivados del desarrollo de sus actividades, siendo esencial el compromiso del Director Nacional y la Dirección Superior. Es indispensable además, que los miembros de los niveles gerenciales del IPS posean las competencias adecuadas, de modo de proporcionar una gestión sana y prudente de los riesgos.

Resulta aconsejable que el IPS cuente con una estructura organizacional adecuada en relación al tamaño y complejidad de sus actividades, debiendo considerar el número y tipo de imponentes/beneficiarios, la complejidad de sus relaciones con otras entidades, la complejidad de sus operaciones y procesos internos, y la asignación de las responsabilidades asociadas a los aspectos claves.

1. Funciones del Director Nacional

En el ámbito del presente Título, se espera que el Director Nacional sea el responsable de aprobar las políticas y los procedimientos de gestión de riesgos y control interno del IPS.

En ese sentido corresponde a una buena práctica el que las responsabilidades del Director Nacional, en relación a la gestión de riesgos, se refieran al menos a lo siguiente:

- Aprobar las directrices de Gestión de Riesgos del IPS.
- Aprobar las directrices generales de aceptación de riesgos, integridad, valores éticos
- Creación de ambientes de control propicios que permitan adoptar una cultura de riesgos en toda la institución.
- Revisar y aprobar, al menos una vez al año, el apetito, el nivel de tolerancia y capacidad de riesgo del IPS.
- Establecer directrices para que la Dirección Superior adopte las medidas necesarias para que los controles internos y los sistemas de monitoreo estén en operación para gestionar y reducir la severidad de los principales riesgos que enfrenta el IPS.
- Revisar al menos anualmente y cada vez que haya un cambio significativo, las directrices y manuales de procedimientos de gestión de riesgos y su cumplimiento, incluyendo los códigos de ética internos y tomar las medidas que se estimen necesarias para propender a que el IPS sea conducido de manera ética y transparente.
- Conocer y revisar al menos anualmente, los principales riesgos que enfrenta el Instituto y las medidas de control implementadas para su adecuado tratamiento.
- Definir roles, responsabilidades y rendición de cuentas en los diferentes niveles de gestión.
- Supervisar de manera efectiva a la Dirección Superior, de modo que el sistema de gestión de riesgos sea implementado y gestionado de acuerdo a la aplicación estricta de las directrices de riesgo definidas.
- Supervisar de manera efectiva a la Dirección Superior, de modo que la información relevante para la gestión de riesgos sea generada, difundida y comunicada fluidamente en todo sentido dentro de la organización, de un modo oportuno, apropiado y confiable.

- Facilitar al interior del IPS el cumplimiento de todas las leyes, normas y políticas institucionales teniendo claridad acerca del alcance y las consecuencias de la regulación aplicable.

- Aprobar y monitorear los planes de auditoría así como conocer las principales conclusiones de los informes de auditoría interna. Controlar el cumplimiento de los compromisos que la administración acuerde para remediar las observaciones efectuadas por Auditoría Interna.

2. Funciones de la Dirección Superior

Se considera una buena práctica de gestión de riesgos que la Dirección Superior del IPS asuma responsabilidades respecto a esta materia, en especial:

- Definir las características necesarias para lograr una cultura consciente del riesgo, acorde con los lineamientos establecidos por el Director Nacional.
- Demostrar el compromiso continuo con la competencia de sus funcionarios, lo que se refleja en la existencia de políticas y procedimientos implementados para atraer, desarrollar y retener funcionarios.
- Analizar y comprender el contexto en el que se desenvuelve el IPS, considerando el entorno, las partes interesadas y el perfil de riesgo.
- Revisar periódicamente la estrategia del Instituto y los objetivos definidos, con el propósito de mantener su alineación con el apetito de riesgo aprobado por el Director Nacional. En este contexto, deberá llevar a cabo procesos formales de planificación estratégica, incorporando en la etapa inicial un enfoque de gestión basado en riesgos.
- Establecer lineamientos y controlar la correcta identificación e implementación de medidas de mitigación oportunas sobre riesgos existentes, nuevos y emergentes que puedan afectar el logro de la estrategia y los objetivos definidos para el Instituto.
- Identificar y definir a los dueños de los procesos.

II.4. Función de la gestión de riesgos

El IPS deberá contar con la función de gestión de riesgos definida formalmente, la que será responsable de supervisar la gestión de riesgos del IPS, apoyando a los dueños de procesos o primera línea de defensa en la administración del sistema de gestión de riesgos. Esta función deberá mantener constantemente comunicaciones con el Director Nacional, la Dirección Superior, todas las unidades de negocio y Auditoría Interna, siendo además responsable de la difusión al interior del Instituto, del sistema de gestión de riesgos implementado.

La función de riesgos deberá elaborar y proponer políticas y procedimientos de gestión de riesgos para ser sometidas a la aprobación del Director Nacional.

Debe entregar apoyo metodológico a las áreas usuarias y dueños de procesos para implementar el modelo de gestión de riesgos.

El responsable de la función de riesgos debe contar con herramientas y recursos para la gestión de riesgos, reportará, al menos trimestralmente, en forma directa al Director Nacional sobre todos los temas relacionados con el funcionamiento del modelo de gestión de riesgos y será la contraparte de la Superintendencia en relación a estas materias.

El responsable de riesgos deberá adoptar las medidas correspondientes destinadas a identificar y monitorear los riesgos y controles implementados. En tal sentido, el responsable de la administración de riesgos debería:

- Asistir al Director Nacional en la definición del apetito, tolerancia y capacidad de riesgo.

- Asistir a la administración en el desarrollo de procesos y controles para la gestión de riesgos.

- Proporcionar guía para la gestión de riesgos y entrenamiento en procesos de gestión de riesgos.

- Controlar la mantención y actualización, al menos anual, de todas las matrices de riesgos del Instituto y que asimismo, estas matrices sean consistentes con los riesgos que enfrentan cada uno de los procesos del negocio.

- Mantener un mapa de riesgos, donde se grafican las medidas de severidad, es decir, las combinaciones de probabilidad e impacto de los riesgos. Este mapa de riesgos se debe actualizar en función de la matriz de riesgos.

- Impulsar y asesorar a la primera línea de defensa en el establecimiento de indicadores de riesgos que proporcionen un adecuado monitoreo de los riesgos potenciales. Tales indicadores deben estar disponibles para la administración de manera oportuna.

- Alertar a la administración de asuntos emergentes y de cambios en los escenarios regulatorios, con el propósito de implementar respuestas de riesgo de manera oportuna.

- Apoyar a la primera línea de defensa en la identificación y reporte oportuno de riesgos materializados y en el establecimiento de controles que permitan evitar su ocurrencia.

- Reportar periódicamente al Director Nacional y a la Dirección Superior, sobre aquellas situaciones de interés que se relacionan con la gestión de riesgos.

- Monitorear el cumplimiento de los planes de acción emitidos en respuesta a las observaciones dadas a conocer por la Superintendencia, en el Informe de Evaluación en Base a Riesgos.

- Difundir y promover la capacitación y entrenamiento del personal en materia de gestión de riesgos.

II.5. Rendimiento de la Gestión de Riesgos

El Instituto tiene la responsabilidad de identificar, evaluar y dar respuesta a los riesgos que pueden afectar su capacidad para lograr la estrategia y objetivos. Debe priorizar los riesgos de acuerdo con la severidad, teniendo presente su adherencia al apetito de riesgo aprobado por el Director Nacional.

La identificación de nuevos riesgos, emergentes y cambiantes, es un proceso continuo que debe realizar el Instituto, a través de la implementación de prácticas desarrolladas a través de todos los niveles de la entidad, que integren el conocimiento de los procesos y la conciencia sobre los riesgos que puedan afectar la estrategia y los objetivos del IPS. Los riesgos identificados deben ser administrados en una herramienta, denominada matriz de riesgos, donde se listan todos los riesgos que enfrenta el Instituto. Asimismo, deberá ser capaz de identificar aquellos riesgos de alto nivel o riesgos estratégicos, que puedan afectar el logro de la estrategia y sus objetivos.

El IPS deberá evaluar la gravedad de los riesgos identificados, ya sea de manera cualitativa, cuantitativa o utilizando una combinación de ambas y las medidas que seleccione para evaluar la gravedad de los riesgos se deben alinear con el tamaño, la naturaleza y complejidad del Instituto, como asimismo con su apetito de riesgo. Como parte de esta evaluación, la Dirección Superior debe considerar el riesgo inherente, el riesgo residual objetivo y el riesgo residual real, debiendo identificar factores desencadenantes o cambios en el contexto en que se desenvuelve el Instituto, que impliquen una nueva evaluación de la severidad, cuando sea necesario. Como resultado de la evaluación, se deberán establecer prioridades para atender riesgos, considerando entre otros factores, el apetito de riesgo definido.

Las respuestas seleccionadas para atender los riesgos que enfrenta el IPS, deben tomar en consideración factores tales como: el contexto en que se desenvuelve el Instituto, los costos y beneficios acordes con la gravedad y priorización del riesgo, obligaciones y expectativas de las partes interesadas y el apetito de riesgo establecido.

II.6 Evaluación y revisión de las capacidades y prácticas de gestión de riesgos

El Instituto debe identificar y evaluar los cambios en el entorno interno y externo que puedan afectar de manera significativa la estrategia y los objetivos establecidos, a través de la implementación de buenas prácticas de gestión. Para ello, debe existir conciencia de la posibilidad de que cambios sustanciales pueden ocurrir y pueden tener un efecto mayor, generando nuevos riesgos o modificando los actuales.

El IPS deberá implementar evaluaciones periódicas sobre el rendimiento de su modelo de gestión de riesgos en las áreas de mayor criticidad y deberá determinar si la gestión de éstos resulta eficiente. Esta actividad debe ser impulsada por el Director Nacional y debe ser realizada en conjunto con la Dirección Superior.

II.7 Información, comunicación y reportes

El Instituto debe utilizar canales de comunicación apropiados para apoyar su modelo de gestión de riesgos que permitan entregar información relevante para su uso en la toma de decisiones, tanto para sus usuarios internos como externos.

- A nivel interno, la comunicación debe ser fluida y llegar a todos los niveles pertinentes de la organización, con especial énfasis en los siguientes aspectos: Deben existir comunicaciones periódicas entre el Director Nacional y la Dirección Superior, instancia en que se debe realizar el análisis de aquellos riesgos relevantes que puedan impedir alcanzar la estrategia y los objetivos.
- Se deben comunicar con claridad las responsabilidades de cada una de las tres líneas de defensa (unidades de negocio, función de riesgos, cumplimiento y auditoría interna).
- El proceso de inducción contempla conocer y comprender la filosofía de gestión de riesgos del Instituto, así como también su modelo de gestión de riesgos.
- Realizar capacitaciones, al menos anualmente, sobre el funcionamiento del sistema de gestión de riesgos, en todos los niveles de la organización.

Respecto de los métodos de comunicación implementados, éstos deben ser lo suficientemente efectivos como para transmitir información relevante en materia de gestión de riesgos, los que deben ser evaluados periódicamente. Los medios de

comunicación utilizados deben considerar la comunicación con las distintas partes interesadas (internas y externas) y con el Director Nacional.

Las comunicaciones internas relevantes se deben encontrar debidamente identificadas y los procedimientos existentes deben definir los lineamientos de comunicación a las partes interesadas. Los métodos de comunicación utilizados por el Instituto responden a las necesidades existentes y pueden ser, sólo a modo de ejemplo, mensajes electrónicos, comunicaciones verbales, capacitaciones, seminarios y documentación interna escrita.

II.8. Gestión de las tecnologías de información (TI), seguridad de la información y continuidad Operacional

Considerando que la información y las tecnologías son cada vez más relevantes dentro de las organizaciones, se espera que el IPS implemente controles que permitan tratar el riesgo sobre los activos de información, lo que incluye proteger la información, las personas y la plataforma que la soportan, resguardándola de la materialización de amenazas internas y externas.

En términos de buenas prácticas el IPS debería gestionar el riesgo de las tecnologías de información. Por lo tanto, debe existir una adecuada gestión de las tecnologías de información definida por la Dirección Superior, que entregue los lineamientos para que la entidad administre las tecnologías de información, la seguridad y la continuidad operacional, con el objetivo de minimizar los riesgos relacionados con la confidencialidad, disponibilidad e integridad de la información.

La gestión de las tecnologías de información debe actuar como un mitigador transversal en la organización y debe incluir elementos tales como: políticas, principios y marcos de referencia, procesos y estructuras organizativas, que permitan una adecuada gestión de las tecnologías de información, de la seguridad de la información y de la continuidad del negocio.

En relación con el riesgo específico referido a Ciberseguridad, el IPS deberá contar con una estructura de controles adecuada para mitigar este tipo de riesgo.

II.9. Unidad de Auditoria Interna

Un elemento clave dentro de la estructura de administración de riesgos es la auditoría interna, debiendo ser su naturaleza y ámbito apropiado al nivel de operaciones del IPS.

El área de auditoría interna del IPS debe entregar una opinión independiente respecto del funcionamiento del sistema de gestión de riesgos implementado.

La unidad de auditoría interna debe tener acceso sin restricciones a todos los departamentos del IPS y a toda la información relevante de la misma y tener suficiente

nivel de autoridad y recursos para llevar a cabo su tarea. Asimismo, la actividad de auditoría interna debe ser independiente de todas las áreas operativas y reportar directamente al Director Nacional.

Debido a la importante naturaleza de sus funciones, el área de auditoría interna debe estar integrada por personas que posean las competencias y experiencia necesarias para tener un claro y cabal entendimiento de su rol y responsabilidades.

El área de auditoría Interna debe preparar y dar cumplimiento a un plan anual de auditoría que sea aprobado por el Director Nacional. Dicho plan debe abarcar aspectos tales como:

a) La naturaleza y extensión de los riesgos que enfrenta el IPS.

b) El apetito y tolerancia al riesgo para el IPS, según las categorías de riesgo que se definan.

c) La probabilidad de que se materialicen los riesgos.

d) La capacidad del IPS para reducir el impacto de los riesgos que se materialicen.

e) El seguimiento de la implementación de las observaciones relevantes efectuadas en auditorías anteriores, cuando corresponda.

f) Debilidades detectadas producto de fiscalizaciones realizadas por el Organismo Regulador.

g) La cobertura y actualización de las matrices de riesgos.

h) Evaluación de riesgos e implementación de controles acorde a la política y al modelo de gestión de riesgos, por parte de las áreas usuarias o dueñas de los procesos.

El alcance de los programas de auditoría interna debe ser acorde al nivel de riesgo y al volumen de actividad del IPS.

Con el propósito de mantener la independencia frente a la gestión de riesgos, la función de Auditoría Interna no debe:

- Establecer el apetito y tolerancia al riesgo del Instituto.
- Imponer procesos de gestión de riesgo.
- Manejar el aseguramiento sobre los riesgos.
- Tomar decisiones en respuesta a los riesgos.
- Implementar respuestas a riesgos a favor de la administración.
- Tener algún tipo de responsabilidad en la gestión de riesgos, distintos a los inherentes a su proceso.

Capítulo III. Gestión de Riesgos Específicos

1. Riesgo de Liquidez

a) Definición

Para efectos de esta norma el riesgo de liquidez se refiere a la falta de acceso en tiempo y forma a las prestaciones por parte de los beneficiarios del IPS, debido a una deficiente administración de los recursos financieros.

b) Gestión del riesgo de liquidez

El IPS deberá gestionar adecuadamente el riesgo de liquidez derivado de la administración de sus recursos financieros. Al respecto, se espera que exista pleno conocimiento del riesgo de liquidez y su medición y control se efectúe a través de mecanismos sistemáticos, formales y estructurados. Se espera que el IPS implemente mejores prácticas en la gestión de este riesgo, en las materias que a continuación se indican:

i. Política de gestión del riesgo de liquidez

Se espera que exista una política de gestión del riesgo de liquidez, que incorpore integralmente de manera clara y detallada el tratamiento del riesgo de liquidez, e incluya las metodologías utilizadas. A su vez, la política y procedimientos utilizados para el tratamiento del riesgo de liquidez deberían ser revisados regularmente.

Constituye una buena práctica que el IPS evalúe el cumplimiento de la política de gestión del riesgo de liquidez y los incumplimientos sean comunicados oportunamente al Comité respectivo y a la Superintendencia, y adopte las medidas necesarias para evitar su ocurrencia en el futuro. Para estos efectos, sería deseable que existiera un cargo o unidad en el IPS formalmente responsable de la gestión del riesgo de liquidez.

ii. Medición y control

Se espera que las herramientas de medición del riesgo de liquidez sean adecuadas para los niveles de riesgo definidos para la administración de los recursos financieros. Los modelos de medición, sus herramientas de análisis y los sistemas o programas deberían contar con documentación actualizada que describa sus funcionalidades y su operación.

Se considera como buena práctica que exista una cuantificación y monitoreo permanente respecto del riesgo de liquidez y muy especialmente de su evolución.

iii. Funcionarios que participan en la administración del riesgo de liquidez

Se espera que los funcionarios que administran el riesgo de liquidez, tengan vasta experiencia y conocimientos relevantes adecuados; asimismo se espera que sean suficientes en número, para asegurar un trabajo adecuado.

El IPS debería implementar programas de entrenamiento para los funcionarios que administran el riesgo de liquidez, que les permita estar actualizados respecto a conocimiento y nuevas tecnologías.

iv. Planes de contingencia de liquidez

Se espera que la Dirección Superior haya aprobado planes de contingencia de liquidez y que éstos se encuentren documentados.

Los planes de contingencia deberían ser conocidos cabalmente por los funcionarios relevantes.

2. Riesgo Operacional y Tecnológico

a) Definición

Para efectos de esta norma, el riesgo operacional y tecnológico se define como la contingencia de que los imponentes o beneficiarios no puedan acceder en tiempo y forma a los servicios y beneficios, o que enfrenten problemas derivados de la pérdida de información personal, debido a fallas o insuficiencias de procesos, personas, sistemas o por eventos externos. Se refiere tanto a las operaciones realizadas con medios del IPS como a las contratadas con proveedores externos. Incluye la pérdida de información de carácter personal y sensible y otras contingencias generadas por fallas en las tecnologías de información y comunicaciones.

b) Gestión del riesgo operacional

Todos los procesos del negocio clave que deben ser ejecutados por el IPS están expuestos a riesgo operacional. Por lo tanto, el IPS debe contar con un adecuado sistema de gestión del riesgo operacional, que incorpore entre otras las mejores prácticas que a continuación se indican:

- Adopción de una metodología reconocida de gestión de riesgos operacionales.

- Existencia de políticas y procedimientos documentados, para los procesos operacionales, los cuales deben estar actualizados y ser conocidos por todos los funcionarios relevantes y acordes a la Política de Gestión de Riesgos del Instituto

- Existencia de indicadores de proceso y de riesgo para los procesos operacionales clave. Existencia, a su vez, de una instancia de análisis de los indicadores de calidad y de riesgo, que permita evaluar y mejorar en forma continua su gestión.

- Control permanente de los procesos operacionales y adopción de medidas para solucionar los problemas o errores detectados.

- Identificación de los riesgos de fuentes internas y externas de los procesos clave, definición de sus controles y los planes de mitigación.

- Existencia de procedimientos de validación de la información de fuentes externas para detectar errores o fraudes.

- Existencia de un adecuado proceso de gestión de reclamos sobre los procesos operacionales.

- Suficiente segregación de funciones relativas a los distintos procesos operativos, que permitan mitigar adecuadamente los riesgos de errores y fraude.

- Funcionarios capacitados, adecuados en número a la complejidad y volumen de operaciones y con experiencia en el área.

- Existencia de una política de subrogación y reemplazo de cargos claves.
- Nivel de automatización de los procesos operacionales, adecuado a la complejidad y volumen de las operaciones.

- Existencia de indicadores de calidad y riesgo respecto al servicio entregado por los proveedores externos relevantes.

c) Gestión del riesgo tecnológico

Un adecuado sistema de gestión del riesgo tecnológico, asociado a los procesos operativos clave del IPS, se refleja en la implementación de las siguientes prácticas:

- El IPS debe contar con políticas de Administración de Tecnologías de Información y de Gestión de Riesgo Tecnológico, documentadas y conocidas por los funcionarios relevantes.

- La política de Administración de Tecnologías de Información, debe definir los lineamientos tecnológicos que permitan al Instituto dar soporte a sus procesos operacionales y de entrega de servicios, garantizando niveles adecuados de disponibilidad, confidencialidad e integridad de la información.

- La política de Administración de Riesgo Tecnológico debe definir los estándares de buenas prácticas que utilizará el Instituto para gestionar los riesgos de tecnología y de los procesos de negocio que apoyan su gestión en ella, haciendo referencia a marcos de referencia ampliamente utilizados, tales como: Cobit, Itil, normas ISO u otras. Debe además, señalar el alineamiento con la estrategia y metodología de gestión global de riesgos del Instituto.

- Las políticas de Administración de Tecnologías de Información y de Riesgo Tecnológico deben ser aprobadas y revisadas constantemente por la Director Nacional del Instituto.

- Las políticas y procedimientos de gestión de riesgo tecnológico se monitorean permanentemente, para adecuarlas a la dinámica de los riesgos emergentes.

- Las políticas y procedimientos de TI deben considerar el marco regulatorio vigente.

- Contar con metodologías, procedimientos adecuados y funcionarios idóneos para gestionar los riesgos tecnológicos.

- Contar con una adecuada segregación funcional y un nivel jerárquico del área de TI que asegure comunicación constante con la Dirección Superior del IPS permitiendo informar al Director el desempeño de las tecnologías y el desarrollo de proyectos de TI de envergadura, recibiendo retroalimentación oportuna para su gestión.

- Contar con una matriz específica que aborde el riesgo de TI, o su inclusión en las matrices de riesgo por proceso del IPS.

- Contar con comités que monitoreen los riesgos de tecnologías de información y que las materias relevantes sean reportadas a la Dirección Superior.

- Que el IPS cuente con indicadores de calidad y de riesgo de los procesos de TI. A su vez, debe existir una instancia de análisis de los indicadores de calidad y de riesgo de tal manera de evaluar su comportamiento, formular mitigadores ante desviaciones relevantes y mejorarlos en forma continua.

- Todos los procesos tecnológicos se encuentren debidamente documentados y actualizados.

- Existencia de controles de administración de incidentes y monitoreo continuo de los procesos tecnológicos.

- Contar con una metodología de adquisición y/o desarrollo de sistemas que considere procedimientos formales para procesos de prueba y planes de puesta en producción, acorde a su modelo de gestión de riesgos.

- Los contratos de mantenimiento y soporte de sus plataformas deben suscribirse con proveedores de reconocido prestigio, con respaldo de los respectivos fabricantes y deben considerar controles adecuados que permitan garantizar los niveles de servicio contratados.

- Los SLA contratados con los proveedores son acordes al tamaño, criticidad, complejidad de las operaciones y el apetito y tolerancia a los riesgos del IPS. El Instituto cuenta con procedimientos de control y gestión de los servicios contratados.

3. Riesgo Legal y Normativo

a) Definición

Para efectos de esta norma se entenderá por riesgo legal y normativo a la contingencia de falta de acceso en tiempo y forma a los servicios o beneficios por parte de los imponentes y beneficiarios, debido al incumplimiento de leyes, regulaciones o normas.

b) Gestión del riesgo legal y normativo

En relación con la gestión del riesgo legal y normativo se espera que la Dirección Superior del IPS sea la encargada de promover el cumplimiento de todas las obligaciones reglamentarias que la afectan. El IPS demuestra su compromiso por el cumplimiento normativo diseñando mecanismos de control que se apliquen sistemáticamente por todos los funcionarios, asumiendo las observaciones y requerimientos del regulador y colaborando con sugerencias para el perfeccionamiento normativo.

En tal sentido, se esperaría que el IPS gestione el riesgo legal y normativo considerando las siguientes herramientas:

- Política explícita de gestión del riesgo legal y normativo, así como los procedimientos para poner en aplicación la política definida y los sistemas de monitoreo y control para velar por su adecuado cumplimiento.

- Responsable por el cumplimiento o compliance. Esta función debería ser realizada por un funcionario de alto nivel, quien identifique, asesore, alerte, monitoree y reporte los riesgos de cumplimiento en el IPS, y vele por la correcta aplicación de los cambios normativos. Se espera que el Director Nacional del IPS nombre al oficial de cumplimiento y verifique que tenga la autoridad para examinar cualquier problema o violación potencial, así como también crear los medios apropiados para prevenirlos y gestionarlos. La función de cumplimiento podría combinarse con otras funciones, siempre y cuando no surjan conflictos de interés y se adopten medidas para asegurar su independencia de las funciones operativas del negocio, mediante procedimientos adicionales de control.

- Estrategias de comunicación y capacitación para sensibilizar a los funcionarios sobre la función de cumplimiento.

- Evaluación del riesgo de cumplimiento en la Dirección Superior.

- Seguimiento al cumplimiento del IPS, cuyo procedimiento se encuentre formalizado y se documente mediante un reporte de cumplimiento. Al respecto, sería esperable que los reportes de cumplimiento en el IPS sean evaluados y se adopten las medidas correctivas oportunamente.

- Planes anuales de auditoría interna que incluyan el cumplimiento legal y normativo como materia de revisión. En ese sentido sería deseable que el proceso global de cumplimiento sea auditado periódicamente y entregue factores clave de retroalimentación.

- Sistemas de difusión del marco legal y normativo a las áreas involucradas, así como capacitación formal y permanente a los funcionarios en aspectos legales y normativos.

- Adecuado proceso de implementación y monitoreo de los cambios regulatorios.

4. Riesgo Estratégico

a) Definición

Para efectos de esta norma el riesgo estratégico es la contingencia de que el IPS adolezca de la falta de capacidad de adaptar su estrategia (esquema operacional y de negocios), ante cambios en el entorno o en la regulación aplicable, impidiendo el acceso en tiempo y forma a los servicios y prestaciones por parte de los imponentes y beneficiarios.

b) Gestión del riesgo estratégico

Los siguientes elementos presentes en el IPS, serán indicativos de una adecuada gestión del riesgo estratégico:

- Que la Dirección Superior del IPS haya desarrollado una visión de largo plazo, a partir de un conocimiento muy preciso de las fortalezas y debilidades de la institución. Esta visión se plasma en planes de varios años, en los cuales se enmarcan las diversas estrategias del IPS y sirven de base para la asignación de los recursos humanos, físicos, tecnológicos y financieros.

- Que el IPS haya establecido una política explícita de gestión del riesgo estratégico, los procedimientos para poner en aplicación la política definida y los sistemas de monitoreo y control para velar por su adecuado cumplimiento.

- Que los proyectos nuevos que comprometen recursos significativos del IPS sean evaluados en forma acuciosa y regularmente por la Dirección Superior, con un adecuado análisis de riesgo. Para ello, sería deseable que:

  - La Dirección Superior establezca la aplicación de una metodología de administración de los proyectos de envergadura, que permita controlar su ejecución, sus riesgos y hacer análisis de calidad adecuados.
  - La Dirección Superior evalúe regularmente los proyectos nuevos de

envergadura, que comprometen grandes recursos, o que impactan significativamente a los imponentes y beneficiarios, o al quehacer interno del IPS.

- Que la Dirección Superior haya establecido y vigile la adecuada implementación de un sistema de información confiable, oportuno y completo, para la efectiva toma de decisiones.

5. Riesgo Reputacional

a) Definición

Para efectos de esta norma el riesgo reputacional es la contingencia de pérdida de confianza de los imponentes y beneficiarios en la integridad o funcionamiento del IPS, debido a una acción u omisión, ejecutada por éste.

b) Gestión del riesgo reputacional

Los siguientes elementos presentes en el IPS, serán indicativos de una adecuada gestión del riesgo reputacional:

- Que el IPS haya establecido una política explícita de gestión del riesgo reputacional, los procedimientos para poner en aplicación la política definida y los sistemas de monitoreo y control para velar por su adecuado cumplimiento.

- Que el IPS haya adoptado buenas prácticas de conducta de mercado y un trato justo hacia los imponentes y beneficiarios.

- Que la Dirección Superior tenga una adecuada comprensión de las operaciones y riesgos que enfrenta el IPS cuya materialización puede dañar la confianza del imponente o beneficiario.

6. Riesgo de Conducta de Mercado

a) Definición

Para efectos de esta norma el riesgo de conducta de mercado se define como la contingencia de que los imponentes y beneficiarios tomen decisiones

desalineadas con sus intereses debido a la falta de información o a la entrega de información parcial, errónea o inoportuna atribuible al IPS.

b) Gestión del riesgo de conducta de mercado

El IPS deberá gestionar adecuadamente el riesgo de conducta de mercado, para un apropiado funcionamiento y desarrollo del sistema previsional que administra y la debida protección a los imponentes y beneficiarios. Al respecto, se espera que el IPS implemente mejores prácticas en las materias que a continuación se indican, tendientes a prevenir situaciones no deseadas de conducta de mercado.

i. Transparencia y divulgación de información

Se considera una buena práctica relativa al tratamiento de información, la existencia de una política de divulgación y transparencia de la información a los imponentes, beneficiarios y público en general, que sea formal, conocida y aprobada por la Dirección Superior. Se espera que la Dirección Superior esté consciente de la importancia de la información que se provea a los imponentes, beneficiarios y público en general, siendo parte de los temas que se tratan en las reuniones de nivel superior.

La política de divulgación y transparencia de la información debe contener los temas más importantes a difundir, incluidos los canales e instrumentos a través de los cuales se transparenta y divulga información relevante para los imponentes y beneficiarios.

El IPS debe adoptar mecanismos para asegurarse que el trato hacia sus usuarios sea éticamente adecuado y honesto. Este principio debería ser parte de la cultura organizacional.

En cuanto al seguimiento de la política de divulgación y transparencia, la Dirección Superior la debe revisar, al menos anualmente, y debe existir una estructura de control interno en el IPS para verificar el cumplimiento de dicha política. Asimismo, la asignación de recursos físicos, humanos y económicos para esta tarea debe ser acorde con el alcance de la política.

El IPS debe otorgar el tratamiento de la información que entrega a sus imponentes, beneficiarios y público en general, reflejando los siguientes elementos:

- Los canales e instrumentos a través de los cuales se divulga información son adecuados a la cantidad de imponentes y beneficiarios y su distribución geográfica.

- La información divulgada al público es exacta, relevante y oportuna.

- La información disponible en todos los canales de información está actualizada, es clara y suficiente.

- Existen esfuerzos por parte del IPS para entregar información personalizada a los imponentes y beneficiarios.

- El IPS tiene actualizados los antecedentes para el contacto con sus imponentes, beneficiarios y empleadores.

- La información entregada en forma privada a los imponentes y beneficiarios se realiza manteniendo la debida confidencialidad de la misma.

Resulta fundamental que los funcionarios que tengan información, cuenten con los conocimientos y habilidades necesarias para esta tarea, debiendo el IPS establecer mecanismos efectivos de control de la calidad de la información entregada. En este contexto, es de especial importancia la capacitación continua de los funcionarios que realizan dicha función.

ii. Atención y servicio en forma presencial y remota

El IPS debe gestionar adecuadamente el funcionamiento de sus centros de atención y de los servicios que entrega en forma remota (Internet, call center y otros).

Al respecto, se considerarán como buenas prácticas en relación al servicio prestado en los centros de atención presencial, las siguientes:

- El IPS cuenta con una certificación de la calidad de servicio en sus centros de atención. Tal certificación cumple con estándares internacionales, fue efectuada por un organismo de reconocido prestigio y se encuentra vigente.

- El IPS cuenta con políticas y procedimientos documentados y actualizados para el funcionamiento de los centros de atención.

- Las políticas y procedimientos son conocidos y son aplicados por todos los funcionarios relevantes.

- El IPS cuenta con una red de atención con una oferta de servicios

estándar en cuanto a imagen, diseño, accesibilidad, estándar de tiempos de espera y de atención y tamaño ajustado a la demanda.

- El IPS asigna los recursos físicos, humanos y tecnológicos de atención de público acordes en cantidad, oportunidad y calidad al volumen de imponentes y beneficiarios.

- El IPS cuenta con políticas y procedimientos documentados para el reclutamiento y capacitación de los funcionarios de atención de público, los cuales están actualizados y son conocidos por todos los funcionarios relevantes.

- El IPS cuenta con procesos eficientes y seguros de atención de imponentes y beneficiarios.

- El IPS cuenta con procedimientos que permiten dar continuidad operacional al servicio que presta; procedimientos que deben estar revisados, actualizados, probados y difundidos a sus funcionarios.
- El IPS ha definido adecuados indicadores de desempeño del servicio que presta.

A su vez, se considerarán como buenas prácticas en relación al servicio entregado a través de canales remotos, las siguientes:

- El IPS cuenta con políticas y procedimientos documentados y actualizados para el funcionamiento de los servicios por canales remotos, que dan cuenta de la preocupación permanente por la calidad y continuidad del servicio que presta a sus imponentes y beneficiarios.

- Las políticas y procedimientos son conocidos y son aplicados por todos los funcionarios relevantes.

- La política relativa a la seguridad contempla herramientas de monitoreo y evaluación constante de la seguridad del sitio web.

- La política relativa a capacidad de servicios contiene un compromiso de capacidad mínima de transacciones respecto de las principales funcionalidades que soportará el sitio web.

- El sitio ha sido conceptualizado como un canal de atención transaccional y no solo interactivo y su diseño se ajusta a las necesidades de sus usuarios y parámetros mínimos de calidad de servicio.

- El IPS ha establecido estándares para la medición de la calidad del servicio que entregan los canales remotos, los cuales son monitoreados y gestionados periódicamente.

- El IPS asigna los recursos físicos, humanos y tecnológicos para el adecuado funcionamiento de los servicios por internet, acordes en cantidad, oportunidad y calidad al volumen de operaciones.

- Los estándares de calidad de servicio del call center en el caso de subcontratos constan en las cláusulas del respectivo contrato.

- El IPS adopta mecanismos de control y realiza análisis periódicos de vulnerabilidades del sitio, para garantizar la seguridad de las operaciones efectuadas a través de éste y la integridad, disponibilidad y confidencialidad de la información.

iii. Protección de la información de los imponentes y beneficiarios

De acuerdo a las obligaciones legales vigentes, el IPS debe adoptar todas las medidas necesarias para proteger la información personal de sus imponentes y beneficiarios, resguardando su confidencialidad. Para ello, debe desarrollar adecuadas políticas y procedimientos de resguardo de la información, capacitar al personal, implementar controles internos para verificar su cumplimiento, contar con tecnología adecuada, identificar y manejar los riesgos y amenazas a la seguridad e integridad de la información y contar con planes de contingencia que permitan mitigar los riesgos y el impacto de cualquier filtración o uso indebido de la información.

El IPS debe considerar el riesgo que representa la externalización de actividades, debiendo verificar que las entidades contratadas cuenten con adecuados mecanismos para resguardar la confidencialidad de la información.

Capítulo IV. Información a la Superintendencia

La Superintendencia tendrá acceso a toda la información que considere relevante para la gestión de riesgos y control interno del IPS, así como a los sistemas de información de gestión de riesgos o cualquier otra información que considere relevante.

En todo caso, el IPS deberá enviar a la Superintendencia el manual de políticas y procedimientos de gestión de riesgos del Instituto, así como toda modificación al mismo que contenga cambios significativos. De igual forma deberá enviar a esta Superintendencia el documento que contenga los principios éticos que lo rigen.

El IPS deberá enviar anualmente a esta Superintendencia, el informe con los resultados obtenidos producto de las auditorías de aseguramiento sobre el proceso de gestión de riesgos y sobre los sistemas de control interno.

Por otra parte, el encargado de auditoría interna deberá enviar el plan anual de auditoría con su respectivo calendario de actividades en forma previa a su ejecución, e informar además, el estado de cumplimiento del plan anual de auditoría referido al año precedente.

Toda renuncia y reemplazo para los cargos de responsable de riesgos y encargado de la unidad de auditoría interna, deberá informarse a la Superintendencia en un plazo de cinco días hábiles de ocurrido el suceso.

V. Vigencia

La presente Norma comenzará a regir a contar del 1 de enero de 2020.

OSVALDO MACÍAS MUÑOZ
Superintendente de Pensiones