Libro V, Título XVII Instrucciones sobre Administración de Riesgo en el Instituto de Previsión Social

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.

Nota de actualización: Este Capítulo fue incorporado por la Norma de Carácter General N°246, de fecha 1 de julio de 2019.