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

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.

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