

REF.: INSTRUYE SOBRE LA IMPLEMENTACIÓN DE LA GESTIÓN DE RIESGO OPERACIONAL EN LAS ENTIDADES DE DEPÓSITO Y CUSTODIA DE VALORES Y EN LAS SOCIEDADES ADMINISTRADORAS DE SISTEMAS DE COMPENSACIÓN Y LIQUIDACIÓN DE INSTRUMENTOS FINANCIEROS.

Para las entidades de depósito y custodia de valores, reguladas por la Ley N° 18.876, y las sociedades administradoras de sistemas de compensación y liquidación de instrumentos financieros, reguladas por la Ley N° 20.345

Esta Superintendencia, en uso de sus facultades legales, y en atención a lo dispuesto en el inciso tercero del artículo 1°, artículos 27° y 28° de la Ley N° 18.876 y en los artículos 7°, 9° y 11°, de la Ley N° 20.345, ha estimado necesario dictar las instrucciones contenidas en la presente circular, referentes a la gestión del riesgo operacional que las entidades de depósito y custodia de valores y las sociedades administradoras de sistemas de compensación y liquidación de instrumentos financieros deberán poner en práctica, con la finalidad de asegurar el cumplimiento de estándares adecuados en el desarrollo de sus actividades.

I. INTRODUCCIÓN

La actividad de gestión de riesgo operacional, incluyendo el necesario desarrollo de mecanismos de control, adquiere especial importancia en el contexto de las entidades de depósito y custodia de valores y de las sociedades administradoras de sistemas de compensación y liquidación de instrumentos financieros (ambas en adelante “la entidad” o “las entidades”), en virtud de su relevancia sistémica en la infraestructura del mercado de valores. Es por esta razón que las recomendaciones y principios internacionales de mejores prácticas asociadas a sistemas de custodia, compensación y liquidación de valores, enfatizan la necesidad de contar con la capacidad de gestionar el riesgo operacional de las entidades proveedoras de estos servicios.

II. DEFINICIONES

- **Riesgo operacional:** Corresponde al riesgo de pérdida debido a la inadecuación o a la falla de los procesos, del personal y de los sistemas internos y/o de los controles internos aplicables o bien a causa de acontecimientos externos.
- **Gestión de riesgo operacional:** Corresponde al proceso de identificación, medición, control y monitoreo del riesgo operacional de la entidad que pueda afectar de forma adversa la consecución de sus obligaciones establecidas en el marco legal. Este proceso es aprobado, implementado y controlado por la gerencia general de la entidad, teniendo presente las responsabilidades del directorio, la administración, las unidades internas de supervisión y todo el

personal de la misma. Este proceso forma parte integral de la política de gestión de riesgo operacional aprobada por el directorio.

- **Dueño del proceso:** Corresponde a aquella persona designada para hacerse responsable de la administración de un proceso y propiciar las mejoras a implementar en éste.
- **Diagrama de procesos:** Corresponde a la representación esquemática de las secuencias de un proceso o subproceso mediante un flujograma y su descripción. El responsable de esta documentación es el dueño del proceso.
- **Matriz de riesgos y controles:** Corresponde a una herramienta a través de la cual se muestran los riesgos de un proceso o subproceso, su evaluación, los controles asociados junto a su efectividad y el nivel de riesgo residual con el objetivo de priorizar, orientar y focalizar el tratamiento de riesgo.
- **Riesgo inherente:** Corresponde a aquel riesgo que por su naturaleza no puede ser separado del proceso o subproceso en que éste se presenta. Corresponde al riesgo que debe asumir cada entidad de acuerdo al ámbito de desarrollo de sus actividades establecido por ley.
- **Riesgo residual:** Corresponde al nivel de riesgo remanente que existe sin perjuicio de haberse implementado las medidas de control.
- **Riesgo aceptado:** Corresponde al nivel de riesgo que la entidad esta dispuesta a aceptar en concordancia con la política de gestión de riesgo operacional y sus responsabilidades establecidas en el marco legal que las rige.

III. ELEMENTOS BÁSICOS PARA IMPLEMENTAR EL PROCESO DE GESTIÓN DE RIESGO OPERACIONAL

Las entidades deberán establecer procedimientos documentados y debidamente aprobados para implementar el proceso de gestión de riesgo operacional, los que deben considerar al menos los siguientes elementos:

1. Directrices del proceso de gestión de riesgo operacional

1.1 Política de gestión de riesgo operacional

El directorio de la entidad deberá aprobar y ordenar la implementación de una política de gestión de riesgo operacional, destinada a establecer las medidas que deberá adoptar la administración de la entidad en dicho ámbito. Dicha política será parte integral de la política de gestión de riesgos contemplada por el artículo 9° de la Ley N° 20.345, la cual debe ser establecida por el directorio de la entidad.

La política de gestión de riesgo operacional deberá abordar a lo menos los siguientes aspectos:

a) Roles y responsabilidades

Se deberán definir las obligaciones y responsabilidades de quienes participan en el proceso de gestión de riesgo operacional. Este aspecto se detalla en la sección IV de esta circular.

b) Definición de objetivos del proceso de gestión de riesgo operacional

La entidad debe establecer los objetivos que persigue la implementación del proceso de gestión de riesgo operacional, los cuales deben alinearse con sus objetivos estratégicos.

c) Definición de riesgos

La entidad debe establecer una definición clara de los riesgos operacionales a gestionar, con el objetivo de determinar los tipos de riesgos que serán administrados y tratados, como por ejemplo: riesgo tecnológico; riesgo de fraude interno o externo; riesgo de fallos en los procesos; riesgo de recursos humanos, etc.

d) Definición de riesgo aceptado

La entidad debe establecer los criterios para determinar el riesgo aceptado, el cual debe ser consecuente con los criterios de evaluación y tratamiento de riesgos y con el marco legal y reglamentario aplicable a la entidad.

e) Criterios de evaluación y tratamiento de riesgos

La entidad deberá definir el criterio de evaluación de riesgo que mejor se adecue a su contexto organizacional y estratégico. Además, debe especificar los criterios de tratamiento de los riesgos, junto con las variables a considerar en cada una de ellas.

1.2 Manual de gestión de riesgo operacional

Basándose en la política, las entidades deberán establecer procedimientos formales para la gestión de los riesgos que surjan de los procesos asociados a las actividades efectuadas por dichas entidades. Tales procedimientos deberán estar debidamente documentados en un manual de gestión de riesgo operacional, el cual debe describir las etapas del proceso de gestión de riesgo operacional, junto a los requerimientos de documentación y de informes resultantes, teniendo en consideración lo que se establece en la presente circular.

En dicho manual, debe estar identificada la unidad responsable de desarrollar, implementar e impulsar la gestión de riesgo operacional en la entidad.

2. Análisis y evaluación de riesgos

La entidad deberá implementar un proceso estructurado bajo el cual los riesgos son identificados, medidos y priorizados, considerando al menos los siguientes aspectos:

- a) La unidad responsable de la gestión de riesgo operacional, a la que se hace referencia en la sección IV, debe identificar los procesos y subprocesos en los que se descomponen las actividades efectuadas por la entidad, identificando a los respectivos dueños de dichos procesos.
- b) Los dueños de procesos deben describir de manera precisa los procesos y/o subprocesos, por medio de diagramas de procesos.
- c) La unidad responsable de la gestión de riesgo operacional en conjunto con el dueño de cada proceso, debe:
 - Identificar y evaluar los diferentes riesgos y factores que influyen sobre éstos mediante un análisis combinado de riesgo inherente, impacto y probabilidad de materialización, considerando la efectividad de las actividades de control implementadas para mitigar dichos riesgos. A partir de ello, se debe estimar el riesgo residual o nivel de riesgo expuesto. Esta evaluación se debe documentar en una matriz de riesgos y controles.
 - Comparar el resultado de esta evaluación con el nivel de riesgo aceptado, definido en la política de gestión de riesgo operacional.
 - Priorizar los riesgos para ser tratados de acuerdo al criterio de evaluación de riesgos establecido en la política de gestión de riesgo operacional..
 - Mantener actualizada y disponible en todo momento la documentación asociada a las actividades mencionadas en este numeral.

3. Tratamiento de riesgos

De acuerdo a las prioridades establecidas en la etapa de análisis y evaluación de riesgos, la unidad responsable de la gestión de riesgo operacional, en conjunto con el dueño de cada proceso, debe analizar las distintas opciones para el tratamiento de los riesgos, definidas en la política de gestión de riesgo operacional, preparar planes de acción para su tratamiento y definir la forma en que estos últimos se implementarán. Esta decisión se deberá documentar en la

matriz de riesgos y controles, la cual, en este ámbito, debe indicar para cada proceso o subproceso revisado, a lo menos lo siguiente:

- a) Descripción del riesgo.
- b) Nivel de riesgo o riesgo inherente.
- c) Descripción de la acción a tomar.
- d) Responsable de la implementación.
- e) Plazo y estado de la implementación.
- f) Apoyo de otras áreas de la entidad.

4. Monitoreo y evaluación

Las entidades deberán monitorear de forma permanente sus principales riesgos, junto a la efectividad de las actividades de control implementadas.

Los resultados de los monitoreos deben ser informados periódicamente a los miembros del directorio, a la gerencia general y a los dueños de procesos, a través de reportes periódicos. Para tales efectos, la unidad responsable de la gestión de riesgo operacional, debe implementar indicadores para realizar los monitoreos sobre:

- a) Los riesgos de la entidad.
- b) Los factores de riesgo asociados.
- c) La efectividad de las medidas de control implementadas o existentes.

Adicionalmente dicha unidad debe mantener la documentación y el registro de al menos los incidentes más significativos ocurridos y las medidas de mitigación aplicadas los cuales deberán permanecer disponibles para su consulta por un periodo de tiempo de al menos cinco años.

5. Información y Comunicación

La unidad responsable de la gestión de riesgo operacional debe mantenerse en constante comunicación con el resto de las unidades de la entidad. Para ello debe diseñar y emitir reportes periódicos a los diferentes interesados (internos o externos a la entidad). Corresponderá considerar a lo menos los siguientes aspectos:

- a) La gerencia general deberá informar a lo menos una vez al año al directorio sobre los principales riesgos de la entidad y los planes de tratamiento adoptados; en este aspecto, se incluyen los planes de tratamiento que se implementarán. De la presentación que se efectúe, su discusión y aprobación, quedará constancia en las actas de sesión de directorio correspondientes.
- b) Igual obligación de información de la letra a) será aplicable a la gerencia general, en el caso de las empresas de depósito y custodia, con respecto al Comité de Vigilancia, dejándose constancia de ello.
- c) La unidad responsable de la gestión de riesgo operacional debe informar oportunamente, o a lo menos trimestralmente, a la gerencia general sobre los procesos revisados, los resultados sobre la efectividad de los controles revisados, el estado de avance de los planes de mitigación acordados con los dueños de procesos, los incidentes registrados y la evolución de los indicadores diseñados para el monitoreo.
- d) La unidad responsable de la gestión de riesgo operacional deberá informar a los dueños de procesos sobre el resultado de la evaluación de gestión de riesgo operacional relativo a sus procesos, y adicionalmente, debe informar sobre el estado de avance mensual de los planes de acción comprometidos.
- e) La unidad responsable de evaluar de forma permanente e independiente la efectividad de las políticas y procedimientos de la gestión de riesgo operacional, a la que se hace referencia en la sección IV, deberá informar a lo menos una vez al año al directorio sobre el cumplimiento de la política y del manual de gestión de riesgo operacional.
- f) La gerencia general deberá informar a toda la organización, como también al público en general, los lineamientos principales de la gestión de riesgo operacional, a través de un informativo puesto a disposición en la página web de la entidad.

IV. RESPONSABILIDADES

Las entidades deberán mantener una estructura organizacional apta para la definición, administración y el control de todos los riesgos pertinentes, derivados del desarrollo de sus actividades.

La estructura organizacional de las entidades deberá considerar, al menos, que:

- a) El directorio de la entidad, en el ámbito de la presente circular, sea responsable de revisar y aprobar la política de gestión de riesgo operacional de la entidad, dejando evidencia de ello. Además, tenga la responsabilidad de estar informado

de la gestión de riesgo operacional de la organización, para lo cual podrá delegar esta responsabilidad en un comité constituido por al menos tres integrantes, siendo al menos uno de ellos miembro del directorio.

- b) La gerencia general de la entidad, en el ámbito de la presente circular, sea responsable de elaborar la política y manual de gestión de riesgo operacional, sin perjuicio de la posibilidad de delegar su elaboración a una persona especialmente calificada, sin eximir sus responsabilidades. También deberá asegurar la implementación del proceso de gestión de riesgo operacional en la entidad.
- c) Exista una unidad responsable de desarrollar, implementar e impulsar la gestión de riesgo operacional de acuerdo a lo dispuesto en la sección III de la presente circular.
- d) Exista una unidad responsable de evaluar de forma permanente e independiente la efectividad de las políticas y procedimientos de la gestión de riesgo operacional. Esta unidad debe informar de su labor directamente al directorio de la entidad.

Esta unidad podrá delegar determinadas funciones de evaluación, tales como la realización de pruebas a los procedimientos y controles, a otras personas o entidades calificadas externas. No obstante, dicha unidad seguirá siendo responsable de aquellas funciones, las cuales se efectuarán bajo su propia supervisión.

- e) Los empleados de la entidad deban conocer y dar cumplimiento cabal a la política de gestión de riesgo operacional. Además deba existir evidencia de la toma de conocimiento de la política.

V. ACTUALIZACIÓN DE POLÍTICAS Y PROCEDIMIENTOS

Las políticas y procedimientos de gestión de riesgo operacional deberán ser constantemente revisados, monitoreados, y de ser el caso actualizados, de forma tal que se asegure una efectiva identificación de los riesgos y se cuente con los controles adecuados para su mitigación. Estas revisiones deberán ser realizadas con una periodicidad de a lo menos de una vez al año.

En tal sentido, toda modificación efectuada a los procedimientos de gestión de riesgo operacional deberá ser incorporada al Manual del que trata la sección II de la presente circular.

VI. OTRAS DISPOSICIONES

La información, los registros y antecedentes que den cuenta del cumplimiento de la presente circular, deberán estar en todo momento a disposición de la Superintendencia.

VII. VIGENCIA

Tratándose de las entidades de depósito y custodia, las disposiciones contenidas en la presente circular deberán ser implementadas antes del 31 de diciembre de 2009.

En el caso de las sociedades administradoras de sistemas de compensación y liquidación de instrumentos financieros, las disposiciones contenidas en la presente circular deberán ser implementadas antes de cumplidos 180 días después del inicio de actividades.

SUPERINTENDENTE