COMISIÓN PARA EL MERCADO FINANCIERO

COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

**Informe Normativo**

# Gobierno Corporativo y Gestión Integral de Riesgos de Bolsas de Valores y Bolsas de Productos

Mayo 2024

**www.CMFChile.cl**

# Contenido

# I. INTRODUCCIÓN Y OBJETIVO DE LA PROPUESTA

En cumplimiento de su mandato legal, a la Comisión para el Mercado Financiero (CMF) le corresponde velar por el correcto funcionamiento, desarrollo y estabilidad del mercado financiero, para lo cual cuenta con sus atribuciones de regulación y fiscalización.

Para ello, utiliza una metodología de supervisión basada en riesgos, la cual implica, entre otras cosas, una focalización en las actividades de las entidades supervisadas que pudieran tener un mayor impacto en caso de materializarse algún riesgo inherente a su giro.

La presente propuesta normativa tiene por objetivo establecer un marco de Gestión Integral de Riesgos para Bolsas de Valores y Bolsas de Productos, en el marco de la metodología de supervisión basada en riesgos.

Todo lo anterior, con el objetivo de complementar y fortalecer la metodología de supervisión basada en riesgos, velando porque las disposiciones aplicables resulten coherentes con la implementación de altos estándares de gestión de riesgos de forma proporcional al tipo de entidad, y otorgando a éstas un alto grado de certeza respecto de cuáles serán las exigencias que le resultarán aplicables por esta Comisión.

# II. DIAGNÓSTICO Y MARCO NORMATIVO LOCAL

El marco normativo propuesto viene a aplicar y dar cumplimiento a las disposiciones legales sobre gestión de riesgos para las entidades mencionadas.

El proyecto normativo busca resolver las siguientes brechas identificadas como parte del diagnóstico:

a) Establecer un marco integral de gestión de riesgos para Bolsas de Valores y Bolsas de Productos, a fin de subsanar la asimetría regulatoria en esta materia que se produce respecto a Intermediarios de Valores, Administradoras Generales de Fondos y entidades de Infraestructura del mercado financiero.

b) Adecuar la regulación a las mejores prácticas internacionales, incluyendo elementos de proporcionalidad para el cumplimiento por parte de las entidades.

c) Establecer un marco normativo que permite la adecuada supervisión basada en riesgos de estas entidades.

A continuación, se describe el marco normativo local aplicable a la gestión de riesgos, para Bolsas de Valores y Bolsas de Productos:

**a) Bolsas de Valores**: artículos 38, 39, 40 (reemplazado por la Ley N°21.521), 42 (modificado por la Ley N°21.521), 43, 44 bis y 51 de la Ley N°18.045. Estas disposiciones requieren que las bolsas cumplan con las exigencias de gobierno corporativo y gestión de riesgos que determine la CMF; cuenten con recursos, medios y sistemas que garanticen que los mecanismos de subastas serán ininterrumpidos; que sus miembros serán debidamente regulados y supervisados por la bolsa; y que ésta contará permanentemente con las condiciones que se requieren a objeto que el mercado preserve los principios que debe tener para la consecución de la mejor ejecución de las órdenes de los clientes.

**b) Bolsas de Productos:** artículos 2 y 3 de la Ley N°19.220. Estas disposiciones requieren

que las bolsas de productos cuenten con un gobierno corporativo, controles internos y gestión de riesgos, junto con los recursos, medios y sistemas que permitan garantizar su correcto funcionamiento, así como la mejor ejecución de órdenes de sus corredores.

## Marco de gestión integral de riesgos existente en la regulación chilena

A continuación, se revisa el marco de gestión de riesgos de las siguientes entidades: Bancos, Compañías de Seguros y Empresas de Auditoría Externa.

### a) Bancos

#### Circular N°2.270

Establece requerimientos patrimoniales adicionales para la gestión de riesgos de acuerdo a los artículos 66 y siguientes de la Ley General de Bancos[1]. Este mayor nivel de patrimonio efectivo no podrá exceder el 4% de los activos ponderados por riesgo del banco, neto de provisiones exigidas. La circular también actualiza el capítulo 1-13 de la Recopilación Actualizada de Normas de Bancos (RAN) e introduce un nuevo capítulo 21-13, los cuales se detallan a continuación.

#### Capítulo 1-13 de la RAN sobre clasificación de gestión y solvencia.

La norma expone el proceso de evaluación realizado por la Comisión a las instituciones bancarias en materias de solvencia y gestión.

Al evaluar la gestión de las entidades bancarias la Comisión supervisa la adecuada implementación del gobierno corporativo. Así, el directorio es el responsable de aprobar y supervisar el cumplimiento de los lineamientos estratégicos, valores corporativos, líneas de responsabilidad, políticas y procedimientos; mientras que la administración debe implementarlos adecuadamente en la práctica en la entidad.

Asimismo, se espera que el directorio defina y apruebe el apetito por riesgo, así como un marco de gobierno corporativo, donde ambos consideren manuales y procedimientos por escrito, y se vele por su cumplimiento. Dentro de las responsabilidades del directorio se incluye promover controles internos sólidos acordes a las actividades realizadas por la entidad, así como procesos de auditoría interna y externa, las que debe contar con la debida independencia, recursos e instancias de comité de auditoría en el directorio. Finalmente, el directorio debe establecer los contenidos de la información que serán divulgados por la institución bancaria a las distintas partes interesadas.

La evaluación considera también los ámbitos de riesgo de crédito y gestión global del proceso de crédito, gestión del riesgo financiero y operaciones de tesorería, administración del riesgo operacional, control sobre las inversiones en sociedades, prevención del lavado de activos y del financiamiento del terrorismo, administración de la estrategia de negocios y gestión de la suficiencia capital, gestión de la calidad de atención a los usuarios y transparencia de información.

Se espera que el directorio defina tres líneas de defensa para la gestión de los riesgos mencionados. La primera de ellas refiere a la gestión de los riesgos realizada por las distintas gerencias del banco, en las que recae la propiedad de los riesgos. Estas deben identificar y

[1] DLF N°3 de 1997 del Ministerio de Hacienda, modificado por la Ley N°21.130.

gestionar los riesgos del banco, así como implementar acciones correctivas para su gestión. Para el riesgo operacional, dicha evaluación y gestión del riesgo debe ser en base a una metodología de evaluación de probabilidad e impacto de los eventos. La función interna de gestión de riesgos del banco constituye la segunda línea de defensa, la que, de forma independiente de la primera línea, es la responsable de identificar, medir, monitorear y controlar los riesgos, así como de facilitar implementación de medidas de gestión por parte de la primera línea de defensa. Finalmente, la tercera línea de defensa corresponde a la función de auditoría interna de la entidad, cuyas responsabilidades incluyen verificar que "el marco de gobierno, de control y de riesgos es eficaz y que existen y aplican consistentemente las políticas y procesos".

Por último, el directorio debe establecer una estrategia para la gestión de riesgo operacional en todos los productos, servicios y sistemas del banco, así como previo a la implementación de nuevos negocios y en su relación con terceras partes. Se recomienda que el banco identifique claramente los principales activos de información e infraestructura física y defina políticas explícitas para el manejo del riesgo operacional que consideren el volumen y complejidad de sus actividades, el nivel de tolerancia al riesgo del directorio y las líneas específicas de responsabilidad.

Esta estrategia involucra la planificación a largo plazo de la seguridad de la información y la infraestructura tecnológica (cap. 20-10 de la RAN), tener planes de continuidad de negocios y realizar pruebas periódicas con cuantificación de las pérdidas esperadas asociadas a los riesgos operacionales (cap. 20-9 de la RAN).

**Capítulo 21-13 de la RAN sobre evaluación de suficiencia del patrimonio efectivo de bancos.**

Establece que los bancos deben llevar a cabo un proceso de autoevaluación del patrimonio mínimo en el que identificarán, medirán y agregarán sus riesgos, y determinarán el patrimonio efectivo necesario para cubrirlos en un horizonte de al menos tres años. Para ello, deberán contemplar al menos los siguientes elementos:

- Modelo de negocio y estrategia de mediano plazo.
- Marco de apetito por riesgo, aprobado por el directorio.
- Perfil de riesgo inherente, determinado a partir de la materialidad y valoración de cada riesgo. El directorio debe aprobar los modelos para la evaluación de riesgos y supervisar la realización de pruebas periódicas de tensión en distintos escenarios macroeconómicos.
- Gobierno corporativo y gestión de riesgos, aprobado por el directorio. La política de riesgos debe definir límites para las exposiciones a cada tipo de riesgo y una estructura jerárquica adecuada en la organización que permita su gestión.
- Análisis de fortaleza patrimonial, incluyendo un proceso formal de planificación de capital mínimo para la gestión de riesgos.
- Control interno, incluyendo una revisión independiente de la función de gestión de capital mínimo por medio de auditorías internas o externas.

**b) Compañías de Seguros**

**Norma de Carácter General N°309**

Establece principios de gobierno corporativo y sistemas de control interno y gestión de riesgos de las aseguradoras. La normativa define requisitos de idoneidad técnica y moral para la designación de directores, permite la delegación de tareas del directorio en comités, y requiere que el directorio apruebe la estructura organizacional, la tarificación y reservas técnicas, la política de remuneraciones, el código de ética, las políticas comerciales y los sistemas de control y auditoría internos.

En lo que respecta al sistema de gestión de riesgos, se debe considerar una definición de apetito al riesgo, estrategias y políticas de gestión de riesgos consistentes con dicha definición y una autoevaluación de riesgo y solvencia, los cuales son descritos en la Norma de Carácter General N°325. La aseguradora debe contar con funciones de auditoría interna de riesgos y de cumplimiento normativo. También se establecen otros requisitos relacionados con riesgos de reaseguro, grupo controlador y divulgación de información al mercado.

**Norma de Carácter General N°325**

El Sistema de Gestión de Riesgos (SGR) considera una Estrategia de Gestión de Riesgos establecida por el directorio, por medio de un documento escrito. En ésta, se define el apetito al riesgo de la compañía, así como las políticas y procedimientos generales del SGR.

Los principales elementos del SGR consideran, en primer lugar, la identificación y evaluación de los riesgos, cualitativa y cuantitativamente, utilizando técnicas acordes a la complejidad y escala del negocio. La aseguradora debe ser capaz de identificar las causas subyacentes a cada tipo de riesgo, las correlaciones entre ellos, así como su impacto para asegurar una adecuada gestión de capital con propósitos de solvencia. La evaluación debe tener una base prospectiva y estar basada en datos confiables y pruebas de estrés periódicas, entre otros requisitos.

El SGR también contempla límites a la exposición de cada tipo de riesgo y mecanismos de control que aseguren su cumplimiento. Dentro de los procesos de control se incluyen estrategias de cobertura de riesgos, por ejemplo, por medio de reaseguro, productos derivados u otros.

**c) Empresas de Auditoría Externa**

**Circular N°1.202**

De acuerdo al mandato del art. 170 de la Ley del Mercado de Valores, las empresas de auditoría externa deben emitir un informe sobre los mecanismos de control interno de las Entidades Aseguradoras y Reaseguradoras, de los Intermediarios de Valores y de las Administradoras Generales de Fondos fiscalizadas por la CMF cuyos estados financieros auditen.

**d) Sistemas Alternativos de Transacción de la Ley N°21.521**

**Norma de Carácter General N°502**

En la sección IV de esta normativa se establecen los requisitos de gobierno corporativo y gestión de riesgos que deberán cumplir los prestadores del servicio sistema alternativo de transacción. Al respecto, se establece el rol del directorio u órgano equivalente como responsable de que la entidad esté organizada adecuadamente, y de la implementación y funcionamiento de las funciones de gestión de riesgos y control interno.

Para esos efectos, el directorio u órgano equivalente deberá aprobar el apetito por riesgo de las entidades; las políticas de gestión de riesgos respecto a sus negocios, incluyendo disposiciones específicas de riesgo operacional; un código de ética que establezca directrices para el actuar del personal de la entidad; la conformación de Comités acordes para tratar y monitorear los aspectos relevantes del negocio; entre otros, así como velar por la adecuada implementación de las funciones de gestión de riesgos y de auditoría interna, y aprobar sus planes de funcionamiento.

## Contenido de la propuesta

La presente propuesta establece un marco para la gestión integral de riesgos, consistente con los requisitos establecidos para otras entidades supervisadas por la Comisión, y que incorpora los siguientes ámbitos:

i. **Rol del directorio**: establece la responsabilidad del directorio respecto de la implementación de lineamientos, políticas y procedimientos de gestión de riesgo, así como de velar por un adecuado ambiente interno y gobierno corporativo. Entre las disposiciones sobre procesos de control interno, o ambiente interno, se encuentran la determinación del apetito por riesgo, la estrategia de gestión de riesgo y la cultura de riesgo de la entidad.

ii. **Políticas, procedimientos y mecanismos de control**: establece las políticas, procedimientos y mecanismos de control que se consideran esenciales para garantizar la implementación de un buen marco de gestión de riesgos, junto con los elementos que garantizarán que cada una de ellas está adecuadamente diseñada.

iii. **Función de gestión de riesgos**: establece la responsabilidad de la función dentro de la organización que se encarga de velar porque las actividades del marco de gestión de riesgos sean desarrolladas adecuadamente en la entidad, y los elementos y condiciones que se deberán cumplir para garantizar que esa función se desarrolla adecuadamente. Las actividades del marco de gestión serán: i) identificación de riesgos; ii) estimación de probabilidad e impacto de los riesgos identificados; iii) definición de la respuesta para cada uno de los riesgos identificados; iv) definición de mecanismos de control asociados a los riesgos que la entidad decida aceptar; v) estimación de los riesgos residuales; vi) monitoreo de la gestión de riesgo; vii) información y comunicación de gestión de riesgos, y viii) mejoramiento continuo de la gestión de riesgos.

iv. **Función de auditoría interna:** establece la responsabilidad de la función de auditoría interna la cual provee al directorio una opinión independiente, respecto del cumplimiento, calidad y efectividad de las políticas, procedimientos, mecanismos de control, de la función de gestión de riesgos, y del cumplimiento de las disposiciones del marco regulatorio vigente que le resulten aplicables a la entidad, así como también, los elementos y condiciones que garantizarán que dicha función es desempeñada

adecuadamente.

## III. PRÁCTICAS INTERNACIONALES

La propuesta normativa considera la revisión de estudios y principios internacionales elaborados por las siguientes organizaciones: *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), *International Organization for Standardization* (ISO), *International Organization of Securities Commissions* (IOSCO) *y Organisation for Economic Cooperation and Development* (OECD).

Asimismo, se revisan las disposiciones regulatorias de similar naturaleza presentes en las legislaciones de Australia, Colombia, Estados Unidos, México, Perú y Singapur.

## COSO

La última versión de COSO[2] aborda la gestión de riesgos en conjunto con la planificación estratégica de la organización, debido a que el riesgo influye la estrategia y el rendimiento en todos los departamentos y funciones. Ese modelo tiene 5 componentes y 20 principios que se describen a continuación:

### 1. Gobernanza y Cultura

La gobernanza señala la importancia de establecer responsabilidades de supervisión para la gestión de riesgos. La cultura es plasmada en la organización por medio de una adecuada compresión de la gobernanza y los riesgos inherentes en la organización:

- El directorio proporciona supervisión de la estrategia y ejecución de las responsabilidades de gobernanza.
- La organización establece las estructuras de gobierno y de operación para el cumplimiento de la estrategia y objetivos de negocio.
- La organización define los comportamientos deseados que caracterizan la cultura deseada para ésta.
- La organización demuestra compromiso con la integridad y los valores éticos.
- La organización se compromete a desarrollar el capital humano en congruencia con la estrategia y objetivos de la entidad.

### 2. Estrategia y Establecimiento de Objetivos

Se debe establecer el apetito por riesgo en línea con la estrategia de la empresa y sus objetivos, de modo de implementar la estrategia y que esta sea la base para identificar, evaluar y responder a los riesgos:

- La organización considera el efecto potencial del contexto empresarial en el perfil de riesgo.

[2] Enterprise Risk Management: Integrating with Strategy and Performance (Executive Summary, COSO, 2017)

- La organización define el apetito de riesgo en el contexto de la creación, preservación y obtención del valor.

- La organización evalúa estrategias alternativas y el impacto en el perfil de riesgos.

- La organización considera el riesgo al establecer los objetivos de negocio en los distintos niveles que alinean y apoyan la estrategia.

**3. Desempeño**

Los riesgos que pudieren impactar negativamente en los objetivos de la estrategia deben ser identificados y evaluados en la declaración de apetito por riesgo. Así, la organización implementa medidas en base a un marco integral, en el cual los resultados del proceso son reportados a las partes interesadas respectivas:

- La organización identifica los riesgos de ejecución que afectan la estrategia y el logro de los objetivos organizacionales.

- La organización evalúa la severidad de los riesgos.

- La organización prioriza los riesgos como una base para la selección de la respuesta al riesgo.

- La organización identifica y selecciona las respuestas al riesgo.

- La organización desarrolla y evalúa una visión de portafolio de riesgos.

**4. Revisión**

Las instancias de evaluación de la organización deben incluir revisiones del marco de gestión de riesgos, identificando aquellos componentes que requieren cambios:

- La organización identifica y evalúa los cambios internos y externos que pueden tener un sustancial impacto sobre la estrategia y los objetivos de negocio.

- La organización revisa el riesgo y desempeño de la entidad.

- La organización procura un mejoramiento en el Marco de Gestión de Riesgo.

**5. Información, Comunicación y Reporte**

La implementación eficaz del proceso de gestión de riesgos requiere de recabar información de forma continua y compartirla oportunamente en la organización:

- La organización aprovecha la información y los sistemas tecnológicos para apoyar la gestión de riesgos.

- La organización usa canales de comunicación para apoyar la gestión de riesgos.

- La organización reporta sobre el riesgo, cultura y desempeño de la organización, a través de toda la entidad.

## ISO 31.000

La norma ISO 31.000:2018 Gestión del riesgo – Directrices, señala que el propósito de gestión del riesgo es la creación y protección del valor. Los principios para una gestión de riesgos eficaz son que ésta sea:

- Integrada en todas las actividades de la entidad.
- Estructurada y exhaustiva.
- Adaptada y proporcional al contexto interno y externo de la entidad.
- Inclusiva, permitiendo la participación apropiada de las partes interesadas.
- Dinámica.
- Utiliza la mejor información disponible.
- Factores humanos y culturales.
- Mejora continua.

La ISO establece un "marco de referencia", con el objeto de asistir a las organizaciones a integrar la gestión de riesgos en todas sus actividades y funciones significativas, señalando que ese marco se basa en el liderazgo y compromiso de la alta dirección y órganos de supervisión, y está determinado por:

1. **Integración**: se refiere a la integración de la gestión de riesgos en todos los niveles de la estructura de la organización y para todos sus miembros.
2. **Diseño**, el cual implica:
    - Comprensión de la organización y de su contexto interno y externo.
    - Articulación del compromiso con la gestión del riesgo mediante una política, una declaración u otras formas que expresen claramente los objetivos y el compromiso de la organización con la gestión del riesgo, dentro de la organización y a las partes interesadas.
    - Asignación de roles, autoridades, responsabilidades y obligación de rendir cuentas en la organización.
    - Asignación de recursos.
    - Comunicación y consulta, es decir, compartir información y recibir retroalimentación.
3. **Implementación** del marco de referencia, desarrollando un plan apropiado (con plazos, recursos, identificando los procesos de toma de decisiones y modificándolos cuando sea necesario).
4. **Valoración** de la eficacia del marco de referencia.
5. **Mejora**, lo cual significa adaptar el marco en función de cambios internos o externos y

procurar la mejora continua del mismo.

## IOSCO

El principio 6 de los 38 principios para la regulación del mercado de valores[3] plantea que los reguladores del mercado deben ocuparse del riesgo sistémico, porque éste puede tener un efecto negativo generalizado en los mercados financieros y en la economía, por lo cual debe tomar medidas para promover una gestión de riesgos efectiva por parte de sus fiscalizados.

Respecto de los intermediarios de mercado, se destaca lo dispuesto en los principios 30 y 31. De acuerdo a ellos, los requerimientos de solvencia que deben cumplir los intermediarios deben estar vinculados a los riesgos asumidos por éstos, quienes, a su vez, deben establecer una función que les permita gestionar adecuadamente sus riesgos.

En referencia con el mercado secundario, el principio 37 reconoce que asumir riesgos es esencial para un mercado activo, ante lo cual la regulación debe promover la gestión eficaz de éstos. A su vez, se establece que la regulación debe garantizar que los requerimientos de solvencia sean suficientes para abordar una asunción adecuada de los riesgos.

En el reporte "*Risk Management and Control Guidance for Securities Firms and their Supervisors*", IOSCO proporciona una orientación relativa a las políticas y procedimientos de gestión de riesgos y control interno para las entidades de valores y sus supervisores. Se señala que la naturaleza y el alcance de la gestión y control de riesgos tienen que adaptarse a la organización donde se desarrolla para satisfacer las necesidades de la estructura organizativa, prácticas de negocio y aversión al riesgo. Asimismo, se establecen doce recomendaciones, identificadas como los "*Elementos de un sistema de gestión y control de riesgos*", las cuales están agrupadas en cinco categorías que se consideran principios fundamentales de todo sistema de control:

### 1. El ambiente de control

Las entidades reguladas tienen que contar un mecanismo para garantizar que cuentan con controles internos de contabilidad y de gestión del riesgo. A su vez, los supervisores deben establecer un mecanismo para garantizar que los supervisados cuentan con controles internos de contabilidad y de gestión del riesgo.

Asimismo, las entidades y los supervisores deben velar que los controles estén establecidos y supervisados por la alta dirección de la empresa; que la responsabilidad de monitoreo de los controles esté claramente definida; y que la alta dirección promueva una cultura de control en todos los niveles de la organización.

### 2. Naturaleza y alcance de los controles

El diseño de controles de riesgos debe cubrir tanto controles internos de contabilidad como controles para la organización en general.

Los controles internos de contabilidad deben incluir requisitos para libros y registros, y segregación de responsabilidades de control que estén diseñadas para proteger los activos de la entidad y de sus clientes.

[3] Objectives and Principles of Securities Regulation (IOSCO, 2003)

Los controles para la organización en general deben incluir límites para la mesa de operaciones, riesgo de mercado, riesgo de crédito, riesgo legal, riesgo operacional, y riesgo de liquidez.

**3. Implementación**

Se deben entregar directrices claras desde la alta dirección hacia las unidades de negocio, en relación con los controles, lo cual debe referirse a una orientación general en los niveles más altos y una orientación específica y detallada de cómo la información fluye hacia a las unidades de negocio menores.

Las entidades deben contar con documentación sobre sus procedimientos de control, a su vez, los supervisores deben requerir dicha información.

**4. Verificación**

Las entidades y los supervisores deben velar porque los controles, una vez establecidos por la administración, operen continua y efectivamente.

Los procedimientos de verificación deben incluir auditorías internas, las cuales deben ser independientes de la mesa de negociación y del área comercial del negocio, y auditorías externas independientes. Las entidades tienen que determinar que las recomendaciones de los organismos de auditoria sean apropiadamente implementadas. A su vez, los supervisores deben llevar a cabo una verificación adicional, a través de un proceso de examinación.

Las entidades y los supervisores deben garantizar que los controles, una vez establecidos, serán adecuados para nuevos productos y tecnologías que incorporen.

**5. Reporte**

Las entidades tienen que establecer, y los supervisores exigir, mecanismos para reportar a la alta dirección y a los supervisores, las deficiencias o fallas en los controles oportunamente.

Las entidades deben estar preparadas para proporcionar a los supervisores información relevante acerca de los controles. Los supervisores deben contar con mecanismos para compartir información entre ellos.

## OECD

El reporte "*Risk Management and Corporate Governance"* de la Organisation for Economic Cooperation and Development (OECD) trata sobre la revisión de la implementación de principios de gestión de riesgos corporativos en un universo de 27 jurisdicciones que participaron en un comité de gestión de riesgos corporativos.

El reporte establece que el costo de los fallos en la gestión de riesgos está todavía subestimado, incluyendo el costo de tiempo de gestión necesario para rectificar la situación. La mayor parte de las normativas existentes de gestión de riesgo están centradas en las funciones de control, auditoría interna y riesgo financiero, apreciándose una carencia en medidas que tengan consideraciones de identificación y gestión integral de riesgos.

Al respecto, señala que un buen gobierno corporativo debe poner suficiente énfasis en la identificación y comunicación previa de los riesgos, así como prestar atención a los riesgos financieros y no financieros, abarcando los riesgos estratégicos y operativos.

De acuerdo con la apreciación de la OECD, no es siempre claro que los directorios tengan la suficiente preocupación por los riesgos potencialmente "catastróficos". En este aspecto, plantea que es necesario establecer más directrices sobre la gestión de los riesgos que merecen especial atención, como los riesgos que potencialmente tendrían grandes impactos negativos en los inversores, grupos de interés, contribuyentes, o el medio ambiente.

Finalmente, el reporte entrega una lista detallada de políticas apropiadas para el correcto desarrollo de la gestión de riesgo corporativo. Dichas políticas corresponden al capítulo V del reporte del *Financial Stability Board* (2013).

## Marco normativo extranjero

### Australia

El marco general de Gestión de Riesgos viene dado por el estándar AS/NZS 4360:1999, la AS/NZS ISO 31000:2009 y las guías RG 104 ("*Licenciamiento: Obligaciones Generales*") y RG 259 ("*Sistemas de Manejo de riesgos de entidades responsables*") de la Australian Securities and Investment Commission (ASIC), los cuales establecen principios generales para la adecuada identificación, evaluación y mitigación de riesgos para todo tipo de entidades. En particular, la RG 104 regula los requisitos para obtener la licencia "Australian Financial Services" y la RG 259 sobre la implementación de un Sistema de Gestión de Riesgos, de manera que cumplan con el requerimiento dispuesto en la s912A(1)(h) de la Corporations Act 2001 que los obliga a mantener un adecuado sistema de gestión de riesgo.

La Regulatory Guide 104 describe lineamientos para el cumplimiento de las obligaciones que le corresponden a los tenedores y postulantes a la licencia AFS, entre ellas, al referirse a mantener sistemas de gestión de riesgo, reconoce que éstos dependerán de la naturaleza, complejidad y alcance de los negocios, y espera que:

- Estén basados en un proceso estructurado y sistemático que tenga en cuenta las obligaciones que le correspondan al regulado de conformidad con la Corporations Act.
- Identifiquen y evalúen los riesgos inherentes al negocio, centrándose en los riesgos que pudieran perjudicar a los consumidores y la integridad del mercado.
- Establezcan, implementen y mantengan controles diseñados para mitigar los riesgos previamente señalados.
- Monitoreen que los controles sean efectivos.

La Regulatory Guide 259 trata específicamente sobre los sistemas de gestión de riesgo, para ello presenta principios y elementos en aspectos referidos a la implementación del sistema de gestión de riesgo, la identificación y análisis de los riesgos, y la gestión de los mismos. Se establece que el sistema de gestión de riesgos debe incluir una definición documentada del apetito al riesgo, roles y responsabilidades del personal y ser revisado al menos anualmente. La metodología de riesgos debe incluir pruebas de estrés, análisis de escenarios, análisis de datos de pérdida y gestión de cambios al interior de la entidad, incluyendo nuevos negocios y sistemas.

**Colombia**

En materia de gestión de riesgos, la Superintendencia Financiera de Colombia (SFC) toma como referencia el estándar australiano AS/NZS 4360:1999, la ISO 31000 (Gestión de Riesgos – Directrices) y las recomendaciones del Comité de Supervisión Bancaria de Basilea.

La SFC cuenta con un Marco Integral de Supervisión y las Guías de Criterio de Evaluación que lo complementan. La medición y evaluación de riesgos para todas las entidades financieras se inicia con la identificación de las Actividades Significativas del negocio de la entidad. Una vez identificadas, se analizan los riesgos inherentes a dichas actividades en los siguientes ámbitos: de crédito, de mercado, operativo, de seguros, de lavado de activos, de cumplimiento regulatorio y riesgo estratégico.

La supervisión basada en riesgos evalúa la efectividad de la estructura de gobierno de riesgo para mitigar los riesgos inherentes en dos niveles: gestión operativa y funciones de supervisión. Estas últimas corresponden a análisis financiero, cumplimiento, gestión de riesgos, actuaria, auditoría interna, alta gerencia y junta directiva.

Una vez determinado el riesgo neto global de la entidad supervisada, se realiza la evaluación del capital, la liquidez y rentabilidad de ésta para determinar los recursos con los que la entidad cuenta para asumir pérdidas, tanto esperadas como no esperadas, su capacidad de generar capital y cumplir con sus obligaciones y la adecuación de su perfil riesgo-retorno. Finalmente, la calificación de riesgo neto global de entidad combinada con la evaluación de la rentabilidad, liquidez y capital, determina el Riesgo Compuesto de la entidad.

Por su parte, la Circular Básica Jurídica establece que las entidades financieras deben contar con un Sistema de Control Interno que abarque los siguientes ámbitos: ambiente de control, gestión de riesgos, actividades de control, información y comunicación, y monitoreo. Asimismo, la Circular contiene disposiciones específicas respecto a la gestión de los riesgos operacional, de crédito y de lavado de activos y financiamiento del terrorismo para las entidades de custodia de valores, como así también la elaboración de protocolos de contingencia para todas las entidades de infraestructura.

**Estados Unidos**

De conformidad con lo establecido en la Section 404 de la Ley SOX[4], la Securities and Exchange Commission (SEC) emitió la Final Rule: Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports.[5] En esta regulación, la SEC especifica que la evaluación sobre la efectividad del control interno para efectos de los reportes financieros de las entidades listadas en bolsa en esa jurisdicción, deberá estar basado en un marco de control reconocido y adecuado, establecido por una organización que ha cumplido con procedimientos de debido proceso, incluyendo una amplia distribución del marco para comentarios del público.

La SEC explica que el marco diseñado por COSO satisface el criterio y puede ser usado para estos propósitos, sin embargo, destaca que la regulación no exige el uso particular de éste u

[4] En 2002 se emitió la Ley Sarbanes Oxley ("SOX"), la cual tuvo como propósito fortalecer la regulación de prácticas de gobiernos corporativos, financieras y de controles internos para las empresas de bolsa de Estados Unidos.

[5] *Final Rule: Management's Report on Internal Control over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports* (SEC, 2008).

otro marco, lo anterior con la intención de reconocer que podrían existir otros estándares de evaluación fuera de los Estados Unidos, o que podrían desarrollarse nuevos modelos. Por lo tanto, las sociedades cotizantes en bolsa del mercado estadounidense deben implementar un modelo de gestión de riesgos corporativos, es decir, para cumplir con la exigencia de la Ley SOX deben instaurar marcos de control, como por ejemplo el modelo de COSO.

Por otra parte, el Commercial Bank Examination Manual de la Reserva Federal (FED) explicita el énfasis en la gestión de riesgo y controles internos que utiliza esa entidad en sus labores de supervisión. Señala que se deben aplicar principios de gestión de riesgos incluyendo, pero no limitado, a riesgo de crédito, mercado, liquidez, operacional, legal y reputacional, y establece que cuando se evalúa la calidad de la gestión de riesgo, los examinadores deben tener en cuenta conclusiones relativas a los siguientes aspectos del sistema:

- Supervisión activa del directorio y la alta gerencia;
- Políticas, procedimientos y limites adecuados;
- Sistemas de medición y monitoreo del riesgo, y sistemas de información adecuados; y
- Controles internos integrales.

El manual determina que un sistema de control interno debe incluir todos los procedimientos necesarios para garantizar una oportuna detección de fallas, y esos procedimientos deben ser realizados por personal competente, quienes no deben tener funciones incompatibles con esta tarea. Así, el manual identifica los siguientes estándares como parte del control interno:

- Existencia de procedimientos que tengan como objetivo detectar fallas en los procesos de la organización.
- Desempeño competente para que el control interno sea efectivo, los procedimientos deben ser realizados por personal competente.
- Desempeño independiente, esto es independencia del personal encargado de los procedimientos.

**México**

La Comisión Nacional Bancaria y de Valores (CNBV) utiliza el estándar regulatorio del Comité de Supervisión Bancaria de Basilea y establece lineamientos generales de Gestión de Riesgos en la Ley del Mercado de Valores.

En materia de gestión de riesgos, se destaca la emisión de las "*Disposiciones de Carácter General aplicables a las Casas de Bolsa*" (2004) y la "*Guía aplicable a las solicitudes de autorización para la organización y cooperación de Casas de Bolsa*" (2015) (donde el término "casa de bolsa" en México es equivalente a intermediario).

Las principales disposiciones referidas al Sistema de Gestión de Riesgos son:

- Aprobación anual de los objetivos, lineamientos y políticas de administración integral de riesgos, los límites de exposición al riesgo y los mecanismos correctivos por el Consejo de Administración.

- Programas semestrales de revisión de límites de exposición y niveles de tolerancia al riesgo aprobados por el Directorio. Al respecto, las Casas de Bolsa deberán operar en niveles de riesgo que sean consistentes con su capital neto y capacidad operativa.

- Delimitar claramente las diferentes funciones, actividades y responsabilidades en materia de administración integral de riesgos entre sus distintos órganos sociales, unidades administrativas y personal. Lo anterior debe considerar los riesgos a los que se encuentran expuestas sus subsidiarias financieras por unidad de negocio.

- Una Unidad de Administración Integral de Riesgos independiente, encargada de identificar y evaluar los riesgos que enfrenta la entidad. La metodología de evaluación se materializa en un Manual de Administración Integral de Riesgos aprobado por el Comité de Riesgos (los riesgos se clasifican en tecnológico, de crédito, liquidez, de mercado, legal y riesgos no cuantificables).

- Un Comité de Riesgos encargado de la administración de los riesgos de la entidad. Está integrado por un miembro del Directorio, el Gerente General, el responsable de la Unidad de Administración Integral de Riesgos y el responsable de la Unidad de Auditoría Interna. Este Comité debe sesionar, al menos, mensualmente.

- Un Área de Auditoría Interna independiente, encargada de la evaluación del cumplimiento de las políticas de Gestión de Riesgos y Control Interno de la entidad.

- Un Comité de Auditoría encargado del seguimiento de las actividades de auditoría interna y externa. Está integrado con al menos dos y no más de cinco miembros del Directorio, uno de los cuales debe ser independiente. Sesiona al menos trimestralmente.

- Un Manual de Administración de Riesgo Operacional, que contiene las políticas y procedimientos para la gestión de riesgo operacional, incluyendo el mantenimiento de una Base de Incidentes y el cálculo del requerimiento de Capital por Riesgo Operacional.

- Procedimientos de seguridad de instalaciones físicas y seguridad lógica.

- Políticas de externalización de servicios de bases de datos y otros procesos operativos.

- Medidas para el control y vigilancia de acceso a los Sistemas de Información. Por ejemplo, cifrado de datos, control de perfiles de acceso a usuarios y auditorías de TI.

**Perú**

En el artículo 16-B, Administración de Integral de Riesgos, de la Ley de Mercado de Valores de Perú se determina que las entidades autorizadas por la Superintendencia del Mercado de Valores ("SMV") deben establecer un sistema de administración integral de riesgos, adecuada al tipo de negocio, de acuerdo con el Reglamento de Gestión Integral de Riesgos y otras normativas complementarias que establezca la SMV.

El Reglamento mencionado establece que las entidades financieras deberán contar con Manual de Gestión Integral de Riesgos, que debe contener los siguientes elementos principales:

- Las políticas y procedimientos de gestión integral de riesgos acordes con la estrategia de negocios, el tamaño y complejidad de operaciones de la entidad.

- La identificación de los riesgos inherentes, su importancia relativa en relación con los objetivos de la entidad y la protección de los intereses y activos de los clientes, y los mitigadores asociados, para cada una de las operaciones que desarrolla.

- Límites internos sobre los riesgos residuales más significativos, teniendo en cuenta la capacidad de riesgo de la entidad.

- Elaboración de los distintos escenarios, incluyendo el más desfavorable, que pueda enfrentar la entidad en función de los riesgos a los que se encuentran expuestas sus operaciones, y su respectivo plan de contingencia.

- La identificación de los cargos de las personas responsables de la aplicación de las políticas y procedimientos de la gestión integral de riesgos, y la descripción de las funciones que correspondan.

- Planes de continuidad de negocio y la identificación de las personas responsables de su definición y ejecución.

- Plan de seguridad de la información.

- La metodología de gestión de riesgo operacional.

- Elaboración de los procedimientos internos para comunicar al directorio, gerencia general u otros grupos de interés, según corresponda, sobre aquellos aspectos relevantes vinculados a la implementación, monitoreo y resultados de la gestión integral de riesgos.

Dentro de las responsabilidades específicas del directorio relacionadas con la gestión integral de riesgos se encuentran:

- Establecer un sistema de gestión integral de riesgos acorde a la naturaleza, tamaño y complejidad de las operaciones de la Entidad.

- Aprobar los recursos necesarios para la adecuada gestión integral de riesgos, a fin de contar con la infraestructura, metodología y personal apropiado.

- Designar al responsable de las funciones de la gestión de riesgos de la entidad, quien reportará directamente a dicho órgano o al Comité de Riesgos, según sea su organización, y tendrá canales de comunicación con la gerencia general y otras áreas, respecto de los aspectos relevantes de la gestión de riesgos para una adecuada toma de decisiones.

- Establecer un sistema adecuado de delegación de facultades, separación y asignación de funciones, así como de tratamiento de posibles conflictos de interés en la entidad.

- Velar por la implementación de una adecuada difusión de cultura de gestión integral de riesgos al personal de la entidad, mediante capacitaciones anuales sobre la normativa vigente relacionada con la gestión de riesgos; así como respecto a las políticas y procedimientos en materia de gestión de riesgos.

Los artículos 9, 10 y 13 determinan que deberá establecerse dos órganos operativos de la gestión integral de riesgos (un comité y una unidad de gestión de riesgos) y un órgano de control (auditoría interna).

Respecto del Comité de Gestión de Riesgos, se señala que podrán constituir los que el directorio u órgano equivalente considere necesarios con el objetivo de cumplir con las disposiciones del reglamento. Este comité deberá ser presidido por un director independiente y estará conformado por al menos dos miembros del directorio.

Cada entidad deberá contar con al menos un órgano, gerencia o unidad de gestión de riesgo, la cual tendrá la responsabilidad de ejecutar las políticas y procedimientos para la gestión integral de riesgos en concordancia con lo establecido en el mismo reglamento. Se establece explícitamente que la unidad de gestión de riesgos debe ser independiente de las áreas de negocios y de finanzas, prestará apoyo y asistencia al resto de las áreas en materia de gestión de riesgos y dependerá organizacionalmente del Comité de Gestión de Riesgos o, si éste no existiese, directamente del directorio.

La auditoría interna evalúa el cumplimiento de los procedimientos utilizados para la gestión integral de riesgos. Esa función, deberá también emitir un informe anual que contenga las recomendaciones que deriven de su evaluación, quedando dicho informe a disposición de la SMV.

**Singapur**

El marco general de Gestión de Riesgos para entidades financieras fiscalizadas viene dado por el estándar AS/NZS ISO 31000:2009, el "*Enterprise Risk Management – Integrated Framework*" del Committee of Sponsoring Organizations (ERM), la ISO 31000:2009 y la guía regulatoria de la Autoridad Monetaria de Singapur (MAS): "*Guía de prácticas de manejo de riesgo – Controles Internos"*.

El documento ERM-COSO establece que un sistema apropiado de gestión de riesgos debe contener:

- Gestión de riesgo y control de objetivos internos (gobernanza).
- Declaración de la actitud de la organización frente al riesgo (estrategia de riesgo).
- Descripción de la cultura de conciencia frente al riesgo o ambiente de control.
- Naturaleza y nivel de riesgo aceptado (tolerancia al riesgo), que considere las expectativas de los *stakeholders* más importantes: accionistas, directorio, administración, personal, clientes y reguladores.
- Acuerdos y organización de la gestión de riesgo (arquitectura de riesgo).
- Detalles de los procedimientos para el reconocimiento y clasificación del riesgo (evaluación del riesgo).
- Documentación para el análisis y la presentación de informes de riesgo (protocolos de riesgo).
- Requisitos de mitigación de riesgos y mecanismos de control (respuesta al riesgo).
- Asignación de roles y responsabilidades en la gestión de riesgo.
- Materias de capacitación en gestión de riesgo y prioridades.

- Criterios para el monitoreo y la evaluación comparativa de los riesgos.

- Asignación de recursos adecuados para la gestión de riesgos.

- Actividades y prioridades de riesgo para el siguiente año.

- Frecuencia de revisión de los sistemas de gestión de riesgos aplicados.

Por su parte, la guía regulatoria del MAS establece el siguiente esquema como proceso genérico de la gestión de riesgos:

- Establecer el contexto: involucra la definición de parámetros internos y externos para el proceso de gestión del riesgo. Entre los factores externos existen aspectos relacionados con la cultura, política y legislación, entre otros. Entre los factores internos, se cuentan la cultura, valores, estructura y sistemas de información de la empresa, entre otros.

- Identificar el riesgo: el objetivo de esta etapa es generar una lista exhaustiva de los riesgos inherentes basándose en aquellos eventos que podrían prevenir, degradar o retrasar el logro de los objetivos.

- Análisis y evaluación del riesgo: comprender las causas y fuentes de riesgo, su probabilidad de ocurrencia y los impactos positivos o negativos de ellas.

- Tratamiento del riesgo: determina si reduce o no el riesgo inherente a un nivel aceptable. Se puede transferir, evitar, reducir o aceptar un riesgo.

- Monitoreo y reporte: para entender cómo se han comportado los riesgos y cómo han interactuado con otros es esencial identificar, diseñar y monitorear indicadores claves (KPI) de riesgo.

- Cultura: se recomienda establecer un código de conducta que definan los límites dentro de los cuales los empleados puedan operar dentro de sus roles y responsabilidades. Asimismo, la política de remuneraciones debe estar alineada con la tolerancia al riesgo y la estrategia general de la compañía.

- Reporte anual: el directorio debe realizar una evaluación anual con el propósito de revelar la efectividad de sus sistemas de gestión de riesgos en relación al año anterior, incluyendo la extensión y frecuencia de la comunicación de los resultados del monitoreo al directorio.

El *Code of Corporate Governance* y el *Risk Governance Guidance for Listed Boards del Corporate Governance Council* establecen diversas prácticas de buen gobierno corporativo, entre los cuales se cuenta contar con un sistema de gestión de riesgos y control interno que incluyan los niveles de riesgo aceptados por el directorio; políticas, procedimientos y controles revisados al menos anualmente; un informe anual sobre la efectividad de estos controles; monitoreo continuo de la exposición de la compañía a los distintos riesgos, incluyendo la comunicación y análisis por el directorio. En relación con esto último, el directorio puede decidir gestionar los riesgos utilizando otros comités. Así, se hace referencia al Comité de Auditoría, comité de riesgos del directorio y al nombramiento de un gerente de riesgo o *Chief Risk Officer* (CRO), como posibles opciones.

# IV. CONSULTA PÚBLICA Y EMISIÓN DE NORMA FINTEC

Esta Comisión sometió a consulta pública entre el 8 de agosto y el 14 de septiembre de 2013 la propuesta normativa de Gobierno Corporativo y Gestión Integral de Riesgos para Bolsas de Valores y Bolsas de Productos[6]. Se recibieron 10 comentarios de distintas entidades, entre los cuales se cuentan a las entidades a las cuales está dirigida la normativa, corredores de bolsa, dos grupos financieros, una administradora general de fondos, y un estudio jurídico.

Al respecto, se recibieron comentarios solicitando definir metodologías o variables mínimas a considerar para la definición del "apetito por riesgo" de las entidades, así como revisar y precisar las responsabilidades de las funciones de gestión de riesgos y auditoría interna y la posibilidad de delegar dichas atribuciones a unidades corporativas.

En cuanto al primer punto, se aclara que el apetito por riesgo de las entidades corresponde al resultado de aplicar una metodología de matriz de riesgo, es decir, se deben definir los principales procesos de la entidad, los riesgos y sus niveles, y la implementación de mitigadores que permitan alcanzar el nivel de riesgo aceptado por la entidad. En cuanto a las funciones de gestión de riesgo y auditoría interna y la delegación de sus actividades, se precisó la redacción para aclarar que se permite la delegación de actividades de esas funciones a una unidad corporativa, en caso de que la entidad pertenezca a un grupo empresarial.

En cuanto al funcionamiento de los comités, se solicitó evaluar la prohibición de participar en los Comités de Gestión de Riesgos y de Auditoría Interna por parte de una misma persona; así como la posibilidad de delegar estos comités en unidades corporativas. Al respecto, se estimó necesario mantener esta prohibición para los miembros del directorio, de manera de asegurar la segregación de las líneas de defensa de las entidades. Sin embargo, no se estableció esta restricción para el resto de los miembros de los comités.

Otros comentarios tenían relación con que se permitiera que el directorio de las entidades determinara la periodicidad para la revisión de las políticas a implementar, así como de los informes que debe presentar la función de gestión de riesgos y los reportes de incumplimientos.

Se estimó mantener la revisión anual por parte del directorio de las políticas contenidas en la normativa (eliminándose la revisión de procedimientos por éste); sin embargo, se modificó el plazo de los informes que debe presentar la función de gestión de riesgos a una periodicidad trimestral. Esto con la finalidad de mantener la simetría regulatoria con los prestadores de servicios financieros de la Ley N°21.521, regulados por la Norma de Carácter General N°502.

Por otra parte, se recibieron comentarios solicitando incorporar elementos de proporcionalidad aplicable para prestadores de servicios financieros de la Ley N°21.521, bajo la premisa de neutralidad tecnológica. No obstante, dada la naturaleza sistémica de las entidades a las que está dirigida la normativa no se incorporaron excepciones a la propuesta normativa.

Finalmente, se solicitó revisar ciertas políticas que eran más bien materias de la gestión de riesgos de los corredores; lo cual fue revisado y subsanado; se consultó respecto a si las políticas contenidas en la normativa deberán ser aprobadas por la Comisión, para lo cual se

[6] La versión que fue sometida a consulta pública se encuentra disponible en https://www.cmfchile.cl/institucional/legislacion_normativa/normativa_tramite_ver_archivo.php?id=2023080851&seq=1

aclara que no es el caso, puesto que no corresponden a políticas que regulen la operación de las bolsas, sino que son políticas referentes a su gestión de riesgos y gobierno corporativo; y se consultó respecto a si el código de conducta de la propuesta normativa correspondía al código de autorregulación de la Norma de Carácter General N°424, comentario que fue incorporado en esta versión, considerando que el código de autorregulación ya contenía las normas de conducta consideradas en la propuesta normativa puesta en consulta.

## V. PROPUESTA NORMATIVA

## A. TEXTO DEFINITIVO

***"REF:*** ***IMPARTE INSTRUCCIONES SOBRE GOBIERNO CORPORATIVO Y GESTIÓN INTEGRAL DE RIESGOS PARA BOLSAS DE VALORES Y BOLSAS DE PRODUCTOS. MODIFICA NORMA DE CARÁCTER GENERAL N°480.***

_____

# *NORMA DE CARÁCTER GENERAL N° xxx*

***[día] de [mes] de [año]***

***A todas las bolsas de valores y bolsas de productos.***

*Esta Comisión, en uso de las facultades conferidas en el Decreto Ley N°3.538, la Ley N°18.045 y la Ley N°19.220, y teniendo en consideración que su mandato legal es velar por el correcto funcionamiento, desarrollo y estabilidad del mercado financiero, ha estimado pertinente impartir las siguientes instrucciones respecto del gobierno corporativo y gestión de riesgos para las bolsas de valores y bolsas de productos.*

*Las bolsas de valores y productos, con el objeto de que puedan gestionar adecuadamente los riesgos que afectan al giro exclusivo que el marco legal les ha encomendado, deberán contar, al menos, con las políticas, procedimientos, controles, estructura organizacional y roles a las que se refiere esta normativa.*

## *I. ROL DEL DIRECTORIO*

*El directorio, como órgano de administración, es el responsable de establecer la estructura organizacional, objetivos y políticas que permitan gestionar adecuadamente los riesgos que pueden afectar las actividades que desarrolle la entidad (marco de gestión de riesgos), debiendo asegurarse de contar con una apropiada cultura de gestión de riesgos, entendida como la adecuada comprensión del gobierno corporativo y la gestión de riesgos inherentes a la entidad. Los miembros del directorio deberán contar con los conocimientos, experiencia y dedicación adecuados a este respecto.*

*El directorio deberá dar cumplimiento, al menos, a los principios y elementos que se señalan a continuación:*

***1.*** *Establecer la misión, visión y objetivos estratégicos, teniendo en consideración las responsabilidades que el marco regulatorio vigente establece para la entidad.*

***2.*** *Aprobar anualmente los niveles de apetito por riesgo de aquellos previamente identificados. Una efectiva definición debiera cuantificar el nivel de riesgo que el directorio desea aceptar en consideración a los objetivos estratégicos de la entidad, los intereses de sus corredores y las responsabilidades que le son aplicables por el marco regulatorio. Además, deberá informarse continuamente del cumplimiento del apetito por riesgo.*

***3.*** *Aprobar las políticas que se señalan en las secciones II, III y IV de esta normativa, considerando para ello:*

***3.1.*** *Que las políticas de gestión de riesgos sean coherentes con la misión, visión, objetivos estratégicos, niveles de apetito por riesgo y el marco regulatorio que le es aplicable a la entidad.*

***3.2.*** *Que las políticas estén alineadas con estándares internacionales de común aceptación o mejores prácticas.*

***3.3.*** *Que las políticas se revisen y actualicen al menos anualmente, o con la frecuencia necesaria en caso de que se produzcan cambios significativos, tales como cambios en la regulación aplicable a la entidad o la introducción de nuevos productos o servicios.*

***4.*** *Velar por que la administración de la entidad establezca los procedimientos que permitan implementar las políticas aprobadas por el directorio. Dichos procedimientos deberán ser aprobados por el gerente general, o por un comité integrado por al menos un miembro del directorio, y ser actualizados cuando el directorio modifique las políticas relacionadas al procedimiento.*

***5.*** *Aprobar las normas de conducta contenidas en el código de autorregulación de la Norma de Carácter General N°424.*

***6.*** *Establecer una estructura organizacional adecuada para la gestión de riesgos de la entidad, que considere lo siguiente:*

***6.1.*** *La definición de los roles, competencias y responsabilidades que permitan realizar sus actividades y gestionar adecuadamente los riesgos que enfrenta la entidad. Lo anterior involucra la segregación apropiada de los deberes y las funciones claves, especialmente aquéllas que, si fueran realizadas por una misma persona, puedan dar lugar a errores que no se detecten o que expongan a la entidad o sus corredores a riesgos no deseados o no mitigados y controlados; y entre las áreas generadoras de riesgo y de control de éstos.*

***6.2.*** *La implementación de la función de gestión de riesgos, de conformidad con lo establecido en la sección III.*

***6.3.*** *La implementación de la función de auditoría interna, de conformidad con lo establecido en la sección IV.*

***6.4.*** *La implementación de la función de auditoría a corredores, de conformidad con lo establecido en la sección V.*

***6.5.*** *El cumplimiento de la segregación de funciones y la independencia entre las funciones de gestión de riesgos, de auditoría interna y de auditoría a corredores.*

***7.*** *Contar con Comités de Auditoría Interna y de Gestión de Riesgos, este último referido a la gestión de todos los riesgos objeto de esta normativa, incluido el riesgo operacional. Sin perjuicio de ello, el directorio deberá evaluar la pertinencia de conformar otros comités que le permitan analizar y monitorear aspectos relevantes de los negocios y la gestión de los riesgos, referidos a materias tales como, por ejemplo: Auditoría Interna; Prevención del Lavado de Activos, Financiamiento del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva; Inversiones y Nuevos Servicios o Productos.*

*El directorio deberá establecer los procedimientos para la conformación y funcionamiento de los comités, los cuales deberán quedar debidamente documentados, como también sus actuaciones, las que deberán ser reportadas al directorio en forma continua, siendo responsabilidad exclusiva de este último la adopción de decisiones sobre los temas tratados. Sin perjuicio de lo anterior, los Comités de Gestión de Riesgos y de Auditoría Interna deberán estar integrados al menos por un miembro del directorio. Ningún miembro del directorio podrá participar del Comité de Gestión de Riesgos y del Comité de Auditoría Interna al mismo tiempo.*

*La actuación de los comités que se conformen, en las materias antes mencionadas, deberá constar por escrito en actas, las que deberán reflejar con claridad los asuntos tratados.*

***8.*** *Asegurar que las actas den cuenta de las principales temáticas tratadas en las sesiones del directorio y los comités. Todo el material que se elabore o presente al directorio o los comités, deberá estar debidamente documentado y archivado de conformidad a las normas generales aplicables en la materia, y estar permanentemente disponible para su examen a solicitud de esta Comisión.*

***9.*** *Aprobar el plan anual de la función de gestión de riesgos y estar en conocimiento, en forma oportuna, de su cumplimiento y de los informes que elabore.*

***10.*** *Aprobar el plan anual de la función de auditoría interna y estar en conocimiento, en forma oportuna, de su cumplimiento y de los informes que elabore.*

***11.*** *Aprobar el plan anual de la función de auditoría a corredores y estar en conocimiento, en forma oportuna, de su cumplimiento y de los informes que elabore.*

***12.*** *Establecer una política de contratación y capacitación del personal de la entidad, de forma de contar con recursos humanos calificados. Esta política deberá considerar:*

***12.1.*** *La adecuada difusión de los valores, principios organizacionales y marco de gestión de riesgos de la entidad, con apego a las disposiciones legales y normativas vigentes.*

***12.2.*** *La capacitación continua en relación con las actividades que realiza el personal de la entidad.*

***13.*** *Establecer sistemas de registro y procesamiento de información con medidas de protección y seguridad adecuadas que permitan que:*

***13.1.*** *El directorio tenga acceso oportuno a información relacionada con el desarrollo del negocio, la gestión de riesgos, y toda otra información relevante para el cumplimiento de sus funciones.*

***13.2.*** *Las áreas de negocios y las funciones de gestión de riesgos, de auditoría interna y de auditoría a corredores tengan acceso a información relevante para el cumplimiento de sus funciones.*

***13.3.*** *La entidad dé cumplimiento a la divulgación de información que el marco regulatorio le exige.*

***14.*** *Mantener comunicaciones con la empresa de auditoría externa para conocer los avances en el plan de trabajo y analizar los principales hallazgos detectados.*

**15.** *Evaluar periódicamente la suficiencia de recursos de las funciones de gestión de riesgos, de auditoría interna y de auditoría a corredores para efectuar su labor, aprobar la asignación de los recursos necesarios para dichas funciones y monitorear el grado de cumplimiento del presupuesto asignado a tal fin.*

## *II. POLÍTICAS, PROCEDIMIENTOS Y MECANISMOS DE CONTROL*

## *II.1. ASPECTOS GENERALES*

*Las políticas, procedimientos y mecanismos de control de la entidad, deberán tener en cuenta los siguientes principios:*

**1.** *Establecer políticas, procedimientos y controles operativos efectivos que guarden relación con la actividad diaria, y respecto de cada uno de los negocios o actividades que se desarrolle.*

**2.** *Las políticas deberán exponer los principios generales y directrices establecidas por el directorio para orientar las actividades de la organización.*

**3.** *Los procedimientos deberán definir cómo llevar a cabo un proceso, con el fin de asegurar el cumplimiento de las políticas aprobadas por el directorio. Para ello, deberán incorporar, al menos: la descripción de las actividades principales que lo componen y la identificación de sus responsables; determinación de los responsables de supervisar y controlar el resultado de las actividades ejecutadas; documentación que evidencia la ejecución de las actividades que conforman los procedimientos; definición y descripción de los controles asociados a dichas actividades. En el caso de actividades externalizadas, siempre deberá existir una persona responsable dentro de la organización respecto al control de éstas.*

**4.** *Las políticas, procedimientos y mecanismos de control deberán estar formalmente establecidos y documentados, siendo consistentes con los niveles de apetito por riesgo que haya definido la entidad.*

**5.** *Las políticas y procedimientos de gestión de riesgo operacional deberán formar parte de las políticas y procedimientos de gestión de riesgos de la entidad, de acuerdo con la normativa de gestión de riesgo operacional emitida por esta Comisión.*

## *II.2. POLÍTICAS Y PROCEDIMIENTOS MÍNIMOS A IMPLEMENTAR*

*La entidad deberá contar, al menos, con las políticas y procedimientos que se detallan a continuación.*

### *II.2.1. Mantención de instrumentos elegibles para transar en sistemas bursátiles*

*Se deberán definir políticas y procedimientos que permitan velar por que los instrumentos sujetos a negociación en los sistemas bursátiles cumplan con los requisitos establecidos por el marco legal y normativo vigente para su transacción en los sistemas bursátiles.*

### *II.2.2. Cumplimiento de requisitos legales y normativos de funcionamiento*

*Se deberán definir políticas y procedimientos que especifiquen la forma en que se monitoreará y garantizará el debido cumplimiento de los requisitos legales y normativos aplicables a la entidad.*

*Además, se deberá definir procedimientos en caso de presentarse eventos de incumplimiento de los requisitos legales de funcionamiento, los cuales deberán ser informados oportunamente a la Comisión.*

### *II.2.3. Inversión de recursos propios en instrumentos financieros*

*Se deberán establecer políticas y procedimientos en las que se definan los criterios de elegibilidad, concentración, límites u otros para la inversión de recursos propios en instrumentos financieros, tales como tipo de instrumento, plazo, clasificación de riesgo, presencia bursátil, entre otros; y la forma en que se controlará el cumplimiento de estos criterios y límites. Al respecto, cumpliendo con el principio de minimizar el riesgo de inversión, la entidad deberá procurar que sus inversiones se realicen en activos de bajo riesgo de crédito, mercado y liquidez. En el caso de que la administración de las inversiones sea delegada a un tercero, se deberá definir los requisitos mínimos que deberán cumplir estos administradores.*

### *II.2.4. Acceso directo al mercado*

*En el caso que se permita el acceso directo al mercado a los clientes de los corredores, se deberán establecer políticas y procedimientos que regulen dicho acceso, las que deberán considerar al menos los siguientes requisitos:*

1. *Posibilitar la identificación de las órdenes ingresadas por cada cliente con acceso directo al mercado, aunque éstas no hayan sido calzadas, de forma que exista trazabilidad íntegra de las órdenes.*

2. *Requerir que los intermediarios que permitan el acceso directo al mercado establezcan procedimientos reforzados para la identificación de conductas de abuso de mercado que puedan efectuar los clientes con acceso directo al mercado. En caso de identificarse dichas conductas, deberán ser comunicadas sin demora a la entidad y a esta Comisión.*

3. *Mantener registros que permitan identificar a las personas con acceso directo al mercado, considerando a lo menos, cédula de identidad, RUT o similar en caso de ser un cliente extranjero; nombres y apellido o razón social; representante legal, de ser el caso; persona natural con facultades suficientes para operar en la cuenta; nacionalidad; dirección y cualquier otra información que permita la identificación del cliente con acceso directo y sus apoderados.*

4. *Establecer mecanismos que permitan suspender operativamente en forma oportuna a los clientes con acceso directo al mercado por motivos calificados.*

5. *Establecer la responsabilidad del corredor por las ofertas y operaciones que el cliente con acceso directo al mercado efectúe en éste.*

### *II.2.5. Utilización de algoritmos en la negociación*

*En caso de permitirse la negociación algorítmica, las bolsas deberán verificar el cumplimiento por parte de sus corredores de los requisitos establecidos para estos efectos en la normativa de gobierno corporativo y gestión integral de riesgos para intermediarios.*

### *II.2.6. Prevención del lavado de activos, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva*

*Las entidades deberán contar con políticas y procedimientos para el cumplimiento de las disposiciones legales y normativas relativas a la prevención del lavado de activos, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva, según lo dispuesto en la Ley N°19.913 y en la normativa dictada por la Unidad de Análisis Financiero.*

### *II.2.7. Integridad de mercado*

*Se deberán establecer políticas y procedimientos destinados a:*

1. *La identificación de conductas de abuso de mercado, de aquellas establecidas en los cuerpos legales que regulan las transacciones que se efectúan en la entidad, las que deberán ser comunicadas oportunamente a esta Comisión.*

2. *El monitoreo del adecuado funcionamiento del mercado, debiendo ser reforzado en caso de permitirse el acceso directo al mercado y/o la negociación algorítmica.*

3. *La identificación y denuncia a esta Comisión, de las conductas de abuso de mercado establecidas en los cuerpos legales que regulan su actividad.*

### *II.2.8. Introducción de nuevos servicios, productos, líneas de negocio, procesos o sistemas*

*Se deberá contar con políticas y procedimientos referidos a la implementación de nuevos productos, servicios, líneas de negocios, procesos o sistemas, que consideren al menos:*

1. *La verificación del cumplimiento del giro exclusivo o si corresponde a una actividad complementaria aprobada.*

2. *La evaluación del riesgo de su implementación y los posibles mitigadores.*

3. *La verificación del adecuado funcionamiento de los servicios y los sistemas e infraestructuras vigentes.*

4. *La revisión y adecuación de los planes de continuidad.*

5. *La evaluación de la compatibilidad con la misión, visión y objetivos estratégicos, y con la gestión de tecnologías de información y comunicación.*

6. *La verificación de la mitigación de riesgos de ciberseguridad.*

### *II.2.9. Garantías de operaciones especiales*

*En caso de requerirse garantías para operaciones especiales que se efectúen en los sistemas de negociación, se deberán establecer políticas y procedimientos referidos a:*

1. *La metodología utilizada para la determinación de garantías.*

2. *La metodología para la valorización de los instrumentos entregados en garantía.*

***3.*** *La elegibilidad de los instrumentos a entregar en garantías.*

***4.*** *La revisión periódica de las metodologías.*

***5.*** *Las pruebas retrospectivas para determinar la suficiencia de las garantías.*

### *II.2.10. Custodia de instrumentos propios y de terceros*

*Se deberán establecer políticas y procedimientos que tengan por objeto velar por:*

***1.*** *El cumplimiento íntegro de las disposiciones legales, normativas y reglamentarias que rigen la actividad de custodia, incluyendo la protección de los activos de terceros ante pérdidas productos de errores o fallas en los sistemas, en las personas y en los procesos.*

***2.*** *El mantenimiento de un registro de custodia con información de saldos y operaciones de sus activos mantenidos en custodia, incluyendo: transacciones y movimientos autorizados por el cliente, posiciones mantenidas por el cliente, transferencias y conciliaciones de valores efectuadas por la entidad, entre otros. La información contenida en el registro de custodia debe ponerse a disposición del cliente en forma veraz, suficiente y oportuna, de forma tal que el cliente conozca cómo se conservan sus activos y las medidas de salvaguarda de los mismos. Los activos registrados en el registro de custodia deben corresponder a los activos que el intermediario mantiene efectivamente por cuenta del cliente.*

***3.*** *La segregación de las cuentas y activos de los clientes de los activos de la entidad, de manera que los activos de los clientes estén claramente identificados y no se pueda hacer uso no autorizado de los activos de terceros en custodia.*

***4.*** *La gestión adecuada de los eventos de capital y societarios permitiendo el ejercicio de estos derechos y/o su entrega inmediata a su legítimo dueño.*

*Anualmente, se deberá contratar a una empresa de auditoría externa, de aquellas inscritas en el Registro de Empresas de Auditoría Externa de esta Comisión, para la revisión de los procesos y controles asociados a la actividad de custodia. Las empresas de auditoría externa deberán emitir un informe, el que deberá contener su opinión respecto a si los procesos y controles fueron diseñados adecuadamente para resguardar los activos en custodia y si están operando con suficiente efectividad, para otorgar una seguridad razonable que, durante el período bajo revisión, se lograron los objetivos de control. Asimismo, el informe deberá contener una descripción general del control interno, una mención a los objetivos de control y una descripción detallada de los controles asociados, las pruebas aplicadas y el resultado de las mismas.*

*La revisión deberá contemplar pruebas de los controles existentes durante un período mínimo de 6 meses en el transcurso de los doce meses anteriores a la emisión del informe. El trabajo de la empresa de auditoría externa deberá realizarse en conformidad con las normas de auditoría. El informe de las empresas de auditoría externa deberá ser remitido esta Comisión a más tardar el 30 de septiembre de cada año y ser difundido a partir de esa fecha, por un medio que asegure su fácil acceso por parte de las personas que mantengan custodia.*

*Si la evaluación de la empresa de auditoría externa determina que existen deficiencias en el diseño u operación de los controles, se deberán adoptar las medidas correctivas y obtener una nueva evaluación en un plazo máximo de cuatro meses de efectuada la evaluación anterior.*

*Las empresas de auditoría externa que realicen este tipo de revisiones deberán contar con documentación escrita de la metodología y procedimientos aplicados para este tipo de revisiones, la que deberá estar disponible a solicitud de la Comisión. De igual forma, las empresas de auditoría externa deberán contar con antecedentes que le permitan demostrar que las personas que efectúan este tipo de revisiones cuentan con la capacitación apropiada y experiencia en el tema.*

*La empresa de auditoría externa que realice la auditoría anual de los estados financieros de la entidad podrá efectuar esta revisión.*

### *II.2.11. Gestión de consultas y reclamos*

*Contar con políticas y procedimientos para la recepción, gestión y resolución de consultas, denuncias y reclamos de sus clientes, trabajadores y el público en general, incluyendo denuncias de incumplimiento al código de conducta o de autorregulación, que permitan resguardar la reserva de quien las formule. Dicha política deberá definir claramente cómo se calificará la gravedad o relevancia de las denuncias o reclamos, y cómo se comunicarán a las instancias que correspondan. El directorio deberá mantenerse informado de los reclamos y denuncias relevantes.*

### *II.2.12. Divulgación de información*

*Contar con un procedimiento de divulgación de información que otorgue a sus clientes, proveedores de servicios y entidades de infraestructura información veraz, suficiente y oportuna para la gestión de sus propios riesgos, tanto aquella que el marco regulatorio vigente le exige divulgar como aquella que adicionalmente la entidad estime necesaria. Dicho procedimiento considerará la frecuencia de actualización de esa información.*

## *III. FUNCIÓN DE GESTIÓN DE RIESGOS*

## *III.1. DISPOSICIONES GENERALES*

*La función de gestión de riesgos tiene por objeto que las actividades del proceso de gestión de riesgos sean desarrolladas adecuadamente en la entidad, conforme a las políticas y procedimientos establecidos para dicho efecto (marco de gestión de riesgo). Además, deberá verificar el cumplimiento del marco legal y normativo aplicable a las bolsas y su reglamentación interna.*

*El marco de gestión de riesgo deberá tener como propósito gestionar eficazmente los riesgos que se presentan en el desarrollo de su negocio, como por ejemplo el riesgo general del negocio, riesgo operacional y riesgo reputacional, entre otros. Las políticas, procedimientos y sistemas de gestión de riesgos deberán cautelar además el cumplimiento de los requisitos establecidos en leyes y normativas aplicables, así como en los reglamentos que regulan el funcionamiento de las bolsas.*

*Para el desarrollo de sus actividades, se deberá dar cumplimiento, al menos, a los principios y elementos que se señalan a continuación:*

***1.*** *La función de gestión de riesgos deberá ser independiente de las áreas generadoras de riesgos, de la función de auditoría interna y de la función de auditoría a corredores; y contar con línea de responsabilidad directa al directorio.*

*En el caso que la entidad pertenezca a un grupo empresarial, la función de gestión de riesgos podrá delegar algunas de las actividades bajo su responsabilidad a la unidad de gestión de riesgos corporativa, en la medida que ésta tenga un conocimiento acabado del marco de gestión de riesgos y ambiente de control de la entidad y que cumpla con los requisitos establecidos en la presente normativa, lo cual deberá ser acordado por el directorio. Se deberá considerar la pertinencia respecto a la idoneidad de la unidad respectiva del grupo empresarial que se encargará de la actividad, en relación al cumplimiento de los requisitos establecidos en esta norma y los conflictos de intereses que pudieran generarse, y, de ser el caso, su mitigación y/o eliminación.*

*Sin perjuicio de lo anterior, la función de gestión de riesgos de la entidad será siempre responsable de las actividades delegadas, debiendo revisar y aprobar los informes realizados al respecto, para lo cual deberá hacerse de toda la documentación relevante.*

***2.*** *La función de gestión de riesgos deberá contar con recursos adecuados al volumen y complejidad de las operaciones de la entidad.*

***3.*** *El personal encargado de la función de gestión de riesgos deberá contar con experiencia y conocimientos comprobables en estándares o mejores prácticas de común aceptación para la gestión de riesgos y de los riesgos específicos que debe gestionar de acuerdo al marco de gestión de riesgos.*

***4.*** *La función de gestión de riesgos deberá proponer políticas y procedimientos para la gestión de riesgos al directorio, consistentes con la misión, visión, objetivos estratégicos y las responsabilidades que el marco regulatorio le asigna.*

***5.*** *La función de gestión de riesgos deberá contar con procedimientos que describan la metodología y herramientas utilizadas para cuantificar, agregar y gestionar los riesgos que enfrenta la entidad, los cuales deberán evaluarse al menos anualmente y en forma prospectiva, incluyendo escenarios tales como cambios en las condiciones económicas, legales, regulatorias, tecnológicas y situaciones de crisis. Además, deberá contar con metodologías y herramientas que le permita verificar el cumplimiento de las políticas, procedimientos y mecanismos de control.*

***6.*** *La naturaleza, el alcance y oportunidad de las actividades que la función de gestión de riesgos desarrollará deberá estar contenida en un plan anual, el que deberá ser aprobado por el directorio. En todo caso, dicho plan deberá ser actualizado cada vez que se produzcan cambios significativos, tales como, cambios en la regulación aplicable a la entidad o la introducción de nuevos productos o servicios.*

***7.*** *La función de gestión de riesgos deberá promover una cultura organizacional responsable en el ámbito de gestión de riesgo, que comprenda programas periódicos de difusión, concientización y capacitación, que contribuyan a que el personal de la entidad, incluyendo al directorio y personal externo que realice funciones críticas para la organización, comprenda los riesgos atingentes a sus funciones, y cuál es su contribución a la efectividad de la gestión de dichos riesgos.*

***8.*** *La función de gestión de riesgos deberá disponer de sistemas de información que optimicen el desarrollo de sus actividades, los que deberán permitir al menos:*

***8.1.*** *Registrar sus actividades, el plan de trabajo y los resultados de éstos.*

***8.2.*** *Respaldar la documentación que evidencie el desarrollo de las actividades realizadas.*

***8.3.*** *Efectuar seguimiento del cumplimiento de los compromisos adquiridos por las distintas áreas, procesos o líneas de negocio auditados, incluyendo la generación de alertas que faciliten el control de los plazos asociados.*

***8.4.*** *Controlar la actualización periódica de políticas y procedimientos.*

## *III.2. PROCESO DE GESTIÓN DE RIESGO*

*El proceso de gestión de riesgos considerará las siguientes actividades principales:*

***1.*** *Identificación de procesos en los que se descomponen las actividades efectuadas por la entidad, y los respectivos responsables de dichos procesos (mapa de procesos).*

*La función de gestión de riesgos, en conjunto con los encargados de los procesos principales, deberá identificar formalmente los riesgos inherentes a los que se expone la entidad en el desarrollo de sus actividades.*

***2.*** *Medición de los riesgos inherentes identificados en las actividades efectuadas por la entidad. Para ello deberá elaborarse una matriz de riesgos que permita estimar una probabilidad de ocurrencia e impacto de los riesgos, como también calificar su severidad considerando estos factores.*

***3.*** *Definición de los mecanismos de control para mitigar los riesgos inherentes identificados. Al respecto, dichos mecanismos de control deberán considerar:*

***3.1.*** *Descripción de cada control y su objetivo.*

***3.2.*** *Identificación de los responsables del control formalmente designados para esos efectos.*

***3.3.*** *Calificación de la efectividad de los controles para la mitigación de los riesgos inherentes, por una instancia independiente del responsable de los mismos.*

***4.*** *Cuantificación de los riesgos residuales, los que será determinado a partir de los riesgos inherentes considerando la calificación de la efectividad de los controles.*

***5.*** *Definición del tratamiento de los riesgos residuales, para lo cual se deberá tener en consideración los niveles de apetito por riesgo.*

***6.*** *Monitoreo de los riesgos y controles establecidos, considerando al menos:*

***6.1.*** *Definición y medición de indicadores clave de evaluación de riesgos.*

***6.2.*** *Procedimientos de monitoreo continuo de riesgos que permitan identificar oportunamente una posible materialización de riesgos por encima de los niveles de apetito por riesgo definidos. Para ello, la entidad deberá implementar un mecanismo de alertas basado en los indicadores clave de riesgos.*

***6.3.*** *Comunicación oportuna de las deficiencias de los controles y la desviación del riesgo residual respecto a los niveles de apetito por riesgo definidos a los responsables de aplicar las medidas correctivas, incluyendo los comités a los que se refiere la sección I y al directorio en el caso de deficiencias significativas.*

***6.4.*** *Seguimiento continuo de las medidas correctivas que se hubieren definido para las deficiencias identificadas en el proceso de monitoreo de riesgos, para que éstas sean efectivamente implementadas en los plazos establecidos.*

***7.*** *Elaboración de procedimientos de información y comunicación de la gestión de riesgos que asegure que la información relevante acerca de la efectividad de los controles mitigantes y el cumplimiento de los niveles de apetito por riesgo llegue al directorio y a todas las partes interesadas.*

***8.*** *Programa de mejoramiento continuo de la gestión de riesgos, con el objeto de evaluar la necesidad de realizar cambios frente a nuevos escenarios económicos, financieros, legales, regulatorios y tecnológicos que vaya enfrentando la entidad; cambios del perfil de riesgo y producto de la implementación o cambios en los estándares o mejores prácticas internacionales de común aceptación para la gestión de riesgo.*

## *III.3. REPORTES*

*La función de gestión de riesgos deberá informar al directorio, al menos trimestralmente, o con una periodicidad mayor, según defina éste, respecto al funcionamiento del sistema de gestión de riesgo, del nivel de exposición a los distintos riesgos y los eventuales incumplimientos a las políticas, procedimientos y controles de gestión de riesgos ocurridos durante el periodo que se informa. Se incluirá recomendaciones de mejora que permitan mantener los riesgos por debajo de los niveles de apetito por riesgo definidos en caso de que pudieran materializarse distintos escenarios.*

## *IV. FUNCIÓN DE AUDITORÍA INTERNA*

*La función de auditoría interna tiene por objeto verificar el correcto funcionamiento del sistema de gestión de riesgos y su consistencia con los objetivos, políticas y procedimientos de la organización, como también del cumplimiento de las disposiciones legales y normativas que le son aplicables a la entidad.*

*Para el desarrollo de sus actividades, se deberá dar cumplimiento, al menos, a los principios y elementos que se señalan a continuación:*

***1.*** *La función de auditoría interna deberá ser independiente de las áreas generadoras de riesgos, de la función de gestión de riesgos y de la función de auditoría a corredores; y contar con línea de responsabilidad directa al directorio.*

*En el caso que la entidad pertenezca a un grupo empresarial, la función de auditoría interna podrá delegar algunas de las actividades bajo su responsabilidad a la unidad de auditoría interna corporativa, en la medida que éste tenga un conocimiento acabado del marco de gestión de riesgos y ambiente de control de la entidad y que cumpla con los requisitos establecidos en la presente normativa, lo cual deberá ser acordado por el directorio. Previo a la delegación de cada actividad, la función de auditoría interna deberá pronunciarse respecto a la idoneidad de la unidad respectiva del grupo empresarial que se encargará la actividad, el cumplimiento de los requisitos establecidos en esta norma y los conflictos de intereses que pudieran generarse, y, de ser el caso, su mitigación y/o eliminación.*

*Sin perjuicio de lo anterior, la función de auditoría interna de la entidad será siempre responsable de las actividades delegadas, debiendo revisar y aprobar los informes realizados al respecto, para lo cual deberá hacerse de toda la documentación relevante.*

***2.*** *El personal encargado de la función de auditoría interna deberá tener experiencia y conocimientos comprobables en marcos de gestión de los riesgos específicos que deberá auditar.*

***3.*** *La función de auditoría interna deberá contar con procedimientos que describan la metodología de auditoría interna, la cual deberá considerar al menos los siguientes aspectos:*

***3.1.*** *La naturaleza, alcance y oportunidad de las auditorías.*

***3.2.*** *Los programas de trabajo de auditoría.*

***3.3.*** *Las categorías utilizadas para calificar las observaciones detectadas.*

***3.4.*** *El seguimiento que se efectuará a las observaciones detectadas.*

***3.5.*** *La forma en que se reportarán las deficiencias significativas al directorio.*

***3.6.*** *La elaboración y estructura de los informes que la función de auditoría interna realice.*

***4.*** *La existencia y ejecución de un plan anual de auditoría que incluya la naturaleza, alcance y oportunidad de las actividades que la función de auditoría interna desarrollará, y considerar:*

***4.1.*** *Que las áreas, procesos, líneas de negocio o riesgos más relevantes sean auditados periódicamente, incluyendo la función de gestión de riesgos y la función de auditoría a corredores.*

***4.2.*** *El seguimiento al cumplimiento de los compromisos adquiridos por las áreas auditadas en revisiones anteriores.*

***5.*** *La función de auditoría interna deberá emitir un informe semestral al directorio que considere:*

***5.1.*** *Respecto de las áreas, procesos, líneas de negocio o riesgos auditados durante el periodo:*

***a.*** *La calidad y efectividad de las políticas, procedimientos y mecanismos de control.*

***b.*** *El resultado de las auditorías efectuadas con su respectiva calificación.*

***5.2.*** *Las acciones o medidas propuestas para subsanar las observaciones levantadas y el plazo estimado para su implementación.*

***5.3.*** *Fecha de la última auditoría realizada a cada unidad auditable.*

***5.4.*** *Respecto de la función de gestión de riesgos:*

***a.*** *La efectividad del sistema de gestión de riesgos.*

***b.*** *Los incumplimientos de políticas y procedimientos de gestión de riesgos detectados en las auditorías, las causas que los originaron y las acciones correctivas adoptadas para evitar su reiteración.*

***5.5.*** *El resultado del seguimiento de la corrección de las situaciones detectadas en las auditorías realizadas.*

*El informe deberá ser remitido al directorio en un plazo no superior a 30 días corridos de finalizado el periodo al cual se refiere. Lo anterior, sin perjuicio de la información mensual que la función de auditoría interna le pueda proporcionar al directorio, de forma de mantenerlo informado de la labor de esta función.*

***6.*** *La función de auditoría interna deberá disponer de sistemas de información que optimicen el desarrollo de sus actividades, los que deberán permitir al menos:*

***6.1.*** *Registrar sus actividades, programas de trabajo y los resultados de éstos.*

***6.2.*** *Respaldar la documentación que evidencie el desarrollo de las actividades realizadas.*

***6.3.*** *Efectuar seguimiento del cumplimiento de los compromisos adquiridos por las distintas áreas, procesos o líneas de negocio auditados, incluyendo la generación de alertas que faciliten el control de los plazos asociados.*

## *V. FUNCIÓN DE AUDITORÍA A CORREDORES*

***1.*** *Las bolsas deberán implementar una función de dedicación exclusiva, destinada a realizar auditorías a sus corredores miembros, la cual deberá contar con los recursos humanos y materiales necesarios para formarse una opinión fundada respecto de la calidad de la gestión de riesgos y de cumplimiento normativo de, al menos, el 35% de esos corredores por año, sin perjuicio de las demás auditorías que corresponda efectuar a sus corredores miembros de acuerdo a lo definido en sus procesos o normativa interna.*

***2.*** *La metodología que se deberá emplear para esos procesos de auditoría deberá estar formalmente implementada y considerar, como mínimo, la revisión de la gestión del riesgo operacional, financiero y legal, entre otros; el cumplimiento normativo (en particular el asociado al servicio de custodia); la planificación de la auditoría (plazos e hitos relevantes); y la elaboración de informes de los resultados de la auditoría.*

***3.*** *A más tardar el 31 de diciembre de cada año, las bolsas deberán remitir a esta Comisión la información respecto a su planificación anual a ejecutar de auditorías a corredores. Asimismo, dentro del quinto día hábil de cada mes, se deberá remitir el estado de ejecución de la planificación anual.*

***4.*** *Previo al inicio de una auditoría a un corredor, la entidad deberá informar tal situación a esta Comisión, indicando el nombre del corredor, objetivo de la auditoría y personas que participan en la auditoría.*

***5.*** *Una vez concluida la auditoría, deberá remitir el informe dando cuenta del trabajo desarrollado, las conclusiones obtenidas, las observaciones que fueron representadas al intermediario y la respuesta a dichas observaciones por parte de este último.*

*Estas comunicaciones deberán ser efectuadas de acuerdo a las instrucciones del anexo técnico disponible en la página web de esta Comisión.*

## *VI. MODIFICACION*

*Elimínese los numerales 5 y 6 de la letra b) de la sección III de la Norma de Carácter General N°480.*

## *VII. VIGENCIA*

*Las instrucciones establecidas en la presente Norma de Carácter General rigen a contar del 1 de febrero de 2025.*

***SOLANGE BERSTEIN JÁUREGUI***
***PRESIDENTA***
***COMISIÓN PARA EL MERCADO FINANCIERO***

## *ANEXO N° 1: DEFINICIONES*

*Para la identificación de riesgos de esta norma se deberá tener en consideración las siguientes definiciones:*

***Apetito por riesgo**: nivel agregado y tipos de riesgos que una entidad está dispuesta a asumir, previamente decidido, y dentro de su capacidad de riesgo, a fin de lograr sus objetivos estratégicos y plan de negocio.*

***Confidencialidad de la información:** protección de los datos contra el acceso y la divulgación no autorizados, definido por el directorio. Incluye los medios para proteger la privacidad personal y la información reservada, en especial de los clientes de la entidad.*

***Encargado del proceso:** corresponde a aquella persona designada para hacerse responsable de la administración de un proceso y propiciar las mejoras a implementar en éste.*

***Eventos de capital:** derechos patrimoniales que derivan de un valor determinado, tales como dividendos, emisiones liberadas o pagadas de acciones, repartos de capital, sorteos, prepagos, intereses, amortizaciones totales o parciales, y cualquier otro beneficio o derecho económico asociado a un valor. Se incluyen también bajo esta misma definición los eventos que confieran al tenedor el ejercicio de derecho a voto y otros.*

***Instancia:** se refiere a un nivel o grado de la estructura organizacional de la entidad, esto incluye, comité, unidad, división, departamento u otro equivalente.*

***Partes interesadas:** se refiere a las personas u organizaciones que se relacionan con las actividades y decisiones de una empresa, tales como empleados, proveedores, clientes, reguladores, entre otros.*

***Proveedor de servicios:** entidad relacionada o no a la institución contratante, que preste servicios o provea bienes e instalaciones a éste.*

***Riesgo aceptado:** corresponde al nivel de riesgo que la entidad está dispuesta a aceptar en concordancia con la política de gestión de riesgos y sus responsabilidades establecidas en el marco legal que las rige.*

***Riesgo de crédito:** potencial exposición a pérdidas económicas debido al incumplimiento por parte de un tercero de los términos y las condiciones estipuladas en el respectivo contrato, convención o acto jurídico. Este riesgo se divide en las siguientes subcategorías:*

- *Riesgo de contraparte: exposición a potenciales pérdidas como resultado de un incumplimiento de contrato por diferencias o derivado o del incumplimiento de una contraparte en una transacción dentro de un proceso de compensación y liquidación.*
- *Riesgo crediticio del emisor: exposición a potenciales quiebras o deterioro de solvencia en los instrumentos financieros de una entidad.*

***Riesgo de custodia:** exposición a pérdidas potenciales debido a negligencia, malversación de fondos, robo, pérdida o errores en el registro de transacciones efectuadas con valores de terceros mantenidos en custodia.*

***Riesgo de liquidez:*** *riesgo que una parte no liquide una obligación por su valor total cuando ésta venza sino en una fecha posterior no determinada.*

***Riesgo de mercado:*** *riesgo de registrar pérdidas debido a variaciones en los precios de mercado.*

***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 operacional:*** *corresponde al riesgo de que las deficiencias que puedan producirse en los sistemas de información, los procesos internos o el personal, o las perturbaciones ocasionadas por acontecimientos externos provoquen la reducción, el deterioro o la interrupción de los servicios que presta la entidad y eventualmente le originen pérdidas financieras. Incluye el riesgo de pérdidas ante cambios regulatorios que afecten las operaciones de la entidad, como también pérdidas derivadas de incumplimiento o falta de apego a la regulación vigente.*

***Riesgo reputacional:*** *riesgo de deterioro en la percepción de clientes, contrapartes, accionistas, inversores y otras partes interesadas acerca de la capacidad de la entidad para mantener o establecer relaciones comerciales y/o acceder en forma continua a fuentes de financiamiento.*

***Riesgo residual:*** *corresponde al nivel de riesgo remanente que existe sin perjuicio de haberse implementado las medidas de control."*

# VI. EVALUACION DE IMPACTO REGULATORIO

IOSCO señala que, para controlar el riesgo sistémico, los reguladores deben tomar medidas para promover una gestión de riesgos efectiva por parte de sus fiscalizados[7], a la vez que reconoce que asumir riesgos es esencial para un mercado secundario activo[8].

La implementación de un adecuado marco de gestión de riesgos (procedimientos, recursos, infraestructura y sistemas para identificar y mitigar la materialización de los riesgos inherentes) es fundamental para que las entidades puedan lograr su visión, misión, valores y objetivos estratégicos, cumpliendo con sus obligaciones. La adecuada gestión de riesgos contribuye a la solvencia financiera y sostenibilidad de la entidad, y así a la estabilidad del mercado financiero en su conjunto.

La presente propuesta normativa establece que las funciones de gestión de riesgos y auditoría interna sean llevadas a cabo por unidades o áreas independientes de la entidad. Ello podría eventualmente requerir la contratación o capacitación de personal. No obstante, la propuesta permite que dichas funciones sean llevadas a cabo por la unidad corporativa del grupo empresarial al que pertenece la entidad, siempre que sus actividades estén adecuadamente segregadas entre sí y respecto de las áreas comerciales de la entidad.

Al respecto, se observa que los fiscalizados han ido internalizando previamente los costos de incorporar formalmente las unidades mencionadas y otros requisitos al ámbito de la gestión de riesgos:

- La reciente norma de Interconexión de Bolsas de Valores[9] establece la obligatoriedad de contar con unidades de gestión de riesgos y auditoría interna.

- La Bolsa de Valores de Santiago cuenta con requisitos específicos de gestión de riesgos producto de su certificación con normas ISO.

- La Bolsa de Productos actualmente no cuenta con una exigencia explícita de unidades de gestión de riesgos o auditoría interna, pero se estima que los costos de incorporarlas no serían significativos considerando que ya cuenta con disposiciones relativas a la gestión de riesgos. En particular, el Reglamento de la Bolsa de Productos exige contar con un sistema de fiscalización de corredores con una evaluación y seguimiento de los riesgos operacionales, liquidación de las operaciones, custodia, riesgos normativos y riesgos tecnológicos.

Dentro de los beneficios de la propuesta se destacan los siguientes:

- La prevención y monitoreo de riesgos significaría un beneficio económico para la entidad y sus clientes, traduciéndose en indicadores de liquidez, rentabilidad, solvencia y cobertura financiera más robustos. Ello mejoraría la viabilidad financiera de la entidad en el mediano plazo.

- Asimismo, la prevención de riesgos fortalecería la confianza de los clientes, mitigando el riesgo reputacional. También permitiría mitigar el riesgo legal derivado de incidentes

[7] Objectives and Principles of Securities Regulation (IOSCO, 2017). Principio 6

[8] Objectives and Principles of Securities Regulation (IOSCO, 2017). Principio 37.

[9] NCG N° 480 (CMF, 2022)

que pudieran afectar la integridad y exactitud de la información que maneja la entidad para fines de cumplimiento regulatorio.

- Un marco regulatorio integrado para la gestión de riesgos a nivel de industria permitiría reconocer externalidades positivas derivadas de la gestión coordinada de fallas operacionales o filtraciones de datos que tengan el potencial de generar riesgos de contagio en todo el sistema financiero.

Por último, en relación con la propia CMF, la propuesta:

- Permitiría un fortalecimiento de la supervisión de la gestión de riesgos de estas entidades y una mejor focalización de los recursos del supervisor.

- Adecuaría la regulación local a los estándares internacionales de gestión de riesgos.

- Tendría costos adicionales de supervisión, destacándose el incremento en horas-hombre destinadas al monitoreo del cumplimiento de los planes de acción anuales comprometidos por las entidades para mitigar sus riesgos.

COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

**www.cmfchile.cl**