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 Intermediarios de Valores y Corredores de Bolsas de Productos – Modificación NCG N°510

Diciembre 2024

www.CMFChile.cl

Contenido

I. INTRODUCCIÓN Y OBJETIVO DE LA PROPUESTA

Como parte 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 alguno de los riesgos identificados.

La presente propuesta normativa tiene por objetivo actualizar el marco de Gestión Integral de Riesgos para Intermediarios de Valores y hacerlo extensivo a Corredores de Bolsas de Productos, en el marco de la metodología de supervisión basada en riesgos.

Asimismo, se modifica la Norma de Carácter General N°510 de Gestión de Riesgo Operacional de entidades del Mercado de Valores, incorporando a dicho marco a los Intermediarios de Valores y Corredores de Bolsas de Productos, de manera que estas entidades lleven a cabo las acciones necesarias para la gestión de incidentes y registro de pérdidas operacionales.

Todo lo anterior, con el objetivo de 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 tamaño, volumen, naturaleza de los negocios y riesgos que enfrenta cada entidad, y otorgando a éstas un alto grado de certeza respecto de cuáles serán las exigencias que le resultarán aplicables por parte de esta Comisión.

II. DIAGNÓSTICO Y MARCO NORMATIVO LOCAL

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

a) Actualizar el marco integral de gestión de riesgos para Intermediarios de Valores y Corredoras de Bolsas de Productos, a fin de homogeneizar el tratamiento regulatorio en esta materia respecto a Bolsas de Valores, Bolsas de Productos, Administradoras Generales de Fondos y entidades de Infraestructura del mercado financiero.

b) Establecer un marco de gestión de riesgo operacional para Intermediarios de Valores y Corredoras de Bolsa de Productos, subsanando de esta forma la asimetría regulatoria con otras entidades que ya cuentan con dicho marco.

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

d) Establecer un marco normativo que permite la adecuada supervisión basada en riesgos de estas entidades, incluyendo la evaluación de la calidad de gestión de riesgos realizada por esta Comisión.

A continuación, se describe el marco normativo local aplicable a la gestión de riesgos, existente para Intermediarios de Valores:

Ley del Mercado de Valores N°18.045

El art. 31 establece que corresponderá a la Comisión establecer, mediante norma de carácter general, los estándares de gobierno corporativo y gestión de riesgos para quienes están inscritos en el registro de corredores. Corresponderá a cada entidad implementar los estándares conforme a su tamaño, volumen y naturaleza de sus negocios, y riesgos.

Ley Fintec N°21.521

El art. 28 establece que los intermediarios de valores y corredores de bolsa de productos deberán adoptar políticas, procedimientos y controles tendientes a evitar la oferta de productos que no sean acorde a las necesidades, expectativas y disposición al riesgo que sus clientes hayan previamente comunicado respecto a los productos que desean adquirir.

Para esos efectos, las entidades pueden solicitar a los clientes información que permita evaluar su experiencia como inversionista, su situación financiera y su objetivo de inversión, sin perjuicio del deber de informar acerca de las características y riesgos asociados a las inversiones.

A su vez, toda información, propaganda o publicidad que las entidades efectúen respecto a su oferta de productos o servicios no podrá contener declaraciones, alusiones o representaciones que induzcan a error o causen confusión respecto a las características del producto o servicio.

Por su parte, el N°5 del art. 32 de la Ley N°21.521 establece cambios a la Ley N° 18.045, donde se faculta a la CMF para que, mediante norma de carácter general, fije los estándares de gobierno corporativo y gestión de riesgo, para todas aquellas empresas que se inscriban en el Registro de Corredores de Bolsa o de Agentes de Valores.

Del mismo modo, el N°3 del art. 42 de la misma ley, modifica la Ley N°19.220 que regula el establecimiento de Bolsas de Productos, incorporando el deber para Corredores de Bolsas de Productos de contar con un gobierno corporativo, controles internos y sistemas de gestión de riesgos a efectos de inscribirse en el Registro de Corredores de Bolsas de Productos de la CMF.

Norma de Carácter General N°502

Esta normativa regula el registro y autorización para la prestación de servicios financieros de la ley Fintec, los requisitos en materia de gestión de riesgos y gobierno corporativo, capital y garantías y las obligaciones de divulgación y entrega de información a los clientes y al público en general.

La normativa establece un marco para el gobierno corporativo y la gestión de riesgos, diferenciado según el tipo de servicio y la escala de operaciones de las entidades (esto último, mediante una definición de bloques asociados al volumen de negocios -clientes, transacciones, monto custodiado). Los requisitos mencionados, en términos generales, están referidos a: rol del directorio u órgano equivalente; las políticas, procedimientos y mecanismos de control mínimos; y las funciones de gestión de riesgo y auditoría interna.

Circular N°2.054

Establece los requisitos de organización, control interno y gestión de riesgos de Intermediarios, los cuales pueden adaptarse según el tamaño del Intermediario y la complejidad de su negocio. Los principales requisitos son los siguientes:

I. Políticas, procedimientos y controles que aseguren la protección de los activos y registros relacionados con la continuidad operacional del intermediario y el manejo de conflictos de interés.

II. Función de gestión de riesgos, encargada de implementar un sistema de gestión de riesgos financieros, operacionales y de cumplimiento normativo adecuado al nivel y complejidad de las operaciones del intermediario. Dicha función puede ser llevada a cabo por un miembro de la alta administración u otro funcionario del Intermediario, pero si el volumen de operaciones o la complejidad de productos ofrecidos es significativa, dicha función debe ser llevada a cabo por una unidad independiente de las unidades operativas y de negocios.

III. Manual de gestión de riesgos, con la descripción de las políticas de gestión y monitoreo de riesgos, la matriz de riesgos del intermediario y los planes de continuidad operacional.

IV. Unidad de auditoría interna, encargada de verificar el correcto funcionamiento del sistema de control interno y gestión de riesgos y su consistencia con los objetivos y políticas de la organización. Esta función depende directamente de la Alta Administración y tiene independencia respecto a las áreas operativas y de negocios del intermediario.

V. Implementación y funcionamiento del Sistema de Control Interno y Gestión de Riesgos a cargo de la Alta Administración, debiendo revisar al menos una vez al año las políticas y procedimientos de dicho sistema. Asimismo, la alta administración debe tomar conocimiento de los reportes emitidos por la unidad de auditoría interna y la función de gestión de riesgos y aprobar sus planes anuales.

VI. Certificación Anual de suficiencia e idoneidad de la estructura de control interno y gestión de riesgos, firmada por el gerente general y los representantes de la alta administración.

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. El marco de gestión de riesgos aplicable a bolsas de valores, bolsas de productos, AGF, empresas de depósito y custodia de valores, y sociedades administradoras de sistemas de compensación y liquidación de instrumentos financieros, serán abordados en sus respectivos informes normativos.

a) Bancos

Capítulo 1-13 de 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, financiamiento del terrorismo *y financiamiento de la proliferación de armas de destrucción masiva;* administración de la estrategia de negocios; 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 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 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 RAN).

Capítulo 21-13 de 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 interno y auditoría interna.

En lo que respecta al sistema de gestión de riesgos, se debe considerar una definición de apetito por 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 por 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) Prestadores de Servicios Financieros (Ley N°21.521)

Norma de Carácter General N°502

Esta normativa regula el registro y autorización para la prestación de servicios Fintec; los requisitos en materia de gestión de riesgos y gobierno corporativo, capital y garantías y las obligaciones de divulgación y entrega de información a los clientes y al público en general.

Marco de gestión de riesgos operacionales existente en la regulación chilena

a) Bancos

RAN Capítulo 1-13

Establece disposiciones generales relativas a la evaluación de la Administración de Riesgo Operacional realizada por los bancos. 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.

Asimismo, el capítulo recomienda contar con una función encargada de la evaluación y gestión de riesgo operacional en base a una metodología de evaluación de probabilidad e impacto, y una función de Auditoría Interna que evalúe el desempeño de la primera para que se adopten medidas correctivas de manera oportuna.

RAN Capítulo 20-7

Contiene pautas de carácter general relativas a servicios externalizados y, en forma particular, a la tercerización de servicios de procesamiento de datos y resguardos adicionales en el caso de servicios en la nube. La norma señala las condiciones que debe cumplir una entidad ante la decisión de externalizar un servicio, contempla requisitos esenciales respecto a los sitios de procesamiento; los aspectos de continuidad del negocio, seguridad de la

información propia y de sus clientes; entre otros. En cuanto a este último aspecto, la entidad bancaria debe exigir al proveedor asegurar la confidencialidad, integridad, trazabilidad y disponibilidad de sus activos de información y la de sus clientes.

RAN Capítulo 20-8

Establece lineamientos para la información que las entidades supervisadas a las que la misma aplica, deben remitir ante la ocurrencia de incidentes operacionales relevantes que afecten la continuidad del negocio, la seguridad de la información o la imagen de la institución y, además, señala las condiciones mínimas que se deben considerar para el desarrollo y mantención de bases de información respecto de incidentes de ciberseguridad. El 31 de agosto de 2018 se introdujeron cambios que perfeccionan el sistema de reporte de incidentes, creando una plataforma digital especialmente establecida por la CMF para reportar los incidentes al regulador en un plazo máximo de 30 minutos. Adicionalmente, se definió la obligación de designar un encargado de nivel ejecutivo para comunicarse con la CMF en todo momento.

RAN Capítulo 20-9

Contempla una serie de lineamientos para la adecuada gestión de los riesgos de continuidad del negocio, teniendo en cuenta el volumen y la complejidad de las operaciones de las entidades supervisadas a las que la misma aplica. De esta manera, indica la debida existencia de una estrategia aprobada por la máxima instancia de la entidad, de una función de riesgos que se encargue de este ámbito en conjunto con instancias colegiadas de alto nivel, de una estructura para el manejo de situaciones de crisis, de la evaluación de escenarios mínimos de contingencia, entre otros. Dentro de los escenarios de contingencia para los cuales se deben definir y probar planes se encuentran los "ataques maliciosos que afecten la ciberseguridad". Incluye la operatoria de los sitios de procesamiento de datos como parte de los aspectos relevantes que contribuyen a fortalecer la resiliencia operacional de las entidades.

RAN Capítulo 20-10

Contiene una serie de disposiciones, basadas en las mejores prácticas internacionales, que deben ser consideradas para la gestión de la seguridad de la información y ciberseguridad. Entre otros, se definen lineamientos específicos respecto del rol que debe tener el Directorio para la adecuada gestión, tanto de seguridad de la información como de ciberseguridad, otorgándole como responsabilidad la aprobación de la estrategia institucional en esta materia, junto a la responsabilidad de asegurar que las entidades mantengan un sistema de gestión de la seguridad de la información y ciberseguridad. Asimismo, se establece la necesidad de que las entidades definan sus activos críticos, así como las funciones de protección de éstos, la detección de las amenazas y vulnerabilidades, la respuesta ante incidentes y la recuperación de la operación normal de la entidad; además de disponer de políticas y procedimientos para la identificación de aquellos activos que componen la infraestructura crítica de la industria financiera y del sistema de pagos, y para el adecuado intercambio de información técnica de incidentes que afecten o pudieran afectar la ciberseguridad de la entidad.

b) Compañías de Seguros

Norma de Carácter General N°454

Establece que las compañías aseguradoras cuenten con un Marco de Gestión de Riesgo operacional, el que debe ser parte del sistema de gestión de riesgos de la compañía y estar debidamente documentado. El marco debe incluir una declaración de apetito de riesgo operacional con un enfoque basado en tres líneas de defensa: actividades del negocio, supervisión y monitoreo de riesgos, y auditoría interna. Dentro de este marco debe incluirse una estrategia de gestión de ciberseguridad y contar con un profesional responsable de la implementación de dicha estrategia.

La norma requiere la adopción de las siguientes prácticas internacionales en materia de ciberseguridad:

a) Identificar riesgos cibernéticos dentro de las funciones y procesos organizacionales. Las aseguradoras deberán mantener un inventario de activos de información. Los activos deberán ser clasificados en términos de su criticidad, considerando su confidencialidad, integridad y disponibilidad. Dentro de este mapeo se deben considerar derechos de acceso individual, dependencias y proveedores externos, así como procesos de inversión, adquisiciones y cambios.
b) Identificar las áreas operativas de la aseguradora expuestas a riesgo cibernético. Este proceso se puede organizar por medio de las siguientes categorías descritas en la norma: (1) tecnologías y tipos de conexión; (2) canales de entrega; (3) características organizacionales; y (4) amenazas externas.
c) Implementar tecnologías y procesos de respaldo y almacenamiento de datos acorde con su criticidad.
d) La aseguradora deberá verificar que sus proveedores externos protejan los datos de los servicios prestados en el mismo grado que se esperaría de la aseguradora.
e) Identificar proactivamente los riesgos cibernéticos de su entorno, actualizando sus política y procesos dinámicamente.

En materia de comunicación de incidentes operacionales, estos deberán ser reportados a la Comisión, tanto al inicio como al cierre de este. La compañía deberá informar a los clientes y usuarios de la aseguradora, actualizando la información hasta que el incidente sea superado. Adicionalmente, la aseguradora deberá compartir información relevante con las entidades de la industria con la finalidad de resguardar a los clientes y al sistema en su conjunto.

c) Prestadores de Servicios Financieros (Ley N°21.521)

Norma de Carácter General N°502

Esta normativa, además de regular el registro y autorización para la prestación de servicios Fintec, y los requisitos en materia de gestión de riesgos y gobierno corporativo, en particular establece requisitos para la gestión de seguridad de la información y ciberseguridad, continuidad del negocio, gestión de servicios externalizados, y el deber de reporte de incidentes operacionales.

d) Entidades del Mercado de Valores

Norma de Carácter General N°510

La NCG N°510[1] establece un marco de gestión de riesgo operacional para Bolsas de Valores, Bolsas de Productos, Administradoras Generales de Fondos, Sociedades Administradoras de Sistemas de Compensación y Liquidación y Entidades de Depósito y Custodia de Valores, de manera que dichas entidades estén preparadas para gestionar el riesgo operacional en los siguientes ámbitos:

- **Seguridad de la Información y Ciberseguridad:** Gestión de eventos que afecten las infraestructuras y sistemas informáticos de la entidad (instalaciones físicas, activos de información, hardware, software).

- **Continuidad del negocio:** Gestión de eventos relacionados con interrupciones o fallas en las operaciones del negocio, incluyendo su comunicación oportuna a los reguladores y al mercado.

- **Subcontratación de proveedores de servicios:** Gestión de eventos operacionales de un proveedor de servicios que afecten la seguridad de la información y ciberseguridad y/o la continuidad del negocio de la entidad.

- **Reporte de pérdidas e incidentes operacionales:** Las entidades deberán comunicar a la Comisión los incidentes operacionales que afecten la continuidad del negocio, los recursos e información de la entidad o de sus clientes y la calidad de los servicios. También, deberán enviar la información de pérdidas operacionales mayores a 150 Unidades de Fomento. La propuesta normativa dispone de anexos técnicos para el reporte de perdidas e incidentes operacionales.

[1] Disponible en Norma de Carácter General N°510.

III. CONTENIDO DE LA PROPUESTA

La presente propuesta establece, por una parte, un marco sobre gobierno corporativo y gestión integral de riesgos para Intermediarios de Valores y Corredores de Bolsas de Productos, y por otra parte, incorpora a estas entidades al marco existente de gestión de riesgo operacional contenido en la Norma de Carácter General N°510.

Respecto al marco de gobierno corporativo y gestión integral de riesgos, éste considera los siguientes ámbitos:

i. **Rol del directorio u órgano equivalente:** establece la responsabilidad del directorio o alta administración 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 u órgano equivalente, una opinión independiente, respecto del cumplimiento, calidad y efectividad de las políticas, procedimientos, mecanismos de control, de la función de gestión de riesgo, 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.

v. **Evaluación de la calidad de la gestión de riesgos:** de acuerdo al mandato legal de la Ley Fintec, la Comisión deberá establecer un proceso de evaluación de la calidad de gestión de riesgos para Intermediarios de Valores y Corredores de Bolsas de Productos. Esta evaluación se efectuará respecto a los estándares de gobierno corporativo y gestión de riesgos establecidos en la presente normativa y formará parte del proceso de supervisión basada en riesgos de la Comisión. El resultado de la evaluación representará, a su vez, un elemento que permitirá activar medidas preventivas, en caso de que los riesgos de las entidades evaluadas no estén debidamente gestionados, de manera tal que se pueda presumir efectos negativos en la solvencia de la entidad, en la fe pública o en la estabilidad financiera. Entre otros requisitos, en caso de presentarse deficiencias en la evaluación de gestión de riesgos, la Comisión podrá solicitar requisitos de gestión de riesgos adicionales

o aumentar el porcentaje de activos ponderados por riesgo que deban constituir las entidades llegando hasta un 6%, para efectos del patrimonio mínimo regulatorio.

Respecto al marco de gestión de riesgo operacional, éste contempla los siguientes ámbitos:

i. **Seguridad de la Información y Ciberseguridad:** Gestión de eventos que afecten las infraestructuras y sistemas informáticos de la entidad (instalaciones físicas, activos de información, hardware, software).

ii. **Continuidad del negocio:** Gestión de eventos relacionados con interrupciones o fallas en las operaciones del negocio, incluyendo su comunicación oportuna a los reguladores y al mercado.

iii. **Subcontratación de proveedores de servicios:** Gestión de eventos operacionales de un proveedor de servicios que afecten la seguridad de la información y ciberseguridad y/o la continuidad del negocio de la entidad.

iv. **Reporte de pérdidas en incidentes operacionales:** Las entidades deberán comunicar a la Comisión los incidentes operacionales que afecten la continuidad del negocio, los recursos e información de la entidad o de sus clientes y la calidad de los servicios. También, deberán mantener un registro e informar las pérdidas operacionales mayores a 150 Unidades de Fomento. La propuesta normativa dispone de anexos técnicos para el reporte de perdidas e incidentes operacionales.

IV. CONSULTA PÚBLICA

Esta Comisión sometió a consulta pública[2] entre el 8 de julio y el 22 de agosto de 2024 una propuesta normativa que regula el gobierno corporativo y gestión integral de riesgos para los Intermediarios de Valores y Corredores de Bolsas de Productos. En este proceso consultivo se recibieron comentarios de distintas entidades y asociaciones de la industria. En ese mismo periodo, también se puso en consulta pública una modificación de la NCG N°510[3] que fija los requerimientos de gestión de riesgo operacional de entidades del mercado de valores, con el fin de incorporar bajo su marco a los Intermediarios de Valores y Corredores de Bolsas de Productos.

En el caso de la nueva normativa de gobierno corporativo y gestión integral de riesgos para los Intermediarios de Valores y Corredores de Bolsas de Productos, cabe señalar que el intermediario podrá utilizar las políticas de gobierno corporativo y gestión de riesgos establecidas para el grupo empresarial, como así también integrar los comités de directorio u órgano equivalente a nivel de grupo empresarial. Lo anterior, previo manejo de potenciales conflictos de intereses.

Respecto de la posibilidad de que la CMF solicite a la entidad una certificación o evaluación de gobierno corporativo y gestión de riesgos o un informe de procedimiento acordado, se precisa en el texto de la norma que sólo podrán ser elaborados por empresas inscritas en el Registro de Empresas de Auditoría Externa de esta Comisión.

En lo que respecta a la metodología de evaluación de calidad de gestión de riesgos, cabe destacar que el resultado de la evaluación no será público y que las "mejores prácticas" o "altos estándares" en las categorías de evaluación deben entenderse como las mejores prácticas y estándares en gestión de riesgos y riesgo operacional descritos en este informe normativo.

Así mismo, se precisa la redacción para aclarar que el contenido del código de ética podrá ser abordado en el código de autorregulación de la Norma de Carácter General N°424 y otros documentos de la entidad.

Con respecto a la normativa de gestión de riesgo operacional (NCG N°510), se incorporó en dicha norma un plazo máximo de 2 horas desde que una entidad toma conocimiento de un incidente operacional para informarlo a la CMF. No obstante, cabe señalar que este reporte no exime al intermediario de los reportes y plazos correspondientes solicitados por otras normativas o cuerpos legales, tales como, la normativa que regula el Sistema de Finanzas Abiertas o la Ley Marco de Ciberseguridad.

Finalmente, se precisó que el monto de las pérdidas operacionales a informar es bruto y no neto.

---

[2] Disponible en: CMF publica en consulta normas sobre gobierno corporativo y gestión integral de riesgos, y gestión de riesgo operacional para entidades del mercado de valores - CMF Chile - Prensa y Presentaciones

[3] Disponible en: Informe Normativo NCG N°510

V. PROYECTO NORMATIVO

A. NORMA DE GESTION INTEGRAL DE RIESGOS PARA INTERMEDIARIOS DE VALORES Y CORREDORES DE BOLSA DE PRODUCTOS

REF: IMPARTE INSTRUCCIONES SOBRE GOBIERNO CORPORATIVO Y GESTIÓN INTEGRAL DE RIESGOS PARA CORREDORES DE BOLSA DE VALORES, AGENTES DE VALORES Y CORREDORES DE BOLSAS DE PRODUCTOS. DEROGA CIRCULAR N°2.054 DE 2011.

NORMA DE CARÁCTER GENERAL N°XXX

[día] de [mes] de [año]

A todos los corredores de bolsa de valores, agentes de valores y corredores de bolsas de productos

Esta Comisión, en uso de las facultades conferidas en el Decreto Ley N°3.538, la Ley N°18.045, la Ley N°19.220 y la Ley N°21.521, 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 los corredores de bolsa de valores, agentes de valores y corredores de bolsas de productos (en adelante, todos conjuntamente, intermediarios).

I. INTRODUCCIÓN

El desarrollo de la actividad de intermediación conlleva que los intermediarios asuman distintos riesgos, los que pueden llegar a afectar su patrimonio o el de los clientes.

En este contexto, se hace necesario que los intermediarios cuenten con la estructura organizacional y los medios materiales y humanos adecuados al tamaño, volumen y naturaleza de sus negocios y riesgos que enfrentan. Asimismo, deben mantener sistemas de control interno y gestión de riesgos que sean compatibles con los objetivos establecidos por la propia entidad, que permitan una adecuada gestión de los riesgos que enfrenta el intermediario en sus negocios, la protección de los activos e intereses de sus clientes y el cumplimiento de las disposiciones legales y normativas que le son aplicables.

Las disposiciones contenidas en esta norma deben entenderse como los requerimientos mínimos que los intermediarios deben cumplir en materia de control interno y gestión de riesgos para el desarrollo de su giro, debiendo al mismo tiempo dichos intermediarios, promover la mejora continua del sistema de gestión de riesgos.

II. RESPONSABILIDAD DEL DIRECTORIO U ÓRGANO EQUIVALENTE

El directorio u órgano equivalente (en adelante el "directorio"), es el principal responsable de que la entidad esté adecuadamente organizada, y de la implementación y funcionamiento del sistema de control interno y gestión de riesgo del intermediario. También deberá promover que tanto el intermediario como sus funcionarios cumplan los procedimientos y normas definidos.

Para esos efectos, el directorio deberá dar cumplimiento, al menos, a los principios y elementos de gestión de riesgos que se señalan a continuación, conforme al tamaño, volumen, naturaleza de los negocios y riesgos de la entidad:

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

***2.** Conocer y comprender los riesgos inherentes a los negocios y actividades que desarrolla el intermediario.*

***3.** Aprobar y revisar al menos una vez al año, o con una mayor frecuencia si es necesario, el apetito a los riesgos identificados, verificando que aquellas definiciones permitan a la entidad cumplir con sus obligaciones legales y objetivos estratégicos.*

***4.** Aprobar y revisar al menos una vez al año, o con una mayor frecuencia si es necesario, políticas de gestión de riesgos y control interno que sean coherentes con los objetivos estratégicos, el marco regulatorio, los valores organizacionales y el apetito al riesgo definido y la utilización de buenas prácticas en materia de gestión de riesgos asociados a los servicios prestados por los intermediarios.*

***5.** Aprobar el código de ética, que dé cuenta de los valores y principios organizacionales y establezca directrices en el actuar del personal de la entidad. Este código de ética podrá adherir a estándares y prácticas reconocidas en códigos de ética internacionales para la industria de inversiones. Las materias mencionadas en el código de ética también podrán ser abordada en otros documentos de la entidad como, por ejemplo, el código de autorregulación dispuesto en la Norma de Carácter General N°424 en el caso de los intermediarios de valores.*

***6.** Contar con un comité de gestión de riesgos compuesto al menos por un director (o miembro del órgano equivalente). Sin perjuicio de ello, el directorio deberá evaluar la pertinencia de conformar comités u otras instancias, que le permitan analizar y monitorear aspectos relevantes de los negocios, referidos a materias tales como auditoría, prevención del lavado de activos, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva, inversiones, nuevos productos, continuidad del negocio, seguridad de la información y ciberseguridad, entre otros.*

***7.** El directorio establecerá los procedimientos para la conformación y funcionamiento de los comités, los cuales deberán quedar debidamente documentados. Sin perjuicio de ello, los comités de gestión de riesgos y de auditoría (éste último, en caso de ser constituido) deberán estar integrados al menos por un integrante del directorio de la entidad. Ningún director podrá ser parte del comité de gestión de riesgo y del comité de auditoría al mismo tiempo.*

***8.** Aprobar los planes anuales de las instancias encargadas de las funciones de gestión de riesgos y auditoría interna, y estar en conocimiento, en forma oportuna, de su cumplimiento y de los informes que elabore.*

9. *Evaluar periódicamente la suficiencia de recursos de las funciones de gestión de riesgos y de auditoría interna, para lo cual deberá tener en consideración la cobertura del trabajo de dichas funciones, aprobando la asignación de los recursos necesarios para dichas instancias y monitoreando el grado de cumplimiento del presupuesto asignado a tal fin.*

10. *Establecer una estructura organizacional adecuada, consistente con el tamaño, volumen y naturaleza de los negocios y riesgos de la entidad, que contemple una apropiada segregación de funciones. Lo anterior, involucra la segregación apropiada de los deberes y las funciones claves, especialmente aquellas que, si fueran realizadas por una misma persona, puedan dar lugar a errores que no se detecten o que expongan a la entidad a riesgos no deseados o no mitigados y controlados; y entre las áreas operativas y de negocios, y las de gestión de riesgos y auditoría interna de la entidad.*

11. *El directorio deberá velar por la existencia de un adecuado diseño, implementación y documentación de políticas para:*

11.1. *Los distintos tipos de operaciones y actividades que realiza el intermediario en el desarrollo de su giro.*

11.2. *El manejo de información confidencial y privilegiada.*

11.3. *La resolución de conflictos de intereses entre el intermediario o sus empleados y sus clientes.*

11.4. *El conocimiento de los clientes, de sus necesidades y objetivos de inversión, y la entrega de información periódica a los mismos, a objeto de no recomendarles u ofrecerles inversiones en instrumentos o activos que no correspondan a las necesidades, expectativas y disposición al riesgo manifestadas por ellos, en conformidad a las disposiciones establecidas en el artículo 28 de la Ley N°21.521.*

11.5. *Prevenir, detectar y evitar la realización de actividades u operaciones prohibidas.*

11.6. *Prevenir, detectar y evitar la realización de operaciones vinculadas al lavado de activos, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva de acuerdo con las disposiciones legales establecidas en la Ley N°19.913.*

11.7. *Incorporar un nuevo producto o servicio.*

12. *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.*

13. *Aprobar los sistemas y metodologías de medición y control de los distintos tipos de riesgos que enfrenta el intermediario.*

14. *Aprobar políticas para el tratamiento de excepciones a los límites de exposición a los diversos riesgos.*

15. *Aprobar el manual de gestión de riesgos y asegurarse de su permanente revisión y actualización.*

16. *Velar por la existencia de una instancia encargada de la función de gestión de riesgos y asegurarse de su independencia y adecuado funcionamiento.*

17. *Velar por la existencia de una instancia encargada de la función de auditoría interna y asegurarse de su independencia y adecuado funcionamiento.*

18. *Implementar políticas de remuneración y compensación para quienes presten servicios a la entidad, las cuales considerarán al menos la forma o mecanismo para prevenir o mitigar que las remuneraciones y compensaciones no produzcan o exacerben conflictos de intereses por parte de quienes gestionan recursos de la propia entidad y de quienes asesoran o mantienen relaciones comerciales con clientes.*

19. *Establecer políticas de contratación de empleados que aseguren que la entidad disponga de personal con la debida experiencia para desempeñar sus funciones, y velar porque se cuente con el recurso humano calificado para la gestión de riesgos, con apego a las disposiciones legales y normativas vigentes. En el caso del personal que efectúe asesorías a los clientes, deberá cumplir con lo establecido en los requisitos de autorización para la prestación de servicios.*

20. *Velar por la implementación de un sistema de información para el desarrollo de las actividades del intermediario, y para el control y gestión de riesgo.*

21. *Definir un proceso adecuado de difusión de una cultura de gestión de riesgo en toda la organización.*

22. *Establecer un mecanismo efectivo para la recepción, gestión y resolución de reclamos internos o externos y denuncias de incumplimiento al código de ética, de manera que permitan resguardar la reserva de quien lo formula. El directorio deberá mantenerse informado de las denuncias y reclamos relevantes.*

23. *Tomar conocimiento de los reportes o informes emitidos por las instancias encargadas de las funciones de gestión de riesgos y auditoría interna.*

24. *Contar con un programa de mejoramiento continuo del sistema de control interno y gestión de riesgos, incluyendo programas de capacitación al personal de la entidad, a objeto de gestionar con mayor eficacia los riesgos que se presentan en el desarrollo de las actividades de la entidad.*

La actuación del directorio en las materias antes mencionadas deberá constar por escrito en las actas de reunión de directorio, cuando el intermediario esté constituido como sociedad anónima, o en una documentación equivalente, cuando se constituya como otro tipo de sociedad. Se deberá asegurar que las actas o documentación equivalente den cuenta de las principales temáticas tratadas en las sesiones del directorio y los comités, así como las políticas mencionadas previamente. Todo el material que se elabore o presente al directorio o los comités, deberán estar debidamente documentados y estar permanentemente disponibles para su examen a solicitud de esta Comisión.

III. GESTIÓN DE RIESGOS

Los intermediarios deberán implementar un sistema de gestión de riesgos adecuado al tamaño, volumen y naturaleza de sus negocios y riesgos. El referido sistema debe tener como propósito gestionar eficazmente los riesgos financieros, operacionales, de lavado de activos, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva, y de cumplimiento normativo que se presentan en los negocios y actividades que realizan en el desarrollo de su giro, como también aquéllos que pueden afectar los intereses y activos de los clientes.

En consecuencia, el sistema de gestión de riesgos que implemente un intermediario debe considerar al menos las siguientes actividades:

***1.** Identificar los procesos en los que se descomponen las actividades efectuadas por la entidad (mapa de procesos que incluya los procesos estratégicos, operativos y de apoyo) a través de:*

***1.1.** Una descripción de las actividades y negocios principales;*

***1.2.** Identificación de los responsables de efectuar dichas actividades, así como de su supervisión.*

***2.** Identificar y evaluar formalmente los riesgos a los que se expone en el desarrollo de sus negocios y actividades, en los procesos y sistemas que utiliza y aquéllos que puedan afectar los activos e intereses de los inversionistas.*

***3.** Determinar los niveles de apetito al riesgo en relación con sus objetivos y a la protección de los activos e intereses de los inversionistas.*

***4.** Establecer controles tendientes a mitigar los riesgos identificados.*

***5.** Monitorear las alertas definidas, el cumplimiento de los límites y controles establecidos o si se han seguido los procedimientos formales de excepción.*

***6.** Establecer un sistema eficaz de comunicaciones que asegure que la información relevante para la gestión y control de riesgos llega en forma veraz, suficiente y oportuna al directorio y otras instancias responsables.*

III.1. Función de gestión de riesgos

La instancia encargada de la función de gestión de riesgos deberá ser desarrollada por personal con experiencia y conocimientos comprobables en marcos de referencia o estándares de gestión de riesgo y de los riesgos específicos que el intermediario enfrenta en el desarrollo de su negocio.

La función de gestión de riesgos podrá ser realizada por una persona o unidad interna. Dicha función deberá ser independiente de las áreas generadoras de riesgos y de la instancia encargada de la función de auditoría interna, con reporte directo al directorio.

En el caso de que el intermediario pertenezca a un grupo empresarial, la función de gestión de riesgos podrá ser ejercida por una unidad de gestión de riesgos corporativa, cuando resulte conveniente por circunstancias específicas de la entidad, y 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 ejercerá la función de riesgos, en relación con 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.

Para todos los efectos, si la función es ejercida por una unidad de gestión de riesgos corporativa, en caso de que la entidad pertenezca a un grupo empresarial, se considerará realizada por una unidad interna.

Sin perjuicio de lo anterior, el directorio del intermediario será siempre responsable de la función de gestión de riesgos aun cuando ésta sea realizada por una instancia perteneciente al grupo empresarial, debiendo revisar los informes realizados al respecto, para lo cual deberá hacerse de toda la documentación relevante.

La instancia encargada de la función de gestión de riesgos al menos deberá:

***1.** Desarrollar las actividades señaladas en los números 1. a 6. de la sección III.GESTIÓN DE RIESGOS.*

***2.** Proponer políticas y procedimientos para la gestión de riesgos, consistentes con la estrategia de negocios y la protección de los activos e intereses de los clientes.*

***3.** Analizar los riesgos asociados a situaciones de crisis, así como los cambios en las condiciones económicas, legales, regulatorias, tecnológicas, de la industria y de los mercados en los que opera el intermediario y sus efectos en la posición de riesgos.*

***4.** Evaluar permanentemente si las políticas y procedimientos de la entidad para gestionar sus riesgos se encuentran actualizados, si son adecuados para el intermediario y si éstos se recogen apropiadamente en el manual de gestión de riesgos.*

***5.** Establecer procedimientos para que el personal esté en conocimiento de los riesgos, los mecanismos de mitigación y las implicancias del incumplimiento de las políticas y procedimientos de control.*

***6.** Efectuar seguimiento permanente al cumplimiento de los límites de exposición al riesgo y de las medidas correctivas que se hubieren definido para las deficiencias identificadas.*

***7.** Emitir un informe, al menos con una periodicidad trimestral, al directorio sobre los incumplimientos detectados en las políticas y procedimientos de gestión de riesgos, causas que los originaron, medidas adoptadas y niveles de exposición al riesgo del intermediario. Sin perjuicio de lo anterior, frente a la detección de un incumplimiento grave de las políticas, se deberá informar oportunamente al directorio.*

***8.** Emitir un informe al cierre de cada ejercicio anual, destinado al directorio, sobre el funcionamiento del sistema de gestión de riesgos respecto del ejercicio que se informa, en el que se pronuncie acerca del funcionamiento de las alertas e indicadores; de la oportuna identificación de eventos relevantes del periodo, debilidades detectadas y mejoras aplicadas al sistema, entre otros aspectos.*

***9.** Proponer un plan anual de actividades, el cual debe ser aprobado por el directorio.*

10. *Monitorear la oportuna corrección de las observaciones por falencias o deficiencias detectadas, tanto interna como externamente, que tengan implicancias en la gestión de riesgo del intermediario.*

11. *Disponer de sistemas de información que optimicen el desarrollo de sus actividades, los que deberán permitir al menos:*

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

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

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

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

III.2. Manual de gestión de riesgos

Los intermediarios deberán contar con un Manual de Gestión de Riesgos, el que deberá ser aprobado por el directorio, al igual que sus modificaciones. Este Manual debe ser revisado al menos una vez al año y actualizado cada vez que exista un cambio significativo en la exposición al riesgo del intermediario. El Manual de Gestión de Riesgos deberá contener al menos lo siguiente:

1. *Las políticas y procedimientos de gestión de riesgos, los que deben ser acordes con la estrategia de negocios y el tamaño, volumen, naturaleza de sus negocios, y riesgos de las operaciones que realiza el intermediario.*

2. *La matriz de riesgo del intermediario, en la que se identifiquen, para cada una de las líneas de negocio o actividades que desarrolla, los procesos que la integran, los riesgos inherentes asociados a dichos procesos, su importancia relativa en relación a los objetivos del intermediario y la protección de los intereses y activos de los clientes, una evaluación sobre la probabilidad de ocurrencia e impacto de dichos riesgos y los controles mitigantes asociados. El diseño de controles mitigantes deberá considerar:*

2.1. *Una descripción de cada control y de su objetivo.*

2.2. *La identificación de los responsables del control formalmente designados para esos efectos y la oportunidad en que se aplica.*

2.3. *La calificación de la efectividad de los controles.*

2.4. *Los riesgos residuales, esto es, aquella parte de los riesgos inherentes que no puede ser mitigada por los controles correspondientes, ya sea por el tipo de control, la calidad o efectividad de éste. A partir de los riesgos residuales, se deberá definir su tratamiento teniendo en consideración los niveles de apetito al riesgo.*

2.5. *La 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 II y al directorio en el caso de detectarse deficiencias significativas.*

3. *Indicadores claves de riesgos, los que deben ser monitoreados periódicamente para evaluar la exposición a los niveles de apetito al riesgo definidos. Para cada indicador se deberá definir y documentar:*

3.1. *Su metodología de cálculo formal.*

3.2. *Los responsables de su generación, monitoreo y reporte.*

3.3. *Los umbrales y niveles de apetito al riesgo para cada indicador.*

4. *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 al riesgo llegue a directorio y a todas las instancias pertinentes.*

5. *La identificación del personal responsable de la aplicación de las políticas y procedimientos, sus cargos y descripción de éstos.*

6. *La identificación del personal responsable de la supervisión de las personas referidas en el literal precedente, cuyo objetivo es verificar que las políticas y procedimientos se están llevando a cabo de acuerdo con lo definido.*

7. *En el evento que se definan situaciones de excepción en determinados procedimientos, la identificación de las personas responsables de autorizar tales excepciones.*

8. *La descripción del proceso de monitoreo, documentación e informe de cumplimiento/incumplimiento de los procedimientos de gestión de riesgo.*

9. *La descripción del procedimiento mediante el cual se aprueban, revisan y actualizan los procedimientos y controles y la periodicidad de estas gestiones.*

III.3. Políticas, procedimientos y controles

Los intermediarios deberán establecer y mantener políticas, procedimientos y controles operativos efectivos en relación con su actividad diaria y respecto de cada uno de los negocios o actividades que desarrollan. Las referidas políticas, procedimientos y controles deben estar formalmente documentados en manuales los que deberán ser divulgados internamente, y orientarse a asegurar, razonablemente, al menos, lo siguiente:

a. Conflictos de intereses

Las políticas y procedimientos deberán considerar la identificación, la prevención y monitoreo los conflictos de intereses que se presenten entre el intermediario o sus empleados y los clientes, lo que será contemplado, además, en las políticas de comunicaciones y de remuneraciones del intermediario. Un intermediario debe esforzarse por evitar los conflictos de intereses con sus clientes, no obstante, si éstos se presentan, deben asegurar un tratamiento justo de todos sus clientes mediante una difusión apropiada de información,

normas internas de confidencialidad o la abstención de intervenir en los casos en que el conflicto resulte inevitable.

b. Confidencialidad de la información

Los intermediarios deberán definir políticas y procedimientos destinados a resguardar la naturaleza confidencial de la información que se relacione con las operaciones de ésta y de la información relativa a terceros con los cuales mantiene una relación comercial. Algunos ejemplos de tales políticas y procedimientos son los códigos de conducta de los empleados y las cláusulas de confidencialidad que contemplen los contratos laborales. En este tenor, el intermediario podrá definir políticas respecto a la celebración de contratos de confidencialidad con el personal temporal, los contratistas y otros proveedores de servicios, que tengan acceso a dicha información.

Asimismo, los intermediarios deberán definir políticas y procedimientos destinados a resguardar la naturaleza confidencial de la información entregada por sus clientes debiendo cumplir con todas las disposiciones legales al efecto, en particular, aquellas que establece la Ley N°19.628 sobre protección de los datos personales.

Las políticas y procedimientos deberán incluir el consentimiento para el uso de la información por parte de los clientes, de acuerdo con la Ley N°19.628 sobre protección de los datos personales, asegurando la protección de los datos contra el acceso y la divulgación no autorizados y los medios para proteger la privacidad personal y la información reservada.

En caso de que la gestión de riesgos sea realizada por un grupo empresarial, se deberá resguardar que la información de los clientes del intermediario no sea usada para un fin para el cual no haya dado su consentimiento.

c. Oferta de productos acorde necesidades, expectativas y disposición al riesgo del inversionista

Los intermediarios deberán definir políticas y procedimientos tendientes a que los inversionistas inviertan sus recursos conociendo la información que les permita entender y aceptar el riesgo que están asumiendo, y evitando ofrecer productos que no sean acordes a sus necesidades, expectativas y disposición al riesgo, según lo dispuesto en el artículo 28 de la Ley N°21.521 y en la sección II.3 de la Norma de Carácter General N°380.

En aquellos casos en que un cliente realice inversiones que en opinión de la entidad no sean acorde a las necesidades, expectativas o riesgos comunicados por el cliente, ésta deberá poder acreditar que aquello fue debidamente advertido, en caso de que le sea solicitado por esta Comisión. Los procedimientos que se definan podrán considerar el requerir a sus potenciales clientes antecedentes tales como, información sobre sus conocimientos y experiencia como inversionista, su situación financiera y objetivos de inversión o ahorro y otra información de esta naturaleza que la entidad considere relevante.

El intermediario deberá establecer procedimientos que permitan monitorear el cumplimiento de la política de oferta de productos en forma periódica, incluyendo una descripción de los procedimientos de detección de necesidades, expectativas y disposición al riesgo asociadas a cada inversionista. La entidad podrá establecer excepciones en esta política, en caso de que la oferta de productos esté dirigida a clientes que tengan la calidad de inversionista institucional o inversionista calificado de entre los señalados en los números 2, 3 y 4 de la Sección II de la Norma de Carácter General N°216 o la que la reemplace.

d. Información al inversionista

El intermediario deberá definir políticas y procedimientos que determinen la forma en que se garantizará que los clientes cuenten con información veraz, suficiente y oportuna, relativa a los productos o servicios ofrecidos, según las disposiciones establecidas en el artículo 28 de la Ley N°21.521 y en la Norma de Carácter General N°380.

Estas políticas deberán especificar, al menos, la información que debe ser conocida por los clientes, y aquella que adicionalmente la entidad estime necesaria que se conozca, así como también la periodicidad establecida para ello. Por su parte, los procedimientos deberán estar referidos a la forma en que la entidad gestionará el cumplimiento de estas disposiciones.

e. Metodología de aprobación, evaluación y control de algoritmos

En caso de corresponder, los intermediarios deberán contar con políticas y procedimientos de aprobación, evaluación y control de algoritmos que garanticen su adecuado funcionamiento. Estas políticas y procedimientos deberán propender a que los algoritmos empleados en que las transacciones operen en el mejor interés y la protección de los clientes, acorde con las necesidades, expectativas y disposición al riesgo que éstos les hayan comunicado previamente.

Las políticas y procedimientos deberán considerar, al menos, que la entidad cuente con personal capacitado que comprenda el funcionamiento de los algoritmos y la verificación continua de su correcto funcionamiento.

f. Garantías

En caso de que las entidades requieran garantías por parte de los inversionistas para realizar operaciones, deberá establecer:

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

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

3. *La revisión periódica de las metodologías.*

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

g. Prevención de lavado de activos, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva

Los intermediarios 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 las normativas dictada por la Unidad de Análisis Financiero.

h. Cumplimiento de requisitos legales y normativos de funcionamiento

Los intermediarios deberán establecer políticas y procedimientos que especifiquen la forma en que se monitoreará y garantizará el debido cumplimiento de los requisitos legales y normativos aplicables al intermediario por parte de sus directivos y empleados.

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 esta Comisión.

i. Gestión de consultas, reclamos y denuncias

Los intermediarios deberán establecer políticas y procedimientos que les permita gestionar y resolver las consultas, denuncias y reclamos de sus clientes, trabajadores y el público general. Para ello deberá considerar, al menos, un manual que establezca, en términos simples, los antecedentes mínimos que se requerirán para efectuar una consulta, denuncia o reclamo, y que describa cómo utilizar los canales especializados que se hubieren dispuesto para esos efectos. El manual deberá establecer:

1. *Procedimiento para resolver las consultas del público que considere los diferentes canales que se disponga para estos efectos. El mecanismo deberá permitir hacer un seguimiento de las consultas efectuadas.*

2. *Procedimientos que permitan resguardar la reserva de quien formula el reclamo o denuncia.*

3. *Definir claramente cómo se calificará la gravedad o relevancia de la denuncia o reclamo, y cómo se comunicará a las instancias que corresponda, incluyendo al directorio en el caso de aquellas más relevantes.*

4. *Las instancias que participarán en la gestión de las consultas, denuncias o reclamos de acuerdo con la relevancia o la gravedad que se hubiere definido para cada caso. Con todo, la gestión de los reclamos deberá ser efectuada por una unidad independiente de las áreas operativas donde se hayan originado los mismos.*

5. *Los tiempos máximos establecidos para gestionar y responder cada consulta, denuncia o reclamo de acuerdo con su gravedad o relevancia.*

6. *Un registro de las consultas, denuncias y reclamos junto con la gravedad o relevancia asignada y la solución implementada.*

7. *Definir una instancia encargada de analizar, monitorear y proponer medidas para evitar que las situaciones que generaron las consultas, denuncias o reclamos se repitan.*

j. Otras políticas

El intermediario deberá definir políticas y procedimientos en los siguientes ámbitos:

1. *La integridad de las prácticas del intermediario en materia de negociación.*

2. *La protección de los activos financieros tanto del intermediario como de sus clientes con el objeto de garantizar que los activos propios y de terceros en custodia estén adecuadamente resguardados y administrados.*

3. *La integridad, disponibilidad y confiabilidad de la información, especialmente el mantenimiento apropiado de registros contables y otros registros exigidos por la normativa vigente, y la integridad, disponibilidad y confiabilidad de la información.*

4. *El análisis de los riesgos asociados a la introducción de nuevos productos, operaciones y actividades, acorde con la estrategia general del negocio, las disposiciones legales, normativas, estatutos y políticas internas, de manera de garantizar la protección de los activos e intereses de los inversionistas (acorde con sus necesidades, expectativas y disposición al riesgo), y verificando la mitigación del riesgo de ciberseguridad.*

5. *La seguridad de la información y ciberseguridad, la continuidad operacional y la externalización de servicios por parte del intermediario, de acuerdo con la normativa de gestión de riesgo operacional emitida a tal efecto por esta Comisión.*

6. *El manejo de información privilegiada.*

III.4. Función de auditoría interna

Los intermediarios deberán contar con una función de auditoría interna, la que estará encargada de verificar el correcto funcionamiento del sistema de control interno y gestión de riesgos y su consistencia con los objetivos y políticas de la organización, como también del cumplimiento de las disposiciones legales y normativas que le son aplicables al intermediario.

La función de auditoría interna deberá ser independiente de las áreas operativas y de negocios de la entidad y de la instancia encargada de la función de gestión de riesgos, con reporte directo al directorio. Esta función podrá ser realizada por una persona o unidad interna o externalizada a un tercero, de acuerdo con la sección IV siguiente.

En el caso que el intermediario pertenezca a un grupo empresarial, la función de auditoría interna podrá ser ejercida por la unidad de auditoría interna 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 con 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. Para todos los efectos, si la función de auditoría interna es ejercida por una unidad corporativa del grupo empresarial al que pertenece la empresa, con las condiciones señaladas, se entenderá que es ejercida por una unidad interna.

Sin perjuicio de lo anterior, el directorio de la entidad será siempre responsable de la función de auditoría interna aun cuando ésta sea realizada por una instancia perteneciente al grupo empresarial, debiendo revisar los informes realizados al respecto, para lo cual deberá hacerse de toda la documentación relevante.

Los informes que se generen producto del plan de revisión deberán dirigirse al directorio y contener como mínimo el objetivo, el alcance, las situaciones detectadas, la importancia relativa de las mismas y las conclusiones correspondientes. Asimismo, deberán señalar los comentarios de las áreas que han sido objeto de la revisión, las medidas correctivas que se adoptarán y los plazos estimados para ello.

La función de auditoría interna deberá contar con personas con experiencia y conocimientos para desarrollar apropiadamente, al menos, las siguientes actividades:

1. *Evaluar la adhesión a los objetivos, políticas y procedimientos en materia de control interno de las distintas unidades o áreas del intermediario.*

2. *Evaluar la efectividad y el cumplimiento de las políticas, procedimientos y controles implementados, conducentes a la protección de activos propios y de sus clientes, a la debida ejecución de operaciones, a la detección de operaciones ilícitas, a garantizar la seguridad de la información, a la protección de la integridad de los sistemas de información, a garantizar el manejo confidencial de la información relativa a sus clientes, al adecuado manejo de los conflictos de intereses con los clientes,* a la *continuidad de los negocios y la evaluación de la prevención del lavado de activos, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva, entre otros.*

3. *Evaluar el funcionamiento de la instancia encargada de la función de gestión de riesgos desarrollada en el intermediario.*

4. *Evaluar que la información financiera utilizada para la conducción de los negocios y aquella utilizada para efectos de control de los riesgos, sea confiable, oportuna, completa e íntegra.*

5. *Revisar la estructura organizacional para verificar la adecuada segregación de funciones.*

6. *Verificar el cumplimiento de las disposiciones legales y normativas que le son aplicables a los intermediarios, sus directivos y empleados, como así también de toda documentación interna tal como reglamentos internos, códigos de ética o manuales operativos.*

7. *Monitorear la oportuna corrección de las observaciones por falencias o deficiencias detectadas en materia de control interno y gestión de riesgo. Sin perjuicio de lo anterior, frente a la detección de un incumplimiento grave de las políticas, el encargado de la función de auditoría deberá informar oportunamente al directorio.*

8. *Se deberá disponer de sistemas de información que optimicen el desarrollo de las actividades de auditoría interna, que permitan al menos:*

- ***8.1.*** *Registrar sus actividades, programas 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.*

Para llevar a cabo estas labores, la función de auditoría interna deberá contar con un plan de revisión anual, debidamente aprobado por el directorio y con procedimientos documentados para el desarrollo de estas revisiones. Para ello deberá contar con una metodología para la planificación de las auditorías que permita garantizar que los procesos relevantes sean cubiertos en un ciclo de tiempo razonable. Con procesos de control que permitan verificar la calidad de sus revisiones.

La función de auditoría interna deberá informar por escrito al directorio, al menos en forma semestral, sobre el desempeño de las labores descritas y sobre el cumplimiento de su plan de revisión anual. Sin perjuicio de lo anterior, frente a la detección de un incumplimiento grave, el encargado de la función de auditoría deberá informar oportunamente al Directorio.

IV. PROPORCIONALIDAD

En línea con lo establecido en el artículo 31 de la Ley N°18.045 y el artículo 7 de la Ley N°19.220, los intermediarios podrán adaptar las disposiciones de esta normativa conforme a su tamaño, volumen y naturaleza de sus negocios y riesgos, de acuerdo con la siguiente clasificación:

1. *Bloque 1: intermediarios que no cumplan ninguna de las métricas de volumen de negocio de las entidades del Bloque 2 o 3. Se considerarán clientes activos aquellos que cumplan con las condiciones definidas en el Anexo N°1 de esta normativa.*

2. *Bloque 2: intermediarios que cumplan alguna de las siguientes condiciones:*

2.1. *Tengan un número de clientes activos entre 500 y 5.000.*

2.2. *Transacciones promedio diarias en los últimos 12 meses entre UF 100.000 y UF 500.000.*

2.3. *Ingresos en los últimos 12 meses entre UF 25.000 y UF 50.000.*

3. *Bloque 3: intermediarios que cumplan alguna de las siguientes condiciones:*

3.1. *Más de 5.000 clientes activos.*

3.2. *Más de UF 500.000 en transacciones promedio diarias en los últimos 12 meses.*

3.3. *Activos custodiados promedio diarios en los últimos 12 meses mayor a UF 0.*

3.4. *Ingresos en los últimos 12 meses sobre UF 50.000.*

La Comisión solicitará que le remitan aquella información necesaria para determinar el cumplimiento de la clasificación de bloques, en la periodicidad, forma y medio que establezca mediante norma de carácter general. Cuando una entidad alcance una de las condiciones que la clasifique en un bloque diferente por más de 6 meses, dispondrá de un plazo máximo de 9 meses desde la comunicación por parte de la Comisión del cambio de bloque, para dar cumplimiento a los requisitos de esta norma. Los intermediarios podrán ser reclasificados a bloques inferiores después de un mínimo de 6 meses y con autorización de la Comisión.

Los intermediarios que clasifiquen dentro de los Bloques 1 o 2 podrán desarrollar la función de gestión de riesgos por una persona o unidad interna.

Los intermediarios que clasifiquen dentro de los Bloques 1 o 2 podrán desarrollar la función de auditoría interna por una persona o unidad interna o por un tercero externo.

En caso de que la función de auditoría interna sea realizada por un tercero externo, en ningún caso dicho tercero podrá ejercer la función de auditoría externa en la entidad, debiendo la entidad velar por la adecuada segregación de ambas funciones.

Las entidades que clasifiquen dentro del Bloque 3 deberán desarrollar las funciones de gestión de riesgos y de auditoría interna a través de una unidad interna.

Sin perjuicio de lo anterior, para las entidades clasificadas en los Bloques 1 y 2, esta Comisión podrá exigir al intermediario la creación de una unidad interna para el desarrollo de las funciones de gestión de riesgos y/o de auditoría interna, en función de la medición de la calidad de la gestión de riesgos que ésta realice.

Tabla. Proporcionalidad para la prestación de los servicios de intermediación.

Bloque	Función de gestión de riesgos	Función de auditoría interna
1 y 2	Persona o unidad interna	Persona o unidad interna o ser realizadas por un tercero
3	Unidad interna	Unidad interna

V. EVALUACIÓN DE LA CALIDAD DE LA GESTIÓN DE RIESGOS

La Comisión evaluará la forma en que el directorio u órgano equivalente y el sistema de gestión de riesgos cumplen con lo dispuesto en las secciones precedentes y en la Norma de Carácter General N°510 sobre gestión de riesgo operacional.

La Comisión informará al intermediario respecto al resultado de dicha evaluación, con el objeto de que se adopten las medidas necesarias para fortalecer la gobernanza y el sistema global de gestión de riesgos del intermediario, en caso de ser necesario.

A continuación, se describen los principales elementos del proceso de evaluación:

V.1 Rol del directorio u órgano equivalente

*La evaluación deberá considerar el grado de cumplimiento de las disposiciones establecidas en la sección **II. RESPONSABILIDAD DEL DIRECTORIO U ÓRGANO EQUIVALENTE** de la presente normativa. En particular, se evaluará la actuación del directorio u órgano equivalente en relación con la adecuada gestión de los riesgos, incluyendo la efectividad de los controles establecidos, el cumplimiento de las políticas y procedimientos establecidos, y la estructura organizacional y fortaleza de las líneas de defensa que haya definido para la gestión de los riesgos, atendiendo a la naturaleza, volumen y complejidad de sus actividades.*

Adicionalmente, la evaluación en esta materia considerará la forma en que la instancia de gobierno asegure la independencia en el ejercicio de la función de control que le corresponde. Lo anterior, en atención a la complejidad de las operaciones y riesgos que asume la entidad.

V.2 Sistema de gestión de riesgos

*La evaluación deberá considerar el grado de cumplimiento de las disposiciones establecidas en la sección **III. GESTIÓN DE RIESGOS** de la presente normativa y en la Norma de Carácter General N°510 de gestión de riesgo operacional aplicable a los intermediarios. Como insumo para la evaluación, se considerará la identificación, evaluación*

y mitigación apropiada de los riesgos que se describen a continuación, en atención a la naturaleza, volumen y complejidad de las actividades que realiza:

Riesgo de crédito: se refiere a una 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 del incumplimiento contractual de la contraparte en una transacción financiera.*

- *Riesgo crediticio del emisor: exposición a potenciales quiebras o deterioro de solvencia en los valores de oferta pública o instrumentos financieros de una entidad.*

Riesgo de mercado: se refiere a una potencial pérdida causada por cambios en los precios del mercado, que podría generar efectos adversos en la situación financiera de la cartera propia o de terceros que maneja el intermediario. Abarca el riesgo de tasas de interés, el riesgo cambiario y el riesgo de precios asociados a la cartera propia del intermediario.

Riesgo de liquidez: exposición del intermediario a una potencial pérdida como resultado de la necesidad de obtener fondos para el cumplimiento de sus compromisos financieros de manera inmediata. Este riesgo se divide en las siguientes subcategorías:

- *Riesgo de liquidez de financiamiento: exposición a una pérdida potencial como resultado de la incapacidad de obtener recursos, conseguir o refundir préstamos a una tasa conveniente o cumplir con las exigencias de los flujos de caja proyectados.*

- *Riesgo de liquidez de mercado: exposición a una pérdida potencial debido a la incapacidad de liquidar un valor en cartera sin afectar de manera adversa el precio del activo, dada la escasa profundidad del mercado de ese activo.*

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 los ámbitos de seguridad de la información y ciberseguridad, continuidad de negocio, externalización de servicios, así como 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 de lavado de activos, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva: se refiere a la posibilidad de pérdida o daño que puede sufrir el intermediario por su propensión a ser utilizado como instrumento para la canalización de recursos hacia la realización de actividades terroristas o financiamiento de armas de destrucción masiva, o cuando se pretende ocultar o disfrazar el origen ilícito de bienes o recursos que provienen de actividades delictivas. Este riesgo está asociado a los negocios en los que opera el intermediario, el tipo de clientes y los montos transados.

Riesgo de conducta: se refiere a los riesgos asociados al cumplimiento de los siguientes principios: i) trato justo a los clientes de entidades financieras; ii) adecuada gestión de conflictos de intereses; iii) protección de la información de los clientes; iv) transparencia en

la comercialización y publicidad de productos financieros y; v) gestión diligente de reclamos y presentaciones.

Otros: otros riesgos que el intermediario haya identificado como relevantes para su operación que no estén considerados en los riesgos definidos anteriormente.

La Comisión podrá evaluar específicamente las materias que estime necesarias, sobre la base de la información que periódicamente requiere a sus fiscalizados o aquella adicional que pudiera requerir para efectos de la evaluación.

Para calificar las materias asociadas a los riesgos previamente definidos se utilizará la siguiente escala:

Calificación de la gestión del riesgo	***Significado***
Cumplimiento	*La entidad cumple integralmente con las mejores prácticas y aplicación de sanos principios que caracterizan una adecuada gestión. No existen deficiencias apreciables.*
Cumplimiento material	*La entidad cumple en forma significativa con las mejores prácticas y aplicación de sanos principios que caracterizan una adecuada gestión. Aun cuando se identifican algunas debilidades en procesos específicos de alguna función, ellas se pueden considerar acotadas, sin perjuicio de lo cual su corrección debe ser atendida por la entidad a objeto de alcanzar los más altos estándares de gestión de riesgos.*
Cumplimiento insatisfactorio	*La entidad no cumple en forma razonable con las mejores prácticas y aplicación de sanos principios que caracterizan una adecuada gestión. Se identifican debilidades en los procesos que componen diversas funciones, entre las que se encuentran algunas relevantes. La corrección de estas debilidades debe ser efectuada con la mayor prontitud.*
Incumplimiento	*La entidad incumple materialmente con las mejores prácticas y aplicación de sanos principios que caracterizan una adecuada gestión. La solución de sus debilidades se considera indispensable.*

V.3 Calificación global de la calidad de gestión de riesgos

Como resultado del proceso de evaluación de uno o más riesgos en cuanto al rol del directorio y del sistema de gestión de riesgos, esta Comisión determinará la calificación global

de la calidad de la gestión de riesgos del intermediario evaluado a partir de la siguiente escala de evaluación:

Calificación global de la calidad de gestión de riesgos	***Significado***
A	*Intermediarios que cumplen satisfactoriamente con altos estándares de gestión de riesgos, por lo que no presentan las características de los niveles B, C o D.*
B	*Intermediarios que en el proceso de supervisión o que en el proceso de monitoreo de su información, reflejan debilidades relacionadas con las materias definidas en la normativa aplicable, especialmente en su gobierno corporativo, controles internos, calidad de la información reportada, sistemas de información para la toma de decisiones, seguimiento oportuno de los distintos riesgos, y capacidad para enfrentar escenarios de contingencia, pero que éstas no exponen a la entidad a riesgos significativos.*
C	*Intermediarios que en el proceso de supervisión o que en el proceso de monitoreo de su información presenten deficiencias significativas en alguno de los factores señalados en la clasificación anterior, cuya corrección debe ser efectuada con prontitud para evitar un menoscabo de la entidad.*
D	*Instituciones que presenten debilidades graves en la gestión de alguno de los riesgos evaluados o que presenten incumplimientos normativos de relevancia, cuya corrección debe ser efectuada de inmediato para evitar un menoscabo relevante en su estabilidad o en los intereses de los clientes.*

*En el caso de las entidades pertenecientes a los bloques 1 y 2 de acuerdo a las consideraciones de la Sección **IV. PROPORCIONALIDAD**, las calificaciones C y D podrán determinar la exigencia de requisitos de gobierno corporativo y gestión de riesgos correspondientes al bloque 3 de esta normativa y la Norma de Carácter General N°510 de gestión de riesgo operacional. En tal caso, la entidad dispondrá de un plazo máximo de 9 meses desde la comunicación por parte de la Comisión de la calificación asignada, para dar cumplimiento a estos requisitos adicionales.*

Lo anterior, es sin perjuicio de los requisitos de patrimonio, garantías, endeudamiento o liquidez que puedan ser requeridos para el intermediario en base a su calificación global, según la normativa que dicte a tal respecto esta Comisión.

VI. DISPOSICIONES ADICIONALES

1. *Los intermediarios deberán enviar a esta Comisión a más tardar 30 días después del cierre de cada ejercicio anual, una autoevaluación de gestión de riesgos, aprobada por el directorio u órgano equivalente. Esta evaluación deberá considerar el grado de cumplimiento de las disposiciones establecidas en las secciones* ***II. RESPONSABILIDAD DEL DIRECTORIO*** *y* ***III. GESTION DE RIESGOS*** *de la presente normativa y en la Norma de Carácter General N°510 de gestión de riesgo operacional aplicable a los intermediarios.*

2. *Esta Comisión podrá asignar una calificación global de la calidad de la gestión de riesgos a través del monitoreo de información u otras acciones de supervisión del intermediario. La Comisión podrá solicitar como insumo para realizar esta evaluación, una certificación o evaluación de gestión de riesgos o un informe de procedimiento acordado efectuados por una empresa de auditoría externa del Registro de Empresas de Auditoría Externa de esta Comisión. La entidad contratada para estos efectos no podrá prestar simultáneamente el servicio de auditoría externa al intermediario.*

VII. DEROGACION

Deróguese la Circular N°2.054.

VIII. VIGENCIA

Las instrucciones establecidas en la presente Norma de Carácter General rigen a contar del 1 de julio de 2025, excepto los párrafos 2 y 3 de la sección V.3 y el párrafo 1 de la sección VI que entrarán en vigencia a partir del 1 de julio de 2027.

SOLANGE BERSTEIN JÁUREGUI

PRESIDENTA

COMISIÓN PARA EL MERCADO FINANCIERO

ANEXO N°1: DEFINICIONES

***Apetito por riesgo**: nivel agregado y tipos de riesgo 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.*

***Ciberseguridad**: corresponde al conjunto de acciones que realiza la entidad para mitigar los riesgos y proteger la información e infraestructura que la soporta, de eventos del ciberespacio, siendo este último el entorno resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red.*

***Cliente activo:** todo cliente que no se considera inactivo será considerado como activo.*

***Cliente inactivo:** se define como cliente inactivo aquel que no ha utilizado en ninguna forma cualquiera de los servicios ofrecidos por el intermediario en los últimos 3 meses. También, aquel cliente que no tiene un contrato vigente con el intermediario. Por último, se define como cliente inactivo aquel que cumpla con las siguientes condiciones de forma conjunta:*

- *No realizan ningún tipo de transacción ni han recibido o solicitado ningún tipo de servicio prestado por el intermediario en los últimos 3 meses (incluidos servicios de custodia).*
- *No dispone de saldos (activos o pasivo) en cuentas provistas por el intermediario.*

***Externalización de servicios:** es la ejecución por un proveedor externo de servicios o actividades en forma continua u ocasional, las que normalmente podrían ser realizadas por la entidad contratante.*

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

***Riesgo inherente:** corresponde a aquel riesgo que por su naturaleza no puede ser separado del proceso o subproceso en que éste se presenta. Corresponde al riesgo que debe asumir cada entidad de acuerdo al ámbito de desarrollo de sus actividades establecido por ley.*

***Riesgo residual:** aquel riesgo que persiste luego de adoptar las medidas de control y mitigación por parte de la entidad.*

B. MODIFICACION NORMA DE CARÁCTER GENERAL N°510

REF: ***MODIFICA NORMA DE CARÁCTER GENERAL N°510 QUE IMPARTE INSTRUCCIONES SOBRE GESTIÓN DE RIESGO OPERACIONAL.***

_____

NORMA DE CARÁCTER GENERAL N°[NUMERO]

[día] de [mes] de [año]

Esta Comisión en uso de las atribuciones conferidas en el Decreto Ley N°3.538, la Ley N°18.045, la Ley N°19.220 y Ley N°21.521; y teniendo en consideración que su mandato legal es velar por el correcto funcionamiento, desarrollo y estabilidad del mercado financiero, ha resuelto modificar la Norma de Carácter General N°510, que imparte instrucciones sobre gestión de riesgo operacional, en los siguientes términos.

1. *Reemplácese el encabezado de la norma por el siguiente párrafo "Esta Comisión en uso de las atribuciones conferidas en el Decreto Ley N°3.538, la Ley N°18.045, la Ley N°18.876, la Ley N°19.220, la Ley N° 20.345, el artículo 1° de la Ley N°20.712 y Ley N°21.521; 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 de la gestión de riesgo operacional para Administradoras Generales de Fondos, Bolsas de Valores, Bolsas de Productos, Intermediarios de Valores, Corredores de Bolsas de Productos, Sociedades Administradoras de Sistemas de Compensación y Liquidación de Instrumentos Financieros y Entidades de Depósito y Custodia de Valores."*

2. *Reemplácese el título de la sección A.2.1. por "Intermediarios de Valores, Corredores de Bolsas de Productos y Administradoras Generales de Fondos".*

3. *Reemplácese el numeral 1.1. de la sección B.1. por "Procedimientos de respuesta ante la ocurrencia de eventos internos o externos que pudieran crear una interrupción en la continuidad de las operaciones del negocio. Estos procedimientos se deberán referir expresamente a la ejecución de un análisis de impacto de negocio (BIA, por su sigla en inglés) y un Análisis de Impacto de Riesgo (RIA, por su sigla en inglés).*

Se exceptúan de la disposición mencionada las entidades de los bloques 1 y 2 definidas en la Normativa de Gobierno Corporativo y Gestión de Riesgos de Intermediarios de Valores y Corredores de Bolsas de Productos, sin perjuicio de lo cual esta Comisión podrá exigir a dichas entidades la realización de un BIA y un RIA u otro procedimiento similar, en función de la medición de la calidad de la gestión de riesgos que realice."

4. *Reemplácese el encabezado del numeral 2 de la sección B.2. por "Realizar o actualizar, al menos anualmente o ante eventos que amenacen la continuidad de las operaciones del negocio, un análisis de los procesos de mayor relevancia para la continuidad de negocio, el*

impacto que tendría una interrupción de esos procesos, y los tiempos y recursos necesarios para la continuidad y recuperación de éstos. Con excepción de las entidades de los bloques 1 y 2 definidas en la Normativa de Gobierno Corporativo y Gestión de Riesgos de Intermediarios de Valores y Corredores de Bolsas de Productos, este análisis se deberá referir expresamente a la realización de un BIA a nivel estratégico, táctico y operativo que considere:"

5. *Reemplácese el numeral 4 de la sección B.2. por "Realizar o actualizar, al menos anualmente, una evaluación de los riesgos de continuidad de negocio que, de materializarse, provocarían una interrupción en los procesos de mayor relevancia de la entidad. Para lo anterior, se deberá considerar escenarios internos y externos, contemplando, entre otros, la falta total y parcial de los sistemas tecnológicos; ataques maliciosos que afecten la ciberseguridad; la ausencia de personal crítico; la imposibilidad de acceder o utilizar las instalaciones físicas y la falta de provisión de los servicios críticos contratados a proveedores."*

6. *Reemplácese el numeral 5 de la sección B.2. por "Definir una estrategia de continuidad de negocio que tenga por objetivo mantener la continuidad de los procesos de mayor relevancia, considerando medidas preventivas para reducir la probabilidad de materialización de daños, minimizar el tiempo de recuperación y limitar el impacto en las operaciones del negocio de la entidad. Dicha estrategia deberá considerar, en caso de que se haya realizado un BIA y un RIA, los resultados de este análisis."*

7. *Reemplácese el numeral 6 de la sección B.2. por "Implementar un Plan de gestión de crisis en el que se determine los procedimientos de escalamiento, comunicaciones, gestión y reporte de eventos de continuidad operacional para mantener informado en forma oportuna al directorio u órgano equivalente, a todas las* partes interesadas *y a esta Comisión, respecto de información relevante del evento de continuidad, las medidas adoptadas para resolverlo y la coordinación de una respuesta adecuada. En caso de que se haya realizado un BIA, la coordinación de una respuesta adecuada deberá considerar los puntos objetivos y tiempos objetivos de recuperación allí previstos."*

8. *Reemplácese el primer párrafo del numeral 1 de la sección D.1. por "Las entidades deberán comunicar a esta Comisión los incidentes operacionales que afecten la continuidad del negocio, los recursos e información de la entidad o de sus clientes y la calidad de los servicios. A modo de ejemplo, y sin el objeto de ser exhaustivos ni taxativos, deberán ser reportadas las fallas en servicios y sistemas importantes para las operaciones del negocio; problemas tecnológicos que afecten la seguridad de la información; ataques del ciberespacio; virus o malware detectados en los activos de información críticos; eventos de indisponibilidad o interrupción de algún servicio o producto que afecte a los clientes, en cualquier canal; pérdidas o fugas de información de la entidad o de clientes; los incidentes que afecten el patrimonio de la entidad producto de fraudes internos o externos; problemas que afecten la continuidad de proveedores de servicios críticos; entre otros. Esta información deberá ser mantenida por la entidad en una base de datos de incidentes y otra base de datos de pérdidas operacionales para el mejoramiento continuo del proceso de gestión de riesgo operacional.*

Las entidades de los bloques 1 y 2 definidas en la Normativa de Gobierno Corporativo y Gestión de Riesgos de Intermediarios de Valores y Corredores de Bolsas de Productos deberán reportar sólo los incidentes relacionados con seguridad de la información y ciberseguridad, quedando exceptuadas de informar incidentes de otro tipo.

9. *Reemplácese el primer párrafo del numeral 2 de la sección D.1 por "En el caso de las Bolsas de Valores, Bolsas de Productos, Sociedades Administradoras de Sistemas de Compensación y Liquidación y Entidades de Depósito y Custodia de Valores, la ocurrencia de un incidente operacional de aquellos mencionados en el numeral anterior deberá ser informada a esta Comisión en un plazo máximo de 15 minutos transcurridos desde que la entidad tomó conocimiento del hecho. En el caso de los Intermediarios de Valores, Corredores de Bolsas de Productos y Administradoras Generales de Fondos, el plazo máximo será de 2 horas desde que la entidad tomó conocimiento del hecho. Las instrucciones para reportar los incidentes operacionales a esta Comisión se encuentran en los Anexos N° 2 y 4*

10. *Reemplácese el numeral 2 de la sección D.2. por "Las entidades deberán enviar a esta Comisión la información de todas las pérdidas operacionales mayores a 150 Unidades de Fomento, de acuerdo con las instrucciones del Anexo N°3 de la presente norma, 15 días hábiles después del cierre de junio y diciembre de cada año.*

Se exceptúan de la disposición mencionada las entidades de los bloques 1 y 2 definidas en la Normativa de Gobierno Corporativo y Gestión de Riesgos de Intermediarios de Valores y corredores de Bolsa de Productos"

11. *Reemplácese el "ANEXO N° 2: REPORTE DE INCIDENTES OPERACIONALES" por el siguiente.*

"A través del menú "INCIDENTES Y PÉRDIDAS OPERACIONALES" del canal oficial de comunicación y envío de información entre la Comisión y sus fiscalizados, la entidad deberá reportar el detalle de cada incidente descrito en la sección I.D.1.

Para aquellos campos en los que al momento del reporte no se cuente con la información, se debe indicar con texto "En evaluación", y para el caso de los campos numéricos, de no contarse con el dato, éstos deben completarse con un cero. Será responsabilidad de la entidad la actualización de los antecedentes mencionados cuando se disponga de nueva información y hasta el cierre del incidente (fecha de cierre del incidente).

1. FECHA Y HORA DEL INICIO DEL INCIDENTE:

Se debe señalar la fecha (DD/MM/AAAA) y la hora (HH: MM: SS) en que comenzó el incidente.

2. TIPO DE INCIDENTE:

En este campo se debe señalar el tipo de incidente, eligiendo entre las siguientes opciones:

- *Afectación de instalaciones*
- *Ausencia de Colaboradores*
- *Sin acceso dependencias y otras áreas específicas*
- *Falla Sistemas Base (SO, BD)*
- *Falla aplicativos (negocio, web, batch)*
- *Falla de comunicaciones*
- *Falla Hardware*
- *Falla en servicios básicos (electricidad/agua)*
- *Pérdida de Recursos Monetarios de la entidad o de clientes*
- *Pérdida de Información de la entidad o de clientes*
- *Interrupción / latencia en servicios otorgados en canales electrónicos*
- *Error de envío de información de cuentas de clientes*

- *Error en cobro de producto o servicios a clientes*
- *Interrupción de servicios en canales físicos*
- *Otros: especificar*[4]

3. DESCRIPCIÓN DETALLADA DEL INCIDENTE:

En este campo se debe detallar en qué consiste el incidente reportado.

4. CAUSA:

En este campo se debe señalar la causa del incidente, eligiendo entre las siguientes opciones:

- *Inundación por causas naturales*
- *Terremoto*
- *Tsunami*
- *Huelga*
- *Pandemia*
- *Incendio*
- *Corte de energía*
- *Corte de agua*
- *Asalto a dependencias*
- *Robo o hurto de activos físicos*
- *Robo o hurto de activos digitales*
- *Daño de infraestructura tecnológica*
- *Daño de infraestructura de comunicaciones*
- *Ataque denegación de servicio*
- *Clonación*
- *Ataque de virus maliciosos*
- *Retraso / Errores en procesos operativos/tecnológicos*
- *Otros: especificar*[5]

5. Dependencias afectadas:

En este campo se deben señalar las dependencias afectadas, eligiendo entre las siguientes opciones:

- *Casa Matriz*
- *Sucursal*
- *Caja Auxiliar*
- *Sitio Producción*
- *Sitio Contingencia*
- *Dependencias proveedor*

[4] En caso de utilizarse este campo, se deberá completar con texto la información, la cual debe dar cuenta del tipo de incidente.

[5] En caso de utilizarse este campo, se deberá completar con texto la información, la cual debe dar cuenta de la ca usa del incidente

- *Otros: especificar*[6]

6. DIRECCIÓN DEPENDENCIAS AFECTADAS (CALLE, COMUNA, REGIÓN)

En este campo se debe informar la dirección de la dependencia afectada, incluyendo la calle, la comuna de acuerdo a la Tabla N° 65 del manual de sistema de información y la región de acuerdo a la Tabla N°2 del manual de sistema de información. Si existe más de una dependencia afectada, se debe indicar la dirección de cada una de ellas, separándolas con un punto y coma (;).

7. CANALES AFECTADOS

En este campo se deben seleccionar los canales afectados por el incidente:

- *Sucursales*
- *Página web*
- *Aplicación móvil*
- *Cajeros automáticos*
- *Atención telefónica*
- *POS*
- *Otros: especificar*[7]

8. NOMBRE DE PROVEEDORES INVOLUCRADOS:

Corresponde al nombre o razón social del proveedor.

9. TIPO DE PROVEEDOR INVOLUCRADO:

- *SAG*
- *Servicios básicos*
- *Telecomunicaciones*
- *Infraestructura tecnológica*
- *Transporte de valores y custodia*
- *Procesamiento*
- *N/A*[8]
- *Otros: especificar*[9]

10. NÚMERO DE CLIENTES AFECTADOS:

---

[6] En caso de utilizarse este campo, se deberá completar con texto la información, la cual debe dar cuenta de las dependencias afectadas.

[7] En caso de utilizarse este campo, se deberá completar con texto la información, la cual debe dar cuenta de los canales afectados.

[8] N/A, en todos los campos donde es utilizado, significa "No Aplica".

[9] En caso de utilizarse este campo, se deberá completar con texto la información, la cual debe dar cuenta del tipo de proveedor afectado.

En este campo se debe completar el número de clientes que fueron afectados por el incidente que se reporta.

11. TIPO DE CLIENTES AFECTADOS:

- *En este campo se debe seleccionar el tipo de cliente afectado, entre las siguientes opciones:*
- *Personas*
- *Empresas*
- *Ambos*
- *N/A*

12. NÚMERO DE EMPLEADOS AFECTADOS:

En este campo se debe completar con el número de empleados que fueron afectados por el incidente que se reporta.

13. PRODUCTOS O SERVICIOS AFECTADOS:

En este campo se deben informar en detalle los productos y servicios afectados por el incidente.

14. NÚMERO DE TRANSACCIONES AFECTADAS:

En este campo se debe completar el número de transacciones que fueron afectadas por el incidente que se reporta.

15. MEDIDAS ADOPTADAS:

En este campo se deben informar en detalle las acciones realizadas por la entidad para superar el incidente.

16. NOMBRE Y CARGO DEL INFORMANTE:

Corresponde a la persona que informa el incidente y su cargo.

17. TELÉFONO CELULAR DEL INFORMANTE:

Se debe señalar en este campo el teléfono celular de la persona que informa el incidente.

18. FECHA Y HORA DE TÉRMINO DEL INCIDENTE:

Este campo se incluirá cuando se cierra el incidente. Se debe completar la fecha (DD/MM/AAAA) y la hora (HH: MM: SS) en que éste finalizó.

"

***12.** Reemplácese el "ANEXO N° 3: REPORTE DE PÉRDIDAS OPERACIONALES" por el siguiente.*

"

A través del menú "INCIDENTES Y PERDIDAS OPERACIONALES" del canal oficial de comunicación y envío de información entre la Comisión y sus fiscalizados, la entidad deberá

reportar al último día hábil de junio y diciembre de cada año el detalle de todas las pérdidas operacionales mayores a 150 Unidades de Fomento.

1. FECHA Y HORA DE CONTABILIZACIÓN:

Seleccionar el día y hora correspondiente a la fecha en la que se contabiliza el incidente. Se debe completar la fecha (DD/MM/AAAA) y la hora (HH: MM: SS).

2. TIPO DE MONTO:

Seleccionar el código que identifica el tipo de monto a reportar, de acuerdo a la siguiente codificación que se desplegará en este campo:

CODIGO	*TIPO DE MONTO*
1	*Pérdida (cargos directos en los estados de resultados)*
2	*Gastos y provisiones (costos incurridos internos o externos con relación directa al evento operacional)*
3	*Recuperación*

3. MONTO:

Corresponde al monto bruto de las pérdidas, gastos o recuperaciones que deben reportarse en la fecha que se contabilicen. Dicho monto debe reportarse en pesos.

4. TIPO DE GASTO

Seleccionar el código que identifica el principal tipo de gasto asociado al evento de pérdida, ya sea interno o externo directamente atribuible al evento operacional, de acuerdo a la siguiente codificación que se desplegará en este campo:

CODIGO	*TIPO DE GASTO*
1	*Legales*
2	*Proveedores*
3	*Asesorías*
4	*Internos*
5	*Otros*
9	*No aplica (debe reportarse cuando el campo "TIPO DE MONTO" toma valores 1 o 3)*

5. TIPO DE RECUPERACIÓN

Seleccione el código asociado a las causas de la recuperación operacional, de acuerdo a la siguiente codificación que se desplegará en este campo:

CODIGO	*TIPO DE RECUPERACIÓN*

1	*Compañías de seguros*
2	*Acciones judiciales*
3	*Otros (liberación de provisión)*
4	*No aplica*

6. NOMBRE Y CARGO INFORMANTE

Corresponde a la persona que informa el incidente y su cargo.

7. TELÉFONO CELULAR INFORMANTE:

Corresponde al teléfono de la persona que informa el incidente.

"

VIGENCIA

Las instrucciones establecidas en la presente Norma de Carácter General rigen a contar de esta fecha.

SOLANGE BERSTEIN JÁUREGUI
PRESIDENTA
COMISIÓN PARA EL MERCADO FINANCIERO

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[10], a la vez que reconoce que asumir riesgos es esencial para un mercado secundario activo[11].

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.

En particular, se plantea la necesidad de una adecuada gestión de riesgo operacional atendido el volumen y complejidad de las operaciones de cada entidad, el tipo de negocio que desarrolla y el impacto sistémico que una interrupción de sus operaciones pudiera tener en el mercado financiero local e internacional. Al respecto:

- La rápida evolución de la infraestructura tecnológica en los últimos años (hardware y software) genera obsolescencia de las medidas de seguridad de información de una entidad, haciéndola vulnerable a brechas de seguridad de datos y ataques cibernéticos.

- La transición hacia la automatización de tareas, el procesamiento de datos en servidores y nube y las modalidades de trabajo remoto incrementan los riesgos derivados de un incidente operacional.

- La externalización de servicios en la nube y otros de estas entidades requieren una adecuada política de contratación y monitoreo de proveedores que esté acorde con las políticas de seguridad de la información y ciberseguridad, y los planes de continuidad y respuesta a incidentes.

- La aparición de nuevos servicios financieros que utilizan la tecnología, contemplados en la Ley N°21.521 (Ley Fintec) requiere tener la capacidad operacional para soportar el procesamiento de las transacciones que se realice mediante los sistemas o infraestructura de las entidades.

La presente propuesta normativa establece que las funciones de gestión de riesgos y auditoría interna puedan ser llevadas a cabo por personal o unidades 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 o por personas que formen parte de la alta administración, siempre que sus actividades estén adecuadamente segregadas entre sí y respecto de las áreas comerciales de la entidad.

Asimismo, se establece que las entidades lleven dos registros: Incidentes Operacionales y Pérdidas Operacionales. No obstante, dichas funciones podrán ser

[10] Objectives and Principles of Securities Regulation (IOSCO, 2017). Principio 6
[11] Objectives and Principles of Securities Regulation (IOSCO, 2017). Principio 37.

desempeñadas por una persona que ya forma parte del staff de tecnologías de información de la entidad, siempre que posea los conocimientos y experiencia adecuados.

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

- La norma de Interconexión de Bolsas de Valores[12] 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.

- Respecto a intermediarios de valores y AGF, la Circular 2.054 requiere que la función de Gestión de Riesgos integral (riesgo operacional y otros riesgos) sea desempeñada por un gerente general, un miembro de la alta administración u otro funcionario, mientras que la Circular 1.869 establece que dicha función recae en el gerente general. De la misma forma, ambas circulares ya establecen la obligatoriedad de contar con una función de Auditoría Interna de Riesgos Integral (Intermediarios de Valores) o Encargado de Cumplimiento y Control Interno (AGF). Adicionalmente, para operar en la Bolsa de Comercio de Santiago y en CCLV, los corredores de bolsa deben acreditar, a través de una empresa de auditoría externa, la existencia de: Manuales de Gestión de Riesgo Operacional; planes de continuidad operacional en, al menos, tres escenarios; y documentación de incidentes significativos y medidas de mitigación aplicadas.

Cabe señalar que la mayoría de las entidades cuenta con saldos mantenidos en custodia por cuenta de clientes, por lo cual automáticamente son clasificadas en el bloque superior de volumen de negocios (de acuerdo con la definición dada en la norma) y le aplican los requisitos más exigentes.

No obstante, los costos de implementar la propuesta serían acotados en la industria, ya que las medidas establecidas en la norma han sido incorporadas en la actualidad por los intermediarios, como se muestra en la siguiente tabla:

Requisito	**Descripción**
Quién ejerce la función de gestión de riesgo (miembro del directorio, gerentes o alta administración, Unidad)	De un total de 6 entidades clasificadas en los bloques 1 y 2 de volumen de negocio, 3 de ellas ya disponen de una unidad de gestión de riesgos. Asimismo, de 33 entidades clasificadas en el bloque 3, 28 de ellas cuentan con una unidad de gestión de riesgos y 5 deberían implementar dicha unidad (actualmente a cargo de un miembro del personal).

[12] NCG N° 480 (CMF, 2022)

Requisito	Descripción
Quién ejerce la función de auditoría Interna (Unidad Interna o tercero externo)	De las 6 entidades clasificadas en los bloques 1 y 2, 3 de ellas disponen de una unidad de auditoría interna. Por su parte, 28 entidades del bloque 3 cuentan con una unidad de auditoría interna y 5 deberían implementar dicha unidad (actualmente a cargo de un tercero).
Implementación de BIA y RIA	De las 6 entidades clasificadas en los bloques 1 y 2, 4 de ellas implementan BIA o RIA. Asimismo, 24 entidades del bloque 3 implementan BIA y RIA, 1 tiene sólo RIA, mientras que los 8 restantes deberían implementar ambos.
Encargado de seguridad de la información	De las 6 entidades clasificadas en los bloques 1 y 2, 3 de ellas tienen un encargado de seguridad de la información. Por su parte, 28 intermediarios del bloque 3 cuentan hoy en día con un encargado de seguridad de la información, mientras que los 5 restantes podrían incorporarlo como buena práctica.

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 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.

- La prevención y monitoreo de incidentes operacionales evitaría brechas de seguridad de la información que podrían significar un perjuicio económico para la entidad y sus clientes producto de delitos informáticos que deriven en una pérdida de información o recursos y pudieran afectar la viabilidad financiera de la entidad en el mediano plazo.

- La reanudación temprana de las operaciones de la entidad ante incidentes fortalecería la confianza de los clientes, mitigando el riesgo reputacional. Asimismo, permitiría mitigar el riesgo legal derivado de incidentes que pudieran afectar la integridad y exactitud de la información que maneja la entidad para fines de cumplimiento regulatorio.

- La implementación de un registro y análisis de incidentes operacionales contribuiría al establecimiento de controles mitigantes de riesgo operacional.

Por último, en relación a 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 acotados, en función de que actualmente la Comisión ya tiene implementado procedimientos de Supervisión Basada en Riesgos para Intermediarios de Valores y Corredores de Bolsa de Productos, incluyendo una evaluación del cumplimiento de los planes de acción anuales comprometidos por las entidades para mitigar sus riesgos.

ANEXO N°1: PRÁCTICAS INTERNACIONALES EN GESTIÓN DE RIESGOS

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 *Organization 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 [13] 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.

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

- La organización define el apetito por 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,[14] 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.

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

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.

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*.

ANEXO N°2: PRÁCTICAS INTERNACIONALES EN GESTIÓN DE RIESGO OPERACIONAL

La propuesta normativa considera la revisión de estudios y principios internacionales para la gestión de riesgo operacional elaborados por el *Comité de Basilea sobre Supervisión Bancaria* (BCBS, por sus siglas en inglés), la *Autoridad Europea de Bancos* (EBA), la *Organización Internacional de Reguladores de Valores* (IOSCO), el *Grupo de los Siete* (G7), el *Banco de Pagos Internacionales* (BIS) y la *Asociación Internacional de Supervisores de Seguros* (IAIS).

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

A continuación, se describen los estudios internacionales y legislaciones de países agrupados según los tres ámbitos de gestión de riesgo operacional descritos: Seguridad de la Información y Ciberseguridad, Continuidad del Negocio y Externalización de Servicios.

Seguridad de la Información y Ciberseguridad

El aumento de incidentes operacionales relacionado con las Tecnologías de Información y Comunicación (TIC) y ciberseguridad podrían gatillar eventos de riesgo sistémico en el mercado financiero. En respuesta a ello, la EBA establece recomendaciones para el desarrollo un **Marco de Gestión de Riesgos de TIC** (EBA, 2019). Se propone que la Alta Administración esté a cargo de desarrollar y documentar una **Política de Seguridad de la Información**. Dicha política debería identificar y clasificar las funciones comerciales, los activos de información y los procesos de soporte en base a consideraciones de confidencialidad, integridad y disponibilidad de los datos y el monitoreo continuo de posibles vulnerabilidades, estableciendo las funciones y responsabilidades del personal a cargo y los proveedores externos, junto con planes de capacitación.

También se recomienda que la **gestión del riesgo** sea asignada a un área separada de los procesos operativos de TIC, por ejemplo, una función de control independiente que responda directamente a la Alta Administración y no realice labores de auditoría. Dentro de sus prácticas incluye procedimientos de **registro y monitoreo** de operaciones críticas para la detección de actividades anómalas que puedan afectar la seguridad de la información; el **respaldo y restauración** de datos y sistemas de TIC; el desarrollo de un **Plan de Continuidad del Negocio** aprobado por la Alta Administración, que incluya un conjunto de escenarios severos pero plausibles sobre cambios en funciones comerciales críticas, procesos de soporte y activos de información.

Otro aspecto relevante es la implementación de **medidas de seguridad** debidamente documentadas que abarquen los ámbitos de la seguridad física y lógica, mediante revisiones de seguridad, evaluaciones y pruebas periódicas que aseguren la identificación eficaz de vulnerabilidades en los sistemas TIC.

Dentro de las buenas prácticas se incluye mantener un **registro** actualizado de procesos, funciones y activos TIC, clasificados de acuerdo a su nivel de criticidad, como también procesos de soporte y otros servicios brindados por proveedores externos.

Como parte de la gestión de continuidad del negocio las entidades deberían realizar un **Análisis de impacto de negocio** (BIA). El BIA debe considerar la criticidad de las funciones

comerciales, los procesos de soporte, los activos de información y sus interdependencias. En base a ello, las entidades deben desarrollar planes de **respuesta y recuperación** de las funciones críticas para el negocio.

Se recomienda participar en el **intercambio oportuno de información** de seguridad cibernética con partes interesadas (autoridades, otras entidades, clientes) sobre amenazas, vulnerabilidades, incidentes y planes de respuesta que limiten el impacto potencial de futuros incidentes y promuevan el **aprendizaje continuo**, revisando el marco de seguridad cibernética regularmente y cuando los eventos lo justifiquen (G7, 2016).

Con respecto a las legislaciones de países, se destaca lo siguiente:

- En Australia se debe notificar al regulador los incidentes de ciberseguridad que detecten. Adicionalmente, en el caso de los Intermediarios de Valores, deben notificar toda conducta que a su juicio les parezca sospechosa en relación a la integridad de las operaciones del mercado.
- En Colombia, las entidades deben mantener un Registro de Eventos de Riesgo Operacional, clasificándolo en dos tipos: Ciberseguridad y Otros. Asimismo, deben realizar una autoevaluación de la eficacia de los controles de Ciberseguridad.
- En EE.UU., se requiere a Intermediarios y Bolsas de Valores realizar auditorías periódicas de sus sistemas y notificar al regulador los incidentes de ciberseguridad detectados, pero no se exige llevar una Base de Registro de Incidentes.
- En México, se requieren políticas y procedimientos de seguridad de TI y de gestión de incidentes operacionales. Asimismo, se requiere mantener una Base de Datos de Eventos por Pérdida de Riesgo Operacional y un cálculo del Capital por Riesgo Operacional.
- En Perú, cada entidad debe contar con una Función de Gestión de Seguridad de la Información y Ciberseguridad encargada del Sistema de Gestión de la Seguridad de la Información. En caso de ocurrencia de eventos de interrupción significativa de operaciones, esta deberá ser comunicada a la SMV al día siguiente hábil. Asimismo, cada entidad debe mantener una Base de Eventos de Pérdida por Riesgo Operacional y registrar incidentes que signifiquen una pérdida superior a tres mil soles (o inferior, lo que será determinado por el regulador).
- En Singapur, el regulador debe ser notificado a más tardar en una hora sobre el descubrimiento de un incidente importante. Dentro de los 14 días siguientes, la entidad debe presentar un Informe con su impacto y las medidas correctivas adoptadas.

Continuidad del Negocio

El documento *Revisions to the Principles for the Sound Management of Operational Risk* (BCBS, 2021) define el **riesgo operacional** como aquel derivado de fallas en procesos, personas, sistemas o eventos externos[15]. La **gestión del riesgo operacional** busca

[15] Incluyendo el riesgo legal, pero excluyendo los riesgos estratégicos y reputacional.

identificar las causas subyacentes de cada riesgo, medir las exposiciones de la entidad a los mismos y mitigar prontamente las exposiciones dentro de los niveles de tolerancia definidos.

High-level principles for business continuity (BIS, 2006) destaca la importancia de la **gestión de la continuidad operativa**, entendida como el conjunto de políticas, estándares y procedimientos que aseguren la capacidad de mantener las operaciones o su pronta recuperación en el caso de interrupción, de manera tal que se minimicen sus consecuencias en los ámbitos operacionales, financieros, legales y reputacionales de la entidad.

Principles for Operational Resilience (BCBS, 2021) define la **resiliencia operacional** como la capacidad de la entidad de continuar sus operaciones producto de una adecuada gestión de incidentes de riesgo operacional. En el caso de la industria bancaria, el documento advierte de un mayor riesgo operacional derivado de la rápida adopción de infraestructura tecnológica y tercerización de servicios. El incremento en los niveles de capital y liquidez de los bancos no sería suficiente para sobrellevar fallas operativas de gran escala derivadas de pandemias, ciberataques y desastres naturales.

Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity (IOSCO, 2015) plantea que el acelerado desarrollo tecnológico en las plataformas de negociación podría desencadenar eventos sistémicos de mercado producto de fallas en los **sistemas críticos** [16] de Intermediarios y Bolsas de Valores. En la misma línea, *Revised Consultation on Guidelines on the management of operational risk in market-related activities* (EBA, 2010) recomienda diseñar sistemas de alertas para advertir a la gerencia cuando se detecten operaciones sospechosas o incidentes materiales en el mercado. Para las relaciones entre los *traders* y sus contrapartes del mercado, son considerados mecanismos adecuados de control los procesos de confirmación, liquidación y conciliación de transacciones.

Market Intermediary Business Continuity and Recovery Planning (IOSCO, 2015) recomienda a las entidades financieras incorporar el riesgo de una **interrupción operativa importante** en sus enfoques para la gestión de la **continuidad del negocio**, así como definir **objetivos de recuperación** que reflejen el riesgo que representan para la operación del sistema financiero. Según corresponda, dichos objetivos pueden ser establecidos en consulta con las autoridades financieras pertinentes. Junto con lo anterior, *High-level principles for business continuity* (BCBS-IOSCO-IAIS, 2006) recomienda que los planes de respuesta y recuperación estén en línea con el apetito de riesgo e incorporen las lecciones aprendidas.

Con respecto a los estándares de continuidad, gestión y resiliencia operacional del sistema financiero, cabe destacar los siguientes principios emanados de BCBS, IOSCO y EBA:

- La responsabilidad de la gestión del riesgo operacional recae en el Directorio y la Alta Administración.

[16] Ejemplos de sistemas críticos de Bolsas de Valores corresponden a Sistemas de entrada y ejecución de órdenes, Sistemas de enrutamiento de pedidos, Sistemas de difusión de datos históricos y en tiempo real, Sistemas de infraestructura de red, gestión de bases de datos, almacenamiento, cortafuegos y conexiones de red, Sistemas de vigilancia, Sistemas de Gestión de Riesgos para monitoreo de límites y márgenes.

- El Directorio debe aprobar y revisar periódicamente el marco de gestión del riesgo operacional y de continuidad operativa, y asegurar que la Alta Administración implemente el marco de gestión en todos los niveles de decisión.

- El Directorio debe aprobar y revisar periódicamente una declaración de apetito y tolerancia al riesgo, en donde se definen los niveles y tipos de riesgo operacional que el banco decide gestionar, y los niveles esperados de fallas residuales en los procesos que se está dispuesto a asumir.

- La Alta Administración debe proponer al Directorio una estructura de gobierno clara, eficaz y sólida con recursos materiales y líneas de responsabilidad definidas, transparentes y coherentes. Es responsable de implementar el marco de gestión de riesgo operacional, dentro de los niveles de tolerancia definidos por el Directorio. Dicho marco debiera permitir el monitoreo regular de los riesgos operacionales con mecanismos de información adecuados a nivel del Directorio, la Alta Administración y las unidades de negocio que respalden la gestión proactiva del riesgo operacional.

- El marco de gestión debería ser implementado de modo proporcional a la naturaleza, el tamaño y la complejidad de los servicios ofrecidos por la entidad. Así, debe garantizar la identificación y evaluación integral del riesgo operacional inherente a todos los productos, actividades, procesos y sistemas para asegurarse de que todo el personal de la entidad comprenda los riesgos e incentivos inherentes.

- El marco de gestión debería estar articulado en tres líneas de defensa. La primera línea de defensa corresponde a la gestión de unidades de negocio, la segunda a la gestión de riesgo operacional y la tercera a la de auditoría interna.

- Los planes de continuidad de negocios tienen por finalidad evaluar y mitigar los riesgos asociados a una interrupción operativa importante del negocio producto de fallas en la infraestructura tecnológica, ataques cibernéticos y errores humanos. Deberían estar vinculados al marco de gestión del riesgo operacional, ser actualizados periódicamente y estar en conocimiento del Directorio. Incluyen la asignación de recursos adecuados para su actualización y prueba periódica; evaluaciones de impacto de eventuales interrupciones operativas en sistemas críticos; protocolos de comunicaciones y escalamiento de incidentes; mantenimiento de registros; redundancia de software y hardware; obligaciones de proveedores de servicios y pruebas y escenarios de estrés. Frente a incidentes mayores o con implicaciones transfronterizas, los planes de continuidad deberían incluir estrategias de comunicación con los clientes, otras entidades del sistema financiero y reguladores de distintos países.

- En el caso de Intermediarios y Bolsas de Valores, los planes de continuidad deberían garantizar que sus sistemas críticos se puedan mantener o recuperar de manera oportuna en caso de interrupción. Dichos sistemas deberían ser revisados en forma periódica por un auditor independiente que informe las deficiencias detectadas y las medidas adoptadas para resolverlas a la Alta Administración (y al regulador cuando corresponda). También deberían incluir medidas para monitorear políticas de monitoreo y restricción de operaciones frente a movimientos de precios anómalos, controles de entrada, seguimiento y cancelación de transacciones.

Los Intermediarios y Bolsas de Valores han demostrado su resiliencia operativa a lo largo de la **pandemia** en un contexto marcado por volúmenes récord de negociación y alta volatilidad del mercado. El documento *Operational resilience of trading venues and market intermediaries during the COVID-19 pandemic* (BCBS, 2022) resalta aspectos sobre la **resiliencia operativa** en pandemia tales como la acelerada transición al trabajo remoto, el consecuente aumento del trabajo híbrido en muchas jurisdicciones y una mayor dependencia en sistemas de Tecnologías de Información y Comunicación (TIC).

Con respecto a las legislaciones de países, se destaca lo siguiente:

- En Australia, EE.UU. Singapur y Perú, se deben contar con planes de continuidad de negocios y recuperación ante desastres incluido el respaldo de datos y la realización de pruebas de vulnerabilidad. Cada entidad debe identificar las funciones críticas de su negocio y contar con una función de gestión de riesgo operacional que asegure la continuidad del negocio.

- En EE.UU. se requiere a Intermediarios y Bolsas la reanudación de funciones críticas a las 2 horas de producida una interrupción. Asimismo, a las Contrapartes Centrales contar con una Unidad de Gestión de Riesgos y otra de Auditoría Interna independientes que respondan al Directorio. Por último, las entidades que operan con derivados deben presentar periódicamente una evaluación de riesgos que incluye la aprobación de límites de tolerancia al riesgo por el Directorio.

- En Colombia, el regulador define las actividades críticas del negocio y elabora una matriz de riesgos con sugerencias de mejora en los planes de continuidad del negocio. Lo anterior, sin perjuicio de que trimestralmente las entidades envían una evaluación integral de la gestión de riesgos, incluido el riesgo operacional.

- En México, las entidades deben llevar a cabo un Análisis de Impacto del Negocio (BIA, por sus siglas en ingles) y contar con un Plan de Continuidad de Negocio que incluya al menos una vez al año pruebas de seguridad de TI y ejercicios de crisis (no se requiere enviar los resultados de estas pruebas). Asimismo, deben contar con una Unidad de Administración Integral de Riesgos, un Área de Auditoría Interna independiente, un Comité de Riesgos y un Comité de Auditoría.

- En Perú, cada entidad debe contar con una Función de Continuidad del Negocio encargada del Sistema de Gestión de la Continuidad del Negocio. Asimismo, debe remitir trimestralmente al regulador un Reporte de Indicadores Clave de Gestión de Riesgo Operacional.

- En Singapur, cada entidad debe realizar un BIA y contar con una Base de Registro de Riesgos, que facilite la respuesta ante incidentes (incluyendo proveedores de servicios críticos).

Externalización de servicios

En los últimos años, ha habido una tendencia creciente por parte de las entidades financieras a **tercerizar servicios** para reducir costos y digitalizar sus procesos. A pesar de sus

beneficios, la tercerización implica riesgos en los ámbitos de la seguridad de información y continuidad operacional. Como respuesta a ello, la EBA en su estudio *Guidelines on outsourcing arrangements* recomienda mejores prácticas y directrices para su adecuada gestión. Allí se define **externalización de servicios** [17] a los acuerdos comerciales por medio de los cuales un proveedor realiza actividades que de otra forma serían llevadas a cabo por la entidad que lo contrata (EBA, 2019). En ningún caso, la externalización podría dar lugar a la delegación de responsabilidades, siendo la entidad contratante totalmente responsable de garantizar la prestación adecuada del servicio y cumpliendo con todas sus obligaciones regulatorias.

Dentro de las responsabilidades de la Alta Administración se incluye la elaboración de una **política de subcontratación**. Esta debe incluir las principales etapas del ciclo de vida del servicio subcontratado, los procesos asociados a cada etapa, los roles y responsabilidades del personal, las líneas de negocio involucrada y los controles pertinentes.

El marco de gestión de riesgos debería abordar **planes de continuidad de negocios** para los servicios subcontratados críticos para gestionar posibles fallas o caídas en calidad por debajo de estándares predefinidos. De este modo, se recomienda **previo a cualquier acuerdo de subcontratación**, que las entidades evalúen en primer lugar si el servicio corresponde a una **función crítica** [18], y si se cumplen las condiciones adecuadas para implementar los mecanismos de control y supervisión del proveedor externo. La gestión de la continuidad incluye **planes de salida** para transferir el servicio a otro proveedor en caso de deterioro, interrupción o falla del servicio.

Las entidades deben **monitorear** de forma continua el desempeño de los prestadores de servicios subcontratados. Fundamental en ello es levantar un **registro de subcontratación** de todos los acuerdos de externalización debidamente documentado, en donde se distinga la subcontratación de funciones críticas. También, debe tomar las medidas apropiadas para garantizar que el regulador y auditores puedan obtener rápidamente, previa solicitud, **información y reportes periódicos sobre las tareas subcontratadas** que sea relevante para el cumplimiento contractual y/o la supervisión regulatoria.

Con el objetivo de prevenir fallas potenciales en las actividades tercerizadas, el marco de gestión debería contemplar estándares para la debida diligencia sobre los prestadores previo a la firma de un acuerdo de subcontratación. Para ello, se debe revisar que el prestador tenga la reputación comercial, la experiencia y los recursos suficientes para proveer la función y si está supervisado por las autoridades competentes. Concluida la etapa anterior, el contrato al menos debería contemplar los derechos y obligaciones de las partes en un acuerdo por escrito, una descripción clara de la función subcontratada y la fecha de finalización, las causas del

[17] No se considera tercerización: (1) Funciones que por ley deben ser realizadas por un proveedor específico, como por ejemplo las auditorias. (2) Servicios de información de mercado como Bloomberg, Fitch. (3) Infraestructuras globales de red como Visa, Mastercard. (4) Acuerdos de compensación con cámaras de contraparte central. (5) Infraestructuras globales de mensajería reguladas, entro otros.

[18] Se define como función critica aquella cuya interrupción perjudique seriamente la resiliencia operacional, la continuidad del negocio, la viabilidad financiera de la entidad y/o afecte de manera importante a sus clientes o perjudique su reputación a largo plazo. Aquella relacionada con procesos comerciales complejos o importantes. Aquella que no pueda transferirse rápidamente a otro proveedor de servicios, considerando los costos y el tiempo para hacerlo. Aquella cuya interrupción tenga impacto potencial en la confidencialidad e integridad de los datos entregados al proveedor.

término de la relación contractual (por ej. cuando haya cambios materiales que afecten la calidad del servicio) y las obligaciones financieras de las partes. Aspectos de importancia también refieren a la disponibilidad y seguridad de los datos, incluyendo el derecho de la entidad y las autoridades a auditar al proveedor con respecto a la función crítica subcontratada.

Por último, en el informe *Principles on Outsourcing* (IOSCO, 2021) se resalta la necesidad de incluir el trabajo remoto en los procesos de diligencia, los planes de recuperación y la ejecución de pruebas de la entidad contratante y el proveedor, asegurando el resguardo y la confidencialidad de los datos.

Con respecto a las legislaciones de países, se destaca lo siguiente:

- En EE.UU., el regulador está facultado para auditar todo servicio subcontratado por Intermediarios y Bolsas de Valores, pero no se exige llevar una Base de Registro de Proveedores.

- En México, se exige contar con una política de externalización de servicios que asegure contar con esquemas de registro, redundancia, continuidad y monitoreo de la calidad del servicio.

- En Perú, la política de subcontratación debe contar con procedimientos para evaluar el nivel de riesgo del servicio subcontratado, selección del proveedor, monitoreo del servicio y planes de continuidad del servicio en caso de término anticipado de la relación con el proveedor. Se requiere llevar una Base de Registro de Proveedores.

- En Singapur, está prohibido subcontratar servicios por plazos inferiores a 6 meses, y el regulador está facultado a realizar una auditoría sobre los mismos

ANEXO N° 2: 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:

a) 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*;

b) Identifiquen y evalúen los riesgos inherentes al negocio, centrándose en los riesgos que pudieran perjudicar a los consumidores y la integridad del mercado;

c) Establezcan, implementen y mantengan controles diseñados para mitigar los riesgos previamente señalados; y

d) 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, financiamiento del terrorismo *y financiamiento de la proliferación de armas de destrucción masiva* 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[19], 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*.[20] 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 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

[19] 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.
[20] Final Rule: Management's Report on Internal Control over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports (SEC, 2008).

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: la 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 del 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 intereses 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 de riesgo (KPI).

- 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.

COMISIÓN
PARA EL MERCADO
FINANCIERO

Regulador y Supervisor Financiero de Chile

www.cmfchile.cl