COMISIÓN PARA EL MERCADO FINANCIERO

Nuevos Estándares de Gestión de Riesgos para intermediarios

Bernardita Piedrabuena
Comisionada

Seminario virtual de la Facultad de Derecho de PUC
14 de septiembre 2023

Agenda

- Introducción
- Normas de Gobierno Corporativo y Gestión Integral de Riesgos
- Norma de Riesgo Operacional
- Palabras finales

Agenda

- Introducción
- Normas de Gobierno Corporativo y Gestión Integral de Riesgos
- Norma de Riesgo Operacional
- Palabras finales

Motivación

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

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

- En el caso de la industria bancaria y seguros, se contaba con normas comprehensivas y actualizadas. Las normas que comentaremos vienen a completar, complementar y actualizar la normativa aplicable a intermediarios del sistema financiero:
  - Es importante aplicar estándares consistentes para todos los actores del mercado, ya que si un actor falla, esto puede tener efectos sobre todo el resto de los actores.

- Las normas en consulta no rebaja los estándares en entidades sistémicas: los PFMI se siguen aplicando a las infraestructuras financieras (custodios y sistemas de compensación y liquidación).

- El marco normativo para la gestión de riesgo operacional abarca la supervisión de aspectos de riesgo operacional tales como seguridad de la información, continuidad operacional y externalización de servicios.

Estructura de la norma

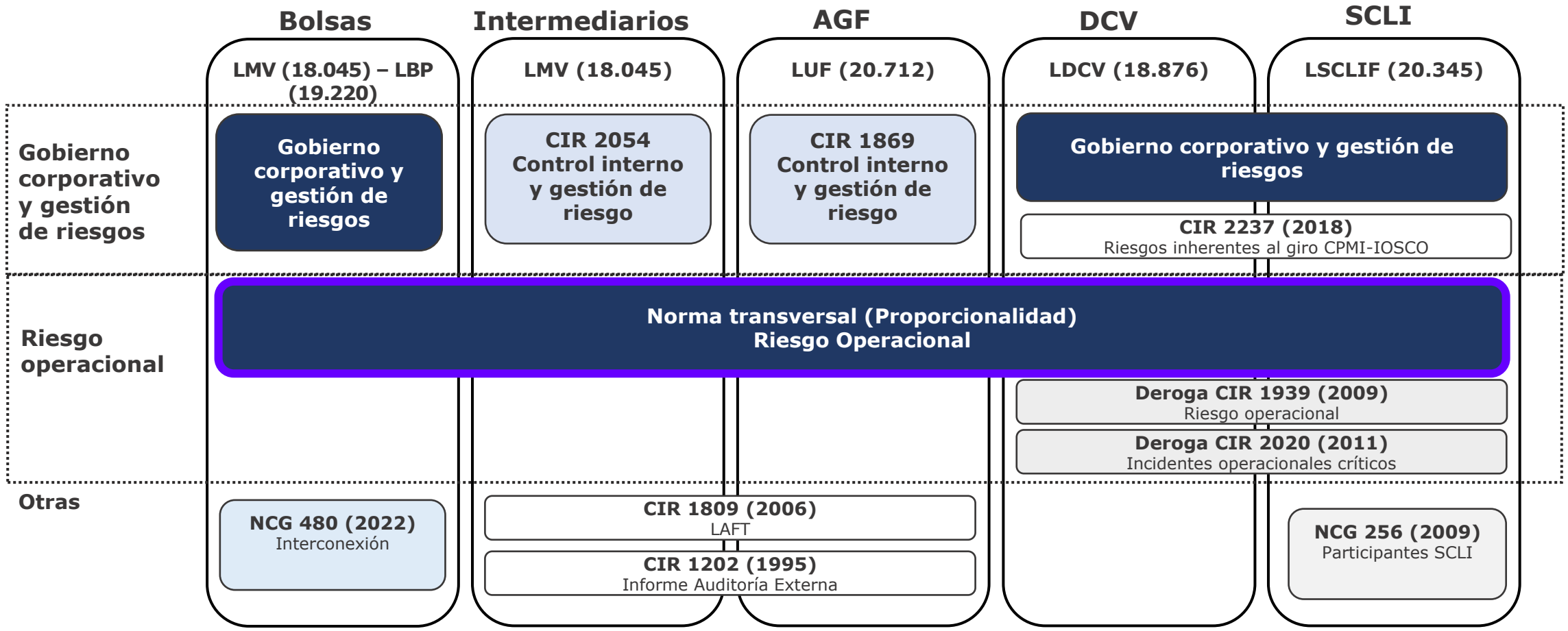
- La propuesta normativa considera la revisión de estudios y principios internacionales de buen gobierno corporativo y gestión de riesgos elaborados por las siguientes organizaciones: el Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO), la Organización Internacional de Normalización (ISO), la Organización Internacional de Reguladores de Valores (IOSCO) y la Organización para la Cooperación y el Desarrollo Económico (OECD).

- 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 revisaron las disposiciones regulatorias de otras jurisdicciones.

Conjunto de Normas de Riesgos

- Se busca fortalecer **las exigencias en materia de gobierno corporativo y gestión de riesgos** de las entidades fiscalizadas del mercado de valores, en línea con estándares internacionales, el marco de la Supervisión Basada en Riesgo de la CMF y el principio de proporcionalidad.



COMISIÓN PARA EL MERCADO FINANCIERO

Agenda

- Introducción
- Normas de Gobierno Corporativo y Gestión Integral de Riesgos
- Norma de Riesgo Operacional
- Palabras finales

Gobierno corporativo y gestión de riesgos

Aspectos comunes en propuestas normativas entidades del mercado de valores

- Rol del directorio u órgano equivalente:
  - Responsable último de la buena Gestión de Riesgos de la entidad.
  - Implementar estructura organizacional, políticas y procedimientos adecuados al nivel de riesgos que enfrenta la entidad.

- Implementación de la función de riesgo y función de auditoría interna, ambas independientes de las áreas generadoras de riesgos y entre ellas:
  - Tres líneas de defensa.

- Identificación de riesgos:
  - Matriz de riesgos.

Gobierno corporativo y gestión de riesgos

Elementos de Proporcionalidad en propuestas normativas entidades del mercado de valores

Entidad	Comités de Directorio (u órgano equivalente)	Procedimientos de Gestión de Riesgos	Gestión de Riesgos y Auditoría Interna
Intermediarios de Valores y corredores de Bolsa de Productos	***Comité de Riesgos obligatorio*** ***Comités de Riesgos y de Auditoría*** deberán estar integrados al menos por un miembro del directorio u órgano equivalente	Adecuados para el volumen y complejidad de actividades de la entidad.	**Función de Gestión de Riesgos - Unidad de Auditoría Interna** En función del volumen y complejidad de actividades de la entidad: • La *Función de Gestión de Riesgos* puede delegar parte de sus actividades en el encargado de cumplimiento, gerentes de área o en otra unidad corporativa de su holding (previo manejo de conflictos de interés). Si el volumen y complejidad de actividades es significativo, deberá crearse una Unidad de Gestión de Riesgos • La *Unidad de Auditoría Interna* puede delegar parte de sus actividades en la unidad corporativa de su holding o en un tercero
Administradoras Generales de Fondos	***Comité de Riesgos obligatorio*** ***Comités de Riesgos, Liquidez, PLAFT* o Auditoría** deberán estar integrados al menos por un miembro del directorio	Adecuados para el volumen y complejidad de actividades de la entidad.	**Unidad de Gestión de Riesgos – Unidad de Auditoría Interna** En función del volumen y complejidad de actividades de la entidad: • La *Unidad de Gestión de Riesgos* puede delegar parte de sus actividades en el encargado de cumplimiento, gerentes de área o en otra unidad corporativa de su holding (previo manejo de conflictos de interés). • La *Unidad de Auditoría Interna* puede delegar parte de sus actividades en la unidad corporativa de su holding o en un tercero
Bolsas de Valores y Bolsas de Productos	***Comité de Riesgos obligatorio*** ***Comités de Riesgos y de Auditoría*** deberán estar integrados al menos por un miembro del directorio	Adecuados para el volumen y complejidad de actividades de la entidad.	**Unidad de Gestión de Riesgos – Unidad de Auditoría Interna** En función del volumen y complejidad de actividades de la entidad, dichas unidades pueden delegar parte de sus actividades en la unidad corporativa de su holding (previo manejo de conflictos de interés)
Sistemas de Compensación y Liquidación - Depósito y Custodia	***Comité de Riesgos obligatorio*** ***Comités de Riesgos y de Auditoría*** deberán estar integrados al menos por un miembro del directorio	Adecuados para el volumen y complejidad de actividades de la entidad.	**Unidad de Gestión de Riesgos – Unidad de Auditoría Interna** En función del volumen y complejidad de actividades de la entidad, dichas unidades pueden delegar parte de sus actividades en la unidad corporativa de su holding

COMISIÓN PARA EL MERCADO FINANCIERO

Agenda

- Introducción
- Normas de Gobierno Corporativo y Gestión Integral de Riesgos
- Norma de Riesgo Operacional
- Palabras finales

Gestión de riesgo operacional intermediarios de valores

- La regulación de riesgo operacional para las entidades del mercado de valores se trataba de manera heterogénea a través de las diferentes entidades del mercado de valores:
  - En Administradores de fondos e intermediarios de valores se trataba tangencialmente.
  - En Depósitos y Custodios de Valores junto con Sociedades de Compensación y Liquidación de instrumentos financieros era virtualmente el único riesgo regulado.
  - En Bolsas y corredores de Bolsa de Productos no era regulado.

- A pesar de que es transversal existen algunos requisitos específicos para algunas industrias en consideración de los riesgos relacionados a la naturaleza de las operaciones (proporcionalidad)

Objetivo de la propuesta

Marco regulatorio integrado industria

- Incorpora requisitos para la **gestión del riesgo operacional** para las entidades:
  - Intermediarios de Valores.
  - Corredores de Bolsas de Productos.
  - Bolsas de Valores.
  - Bolsas de Productos.
  - AGF
  - SCLI
  - DCV

Marco para evaluación de gestión de riesgos

- Fortalece supervisión por medio de **marco para la evaluación de gestión de riesgos** asociada al riesgo operacional.

Reporte de Incidentes

- Las entidades deberán reportar a CMF:
  - Registro de **incidentes** operacionales.
  - Registro de **pérdidas** operacionales.

Definición de riesgo operacional usada

- 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 contingencias físicas, errores, fraudes.

- Incluye el riesgo de pérdidas ante cambios regulatorios que afecten las operaciones de la entidad, como también pérdidas derivadas de incumplimiento o falta de apego a la regulación vigente.

Gestión de Riesgo Operacional

Sistema de Gestión del Riesgo Operacional (SGRO)

- Políticas, procedimientos y controles que permitan la resiliencia operativa de la entidad, consistentes con el apetito al riesgo definido por el directorio u órgano equivalente.
- Líneas claras de responsabilidad sobre la gestión del riesgo operacional.
- Indicadores de medición del riesgo operacional que permitan evaluar y monitorear periódicamente el grado de exposición a los distintos riesgos, permitiendo establecer niveles de alerta y evaluar la eficacia de los controles adoptados.
- Políticas de capacitación del todo el personal en gestión de riesgo operacional.
- Procedimientos de mejoramiento continuo de la gestión de riesgo operacional (herramientas, procedimientos y controles), incluyendo el análisis de incidentes y pérdidas operacionales.

Gestión de Riesgo Operacional

Seguridad de la información y ciberseguridad

- Identificación
- Protección y detección
- Respuesta y recuperación

Continuidad de negocio

Externalización de servicios

Información de incidentes operacionales

Seguridad de la información y ciberseguridad

Identificación

- Definir los activos de información críticos
- Clasificar la información, considerando dimensiones de disponibilidad, confidencialidad e integridad
- Llevar un inventario actualizado de activos de información.

Seguridad de la información y ciberseguridad

Protección y detección

- Controles de acceso a instalaciones físicas.
- Herramientas de registro, control y monitoreo de las actividades realizadas por los usuarios.
- Procedimientos de acceso del personal y los clientes a los sistemas (otorgamiento, modificación, revocación).
- Herramientas y controles para la detección y monitoreo de ataques cibernéticos y actividades anómalas (ej. firewalls de aplicaciones web, sistemas de prevención de intrusos, sistemas anti-denegación de servicios, filtrado de correo electrónico, antivirus, etc.).
- Gestión de configuración de activos de información y actualización de seguridad de software
- Respaldo, transferencia, restauración y eliminación de información, tomando en consideración técnicas de encriptación y segmentación de redes.
- Procedimientos de almacenamiento, transferencia y respaldo de información en la nube.

Seguridad de la información y ciberseguridad

Respuesta y recuperación

- Procedimientos de respuesta y recuperación ante incidentes que consideren la recuperación oportuna de las funciones críticas, los procesos de respaldo y soporte, los activos de información y las interdependencias con terceros.
- Procedimientos de comunicaciones para mantener informado en forma oportuna al directorio u órgano equivalente, a otras partes interesadas y a la CMF de las medidas adoptadas para resolver incidentes, incluyendo el cumplimiento de las normas de protección de datos personales y derechos del consumidor.
- Proceso de gestión de cambio con la implementación de pruebas integrales para asegurar que no hubiere un impacto adverso previo al paso de producción de un servicio o activo de información.
- Proceso de gestión de obsolescencia tecnológica del hardware y software.

Continuidad del negocio

- Análisis de Impacto del Negocio (BIA) que considere los tiempos máximos tolerables de recuperación, los tiempos objetivo de recuperación, los puntos objetivo de recuperación y los niveles mínimos aceptables de operación.
- Análisis de Impacto de Riesgo (RIA) que permita identificar los riesgos de posibles eventos de continuidad y las medidas preventivas para cumplir los objetivos del BIA.
- Plan de Continuidad del Negocio y Recuperación ante Desastres:
  - Realización de pruebas anuales, diseñadas en proporción al volumen y complejidad de las operaciones de la entidad.
  - Las pruebas deberán estar basadas en escenarios no sólo asimilables a eventos reales sino a eventos severos pero plausibles.
- Sitio secundario para reanudar las operaciones en caso de un evento de continuidad.

Externalización de servicios

- Identificar los servicios relevantes para el cumplimiento normativo, la seguridad de la información o la continuidad del negocio (servicios críticos)
- Identificar servicios que requieren aprobación del directorio u órgano equivalente para ser externalizados.
- Mantener un registro de servicios externalizados que describa en detalle el servicio, su fecha de inicio y término, el proveedor que lo prestó y las obligaciones contraídas por éste.
- Definir los elementos mínimos del contrato de prestación de servicios externalizados (eg. las obligaciones contraídas por el proveedor y las estrategias de término de la prestación).
- Procedimientos para la selección de proveedores, incluyendo un due diligence.
- Procedimientos para el monitoreo de proveedores, incluyendo la realización de auditoría de servicios por parte del proveedor o bien certificaciones o revisiones independientes.
- En el caso de subcontratación en cadena, el proveedor es responsable en última instancia de la calidad de la prestación del servicio contratado.

Reporte de incidentes operacionales

Registro y comunicación de incidentes

- Incidentes operacionales críticos.
- Plazo máximo de 3 horas para intermediarios y AGF.
- Directorio u órgano equivalente define encargado de reporte de incidentes.
- En caso de que lo requiera la CMF, la entidad elaborará un informe de las causas del incidente y las medidas adoptadas para su resolución.

Registro y comunicación de pérdidas

- Pérdida financiera resultante de la materialización de riesgo operacional
- Umbral de 150 UF.
- Criterios para elaborar el registro de pérdidas.

Criterios para el registro de pérdidas

- Contar con procesos documentados (la CMF podrá requerir su validación por auditores externos).
- Incluir totalidad de actividades y exposiciones.
- Cálculo de pérdidas brutas y pérdidas netas.
- Detalle de información descriptiva sobre las causas del evento de pérdida en proporción al importe bruto de la pérdida.

Palabras finales

- En el corto plazo se analizarán los comentarios de la consulta pública que finalizó hoy:
  - La norma entra en vigencia a fines de 2023.

- En los próximos meses publicaremos la norma para los intermediarios de instrumentos financieros de la Ley Fintec.

- Importancia de un adecuado involucramiento de la más alta administración en la gestión de los riesgos.

- Los riesgos operacionales evolucionan, en particular los relacionados a ciberseguridad: importancia de actualizaciones continuas.

COMISIÓN PARA EL MERCADO FINANCIERO

Nuevos Estándares de Gestión de Riesgos para intermediarios

Bernardita Piedrabuena
Comisionada

Seminario virtual de la Facultad de Derecho de PUC
14 de septiembre 2023