COMISIÓN
PARA EL MERCADO
FINANCIERO

Mesa Consultiva de Gobierno Corporativo y Gestión de riesgos

Asesorías de crédito e inversión

Mayo 2023

www.CMFChile.cl

Mesa Gobierno Corporativo y Gestión de Riesgos

Alcance de la Mesa.

Servicios de asesoría de inversión y asesoría de crédito de la ley N° 21.521.

Definiciones

Asesoría crediticia: la prestación de servicios de evaluaciones o recomendaciones a terceros respecto de la capacidad o probabilidad de pago de personas naturales y jurídicas o entidades, o de la identidad de éstas, para fines de la obtención, modificación o renegociación de un crédito o financiamiento.

Asesoría de inversión: la prestación de servicios de evaluaciones o recomendaciones a terceros respecto de la conveniencia de realizar determinadas inversiones u operaciones en valores de oferta pública, instrumentos financieros o proyectos de inversión. No comprende la asesoría previsional, entidades de asesoría previsional, asesores financieros previsionales o entidades de asesoría financiera a que se refiere el decreto ley N° 3.500, de 1980, ni los agentes de venta de compañías de seguros.

Propuesta de Norma de Gobierno Corporativo y Gestión Integral de Riesgos

El desarrollo de las actividades de asesoría de inversión y asesoría crediticia lleva a las entidades que prestan dichos servicios a asumir distintos riesgos, los que pueden llegar a afectar el patrimonio de sus clientes, así como información sensible de ellos.

En este contexto, se hace necesario que dichas entidades cuenten con la estructura organizacional y los medios materiales y humanos adecuados al volumen y complejidad de sus operaciones de negocio. Para ello, la CMF propone una norma de gobierno corporativo y gestión integral de riesgos.

La entidad deberá contar con políticas y procedimientos de gobierno corporativo y gestión de riesgos al menos en los siguientes ámbitos: funcionamiento, toma de decisiones y monitoreo de riesgos de la alta administración (o directorio, en caso de contar con uno); políticas procedimientos y controles de riesgos; seguridad de la información y registro de incidentes y pérdidas operacionales; manejo de conflictos de interés; prevención del lavado de activos y financiamiento del terrorismo; conservación y manejo de información confidencial; divulgación de información veraz y oportuna a los clientes y otras partes interesadas; idoneidad y conocimientos del personal de la entidad para efectuar recomendaciones o evaluación de productos; contratación de personal y cumplimiento regulatorio.

I. Políticas, procedimientos y controles de gestión de riesgos.

Establecer políticas, procedimientos y controles de riesgos en los siguientes ámbitos:

- Política que aborde y divulgue los conflictos de interés que se presenten entre la entidad o sus empleados y los clientes en la prestación de la asesoría. Esto incluirá, pero no se limitará a comunicar comisiones que reciban por productos ofrecidos; vínculos de la empresa con los oferentes de productos recomendados; exposiciones de inversión a los productos ofrecidos. Dicha política deberá ser divulgada en el sitio web del prestador en un lugar de fácil acceso (o mecanismo alternativo), con un nivel de detalle que permita a cada cliente tomar una decisión informada respecto de los potenciales conflictos para los servicios ofrecidos.
- Política de idoneidad en la comercialización y publicidad de productos. La asesoría debe procurar que los servicios ofrecidos al cliente sean entendidos por él, incluidos los riesgos derivados de la recomendación o evaluación realizada a través de la asesoría. Además, debe haber procedimientos que aseguren un análisis sobre la necesidad del producto para los clientes, resguardando que quienes solicitan el servicio cuenten con la suficiente información para tomar sus decisiones, en aspectos como los riesgos y costos de una recomendación de inversión.
- Políticas, procedimientos y controles que garanticen que las recomendaciones o evaluaciones se realicen en el interés y la protección de los clientes de la entidad, en forma transparente y acorde con las necesidades, expectativas y disposición al riesgo que éstos les hayan comunicado previamente.
- Procedimientos y sistemas que permitan el mantenimiento apropiado de registros exigidos por la normativa vigente, considerando la integridad, disponibilidad y confiabilidad de la información.
- Cumplimiento de leyes y normativas de prevención del lavado de activos y financiamiento del terrorismo, la debida diligencia con clientes y proveedores, entre otras.
- Establecer políticas y procedimientos que aseguren que el prestador cuente con los conocimientos necesarios y la debida experiencia para poder prestar sus servicios (acorde a NCG N° 472).

  Sin perjuicio de lo anterior, las políticas y procedimientos mencionados deberán cumplir los requisitos de publicidad, comercialización y educación financiera establecidos en la normativa de Obligaciones de Información que debe dictar esta Comisión como parte del conjunto de normas de la ley Fintec. Asimismo, deberán cumplir los requisitos de idoneidad y acreditación de conocimientos del personal, idoneidad de algoritmos (incluyendo su verificación o certificación) y de educación financiera establecidos en la normativa de Autorización de Asesores Crediticios y de Inversión que debe dictar esta Comisión.

II. Otros elementos que podría incluir la norma (Proporcionalidad)

1. Alta administración (o directorio)

La alta administración es responsable del gobierno corporativo y la gestión de riesgos de la entidad en concordancia con el volumen y complejidad de sus negocios para lo cual:

- Aprueba los niveles de tolerancia de riesgos identificados en el desarrollo de su actividad, tales como riesgo operacional y riesgo reputacional.
- Aprueba y monitorea el cumplimiento de los planes de las funciones de Gestión de Riesgos y Auditoría Interna.
- Establece un mecanismo efectivo para la recepción, gestión y resolución de reclamos internos o externos y denuncias de incumplimiento al código de ética.

2. Función de Gestión de Riesgos.

- Independiente de áreas operativas y con reporte directo a la alta administración.
- Puede ser desempeñada por una unidad del grupo económico al que pertenece o incluso por una sola persona, en función del volumen y complejidad de las operaciones de la entidad.
- Establece las políticas y procedimientos de gestión de riesgos de la entidad.
- Establece una metodología para el control y monitoreo de riesgos, la que debiera incluir un mapeo de los distintos procesos del negocio de asesoría, determinación de los riesgos operacionales y reputacionales relevantes y establecimiento de controles mitigantes.
- Elabora un plan de gestión de riesgos actualizado al menos anualmente.
- Emite un informe periódico sobre el plan de gestión de riesgos para la alta administración, indicando los incumplimientos detectados, causas que los originaron, medidas adoptadas y efectividad de dichas medidas.
- Reevalúa los riesgos ante distintos escenarios, por ejemplo:
    - **a.** Cambios en las condiciones del entorno económico, de la industria y de los mercados en los que opera la entidad.
    - **b.** Introducción de nuevos productos, operaciones y actividades del negocio.
- Establece un sistema eficaz de comunicaciones que asegure que la información relevante para la gestión de riesgos llega en forma veraz, suficiente y oportuna a la alta administración y otras instancias responsables.

3. Función de Auditoría Interna

- Independiente de las áreas operativas, reporta a la alta administración.
- Puede ser desempeñada por una unidad del grupo económico al que pertenece o incluso por una sola persona, en función del volumen y complejidad de las operaciones de la entidad.
- Evalúa el correcto funcionamiento del sistema de control interno y gestión de riesgos, el cumplimiento regulatorio y del código de ética.
- Cuenta con un plan de auditoría actualizado al menos anualmente para monitorear la oportuna corrección de las observaciones por deficiencias en la gestión de riesgos

GESTION DE RIESGO OPERACIONAL

La gestión de riesgo operacional de los servicios de asesoría de inversión o crediticia se guiará por la normativa de gestión de riesgo operacional a publicarse por la CMF, tomando en consideración una **Gestión de la Seguridad de la Información** con los siguientes lineamientos:

- Capacitación del personal en la materia, de manera que sea consciente de los riesgos de seguridad de la información y ciberseguridad y contribuya a una adecuada gestión de éstos.
- Clasificar la información, teniendo en consideración, dimensiones tales como disponibilidad, confidencialidad e integridad.
- Resguardar debidamente la información de los clientes:
    - **a.** Implementar un inventario de esos activos de información, incluyendo una clasificación de estos.
    - **b.** Implementar un inventario de servicios relacionados con los activos de información.
    - **c.** Implementar controles de acceso a las instalaciones, infraestructuras de negocios y sistemas de información.
    - **d.** Implementar herramientas de registro, control y monitoreo de la actividad de los usuarios de sistemas.
    - **e.** Políticas y procedimientos para resguardar la confidencialidad de la información de los clientes, incluyendo el consentimiento expreso para el uso de la información por parte de estos, y 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. Dichas políticas, deberán incluir un proceso de gestión de reclamaciones en línea con lo dispuesto en el título II de la ley N°19.628 sobre la protección de datos de carácter personal.
- Implementar controles que permitan mitigar los riesgos derivados del uso de dispositivos móviles y del acceso remoto realizado por el personal.
- Gestionar las condiciones ambientales para la localización segura para los equipos y herramientas.

- Procedimientos y controles adecuados para el desarrollo e implementación de los algoritmos, incluyendo *robo-advisors*, que garanticen que las recomendaciones o evaluaciones del asesor se realicen en el interés y la protección de sus clientes, acorde con las necesidades, expectativas y disposición al riesgo que éstos les hayan comunicado previamente.
- Políticas, procedimientos y controles de seguridad de la información que resguarden la privacidad de los datos del cliente que contrate los servicios de asesoría.
- Considerar herramientas de gestión de la ciberseguridad tales como programas de gestión de parches de *software* y *firmware*, segmentación de redes, protección de redes ante ataques por medio de *firewalls*, sistemas de prevención de intrusos, elevación de privilegios, gestión de identidades y acceso físico y lógico, mecanismos de control de identidad para evitar suplantación de terceros, normas y procedimientos que establecen la información que requiere ser protegida a través de técnicas de cifrado, entre otras.
- Procedimientos de identificación de amenazas de ciberseguridad tales como *pentesting*, vectores de ataque, denegación de servicios, *phishing*, *malware*, inyección de código, entre otros.

Preguntas.

- ¿Qué métricas deben usarse para establecer la proporcionalidad de esta regulación?
- ¿Qué "umbral" cree que debe usarse para eximir requerimientos? ¿Qué requerimientos cree que debería eximirse?
- ¿Qué definiciones requieren una mayor precisión?
- ¿Existen otros elementos que debieran regularse en gestión de riesgo o gobierno corporativo que no se encuentren contenidos en esta propuesta? ¿Qué otros servicios adicionales prestan en conjunto con asesorías de inversión y/o crédito de forma regular?
- ¿Qué interrelación y/o dependencia tienen con las entidades fiscalizadas por la CMF?