COMISIÓN
PARA EL MERCADO
FINANCIERO

Mesa Consultiva de Gobierno Corporativo y Gestión de Riesgos

Intermediarios y Custodios de Instrumentos Financieros y Enrutadores de órdenes

Mayo 2023

www.CMFChile.cl

Mesa Gobierno Corporativo y Gestión de Riesgos

Alcance de la Mesa.

Servicios de intermediación, custodia de instrumentos financieros y enrutamiento de órdenes de la ley N° 21.521.

Definiciones.

Intermediación de instrumentos financieros: servicio en virtud del cual se realizan actividades de compra o venta de instrumentos financieros para terceros, mediante cualquiera de las siguientes formas: adquiriendo o enajenando por cuenta propia instrumentos financieros, con el ánimo anterior de vender o comprar esos mismos instrumentos al tercero, o adquiriendo o vendiendo instrumentos financieros a nombre de o para dicho tercero.

Custodia de instrumentos financieros: mantener a nombre propio por cuenta de terceros, o a nombre de éstos, instrumentos financieros, dinero o divisas que provengan de los flujos o de la enajenación de instrumentos financieros mantenidos en custodia, o que hayan sido entregados por éstos para la adquisición de instrumentos financieros o para garantizar las operaciones con esos instrumentos.

El servicio de custodia incluirá márgenes o colaterales de terceros y custodia de contraseñas (claves privadas) que permitan acceso a los activos digitales.

Enrutamiento de órdenes: servicio de canalización de órdenes recibidas de terceros para la compra o venta de valores de oferta pública o instrumentos financieros a sistemas alternativos de transacción, intermediarios de valores o corredores de bolsas de productos.

Propuesta de Norma de Gobierno Corporativo y Gestión Integral de Riesgos

El desarrollo de la actividad de intermediación, la custodia de instrumentos financieros y el enrutamiento de órdenes llevan a las entidades que prestan dichos servicios a asumir distintos riesgos, los que pueden llegar a afectar su patrimonio o el de los clientes.

Así, estas entidades deberán contar con la estructura organizacional y los medios materiales y humanos adecuados al volumen y complejidad de sus operaciones de negocio. La CMF propone una norma de gobierno corporativo y gestión integral de riesgos en línea con la norma equivalente para intermediarios de valores[1], que se puede resumir en los lineamientos expuestos a continuación.

[1] Nueva versión a ser publicada prontamente, con los elementos incluidos en este documento.

1. Alta administración de la entidad (o del directorio en caso de contar con uno).

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; políticas, procedimientos y controles de riesgos; funciones de gestión de riesgos y auditoría interna; seguridad de la información, externalización de servicios y registro de incidentes y pérdidas operacionales; manejo de conflictos de interés; manejo, transferencia y custodia de instrumentos financieros de clientes (realizada por la propia entidad o terceros); prevención del lavado de activos y financiamiento del terrorismo, incluyendo operaciones transfronterizas; manejo, transferencia y conservación de información confidencial; divulgación de información veraz y oportuna en el interés de los clientes y otras partes interesadas; idoneidad, conocimientos y contratación del personal de la entidad; cumplimiento regulatorio, incluido capital y garantías.

Sin perjuicio de lo anterior, las políticas de divulgación de información veraz y oportuna a clientes y otras partes interesadas 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.

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

- Aprobar una estructura de la organización que permita el tratamiento y seguimiento adecuado de los temas específicos. Podrá generar comités u otras estructuras que permitan una gestión eficiente de la organización.
- Aprobar los niveles de tolerancia a los riesgos identificados.
- Aprobar y monitorear el cumplimiento de planes de las funciones de Gestión de Riesgos y Auditoría Interna.
- Establecer políticas y procedimientos de contratación de empleados que aseguren que el prestador disponga de personal con la debida experiencia para desempeñar sus funciones, y velar por que la entidad cuente con el recurso humano calificado para la gestión de riesgos.
- Establecer mecanismos para la recepción, gestión y resolución de reclamos internos/externos y denuncias de incumplimiento al código de ética.
- Establecer un programa de mejoramiento continuo de la gestión de riesgos de la entidad.
- Política de idoneidad en la oferta, publicidad y comercialización de productos. La entidad debe procurar que los servicios ofrecidos al cliente sean entendidos por él, incluidos los riesgos derivados, para lo cual

contará con un procedimiento de divulgación y aceptación de riesgos previo a la contratación del servicio.

- Establecer procedimientos de debida diligencia, requisitos, y los procesos de aprobación que se aplican antes de admitir instrumentos financieros y/o prestar servicios. Antes de admitir un instrumento, se deberá verificar que este cumpla las políticas y procedimientos de funcionamiento de la entidad, así como evaluar la calidad del instrumento, considerando aspectos tales como la experiencia y reputación del emisor.

2. Políticas, procedimientos y controles de riesgos.

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

- Integridad de los sistemas de negociación de instrumentos financieros que garantice que el acceso y el uso de dichos sistemas por parte de los clientes de la entidad sea transparente, equitativo y evite prácticas de manipulación de precios de los instrumentos negociados.
    - **a.** Políticas y procedimientos para el servicio de enrutamiento de órdenes:
        i. Se divulgue apropiadamente la información al cliente sobre los beneficios recibidos por dirigir las órdenes hacia ciertas plataformas de negociación o intermediarios en particular.
        ii. Resguarden la privacidad de las órdenes pendientes de ejecutar de clientes, así como el debido uso de esta información por los empleados del prestador, así como cualquier otro tipo de información confidencial.
    - **b.** Políticas y procedimientos para el servicio de intermediación.
        i. Políticas y procedimientos de ejecución de órdenes en nombre de terceros, que aseguren la transacción de mayor conveniencia para el cliente al considerar factores como precio, costo, prontitud, etc.
        ii. Comunicar estas políticas y procedimientos a sus clientes.
- Política que aborde y divulgue los conflictos de interés que se presenten entre la entidad o sus empleados y los clientes, lo que deberá ser considerado en las políticas de comunicaciones y remuneraciones de la entidad, y en los contratos de prestación de servicios. Esto incluirá, pero no se limitará a comunicar comisiones; 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 método alternativo), con un nivel de detalle que permita a cada cliente tomar una decisión informada respecto de los potenciales conflictos para los servicios ofrecidos.
- Definir procedimientos para la adecuada protección de los activos financieros, tanto de la entidad como de sus clientes, incluyendo:

a. Resguardo de los activos de los clientes en caso de insolvencia del prestador.

b. Segregación de los activos de la entidad de aquellos de los clientes.

- Sistemas que permitan el mantenimiento apropiado de registros exigidos por la normativa vigente, considerando la integridad, disponibilidad y confiabilidad de la información.
- Sistemas que provean información de forma periódica al cliente sobre sus posiciones (por ejemplo, cartolas). En el caso de servicios de custodia derechos sobre activos, cuando se requiere su autorización sobre el activo custodiado, entre otras.
- Segregación apropiada de los deberes y las funciones claves.
- Procedimientos de control para el cumplimiento de regulaciones aplicables a la entidad, incluyendo prevención del lavado de activos y financiamiento del terrorismo, la debida diligencia con clientes y proveedores.
- Procedimientos de aprobación, evaluación y control de algoritmos de negociación que garanticen que las transacciones 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.
- Contrato de custodia entre el prestador y clientes que incluya elementos tales como: la identidad de las partes, la descripción del servicio, los medios de comunicación entre las partes, descripción de los sistemas de seguridad del prestador, las tarifas y la legislación aplicable al acuerdo.
- Política, procedimientos y controles de riesgos de custodia para:

a. Los medios de acceso del cliente a los instrumentos financieros, activos virtuales o claves criptográficas.

b. Los activos de propiedad de terceros están protegidos de pérdidas producto de errores o fallas de sistemas, personas o procesos.

c. La información contenida en el registro de custodia corresponde a transacciones y movimientos autorizados por el cliente, es fidedigna y representa debidamente los derechos de los clientes sobre los valores de su propiedad.

d. La información entregada al cliente acerca de los movimientos y saldos de sus valores en custodia es veraz, completa y consistente con el registro de custodia.

3. Función de Gestión de Riesgos.

- Independiente de las áreas operativas y 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 (financieros, operacionales, mercado, legal, reputacional, según aplique).
- Establece una metodología para la medición, control y monitoreo de riesgos, la que debe incluir un mapa de procesos, determinación de los riesgos de cada uno, exposición y mitigadores.
- Elabora un plan de gestión de riesgos, consistente con la estrategia de negocios y la protección de los activos e intereses de los clientes. Dicho plan se actualiza anualmente.
- Emite un informe periódico sobre el cumplimiento del plan de gestión de riesgos para la alta administración, indicando los incumplimientos detectados, causas que los originaron, medidas adoptadas.
- Reevalúa los riesgos ante distintos escenarios, por ejemplo:
    - **a.** Cambios en las condiciones del entorno económico, industria y mercados relevantes.
    - **b.** Introducción de nuevos productos, operaciones y actividades del negocio.
- Establece un sistema de comunicaciones que asegure que la información relevante para la gestión de riesgos llega en forma veraz, suficiente y oportuna a instancias responsables.

4. Función de Auditoría Interna.

- Independiente de las áreas operativas, reporta a la alta administración.
- Puede ser desempeñada por una unidad (o persona) del grupo económico al que pertenece, en función del volumen y complejidad de las operaciones de la entidad.
- Cumple las siguientes funciones:
    - **a.** Evalúa el correcto funcionamiento del sistema de control interno y gestión de riesgos y el cumplimiento de las disposiciones regulatorias de la entidad.
    - **b.** Verifica el cumplimiento de los códigos de ética y manuales operativos.
- Cuenta con un plan de auditoría actualizado al menos anualmente.
- Los prestadores de servicios de custodia deberán efectuar anualmente una revisión por empresas de auditoría externa, de los procesos y controles asociados a la actividad de custodia.
    - **a.** Empresas de auditoría externa deberán emitir un informe, el que deberá contener su opinión respecto a si los procesos y controles fueron diseñados adecuadamente.

b. La revisión deberá contemplar pruebas de los controles existentes.

c. Un proceso de revisión regular de los saldos de activos de terceros que mantiene en custodia.

GESTION DE RIESGO OPERACIONAL

La gestión de riesgo operacional de la intermediación, custodia de instrumentos financieros y enrutamiento de órdenes será incluida en la norma de gestión de riesgo operacional de entidades de valores[2].

Dicha norma requiere que la alta administración apruebe y supervise en forma continua la gestión de los siguientes ámbitos:

1. Seguridad de la información y ciberseguridad

Contar con una política de seguridad de la información y ciberseguridad, que considere:

- Capacitación del personal en la materia para la concientización de los riesgos de seguridad de la información y ciberseguridad y contribución de una adecuada gestión de éstos.
- Clasificar e implementar un inventario de los activos de información, considerando aspectos tales como su disponibilidad, confidencialidad e integridad, también, identificar activos críticos para el funcionamiento del negocio.
- Implementar controles de acceso a instalaciones, infraestructuras y sistemas de información, así como contar con herramientas de registro y control de actividad de usuarios.
- Implementar controles que permitan mitigar los riesgos derivados del uso de dispositivos móviles y del acceso remoto realizado por el personal.
- Gestionar las condiciones para la localización segura para los equipos.
- Tener procedimientos de respuesta y recuperación ante incidentes. Esto incluye: recuperación oportuna de funciones críticas; procesos de respaldo y soporte; activos críticos de información y; las interdependencias con terceros.
- Políticas y procedimientos para resguardar la confidencialidad de la información de los clientes, 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,

[2] Se encuentra en proceso de publicación por la CMF.

deberán estar en línea con lo dispuesto en el título II de la ley N°19.628 sobre la protección de datos de carácter personal.

- 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*, entre otros mecanismos de seguridad, además de normas y procedimientos que establecen la información que requiere ser protegida a través de técnicas de cifrado.
- Procedimientos de identificación de amenazas de ciberseguridad tales como *pentesting*, vectores de ataque, denegación de servicios, *phishing*, *malware*, inyección de código, entre otros.

2. Continuidad de negocio.

Contar con una política de mejoramiento de la continuidad de negocio, que considere:

- Desarrollo, adquisición y actualización de infraestructura tecnológica
- Disponer de un sitio secundario que permita a la entidad reanudar la operación en caso de que esta se vea interrumpida en el sitio principal.
- Contar con un Plan de Continuidad de Negocio, que contenga los procedimientos de respuesta y recuperación ante incidentes, los roles y responsabilidades del personal y un Análisis de Impacto del Negocio, incluyendo puntos y tiempos objetivo de recuperación, el que no podrá ser inferior a 20 minutos cuando el intermediario sea la única contraparte potencial del cliente. Además, deberá existir un uptime de la provisión de servicios (establecido por producto) definido por la entidad no menor a xx%, en términos mensuales. Los horarios de servicios deberán estar establecidos en los términos del contrato.
- Procedimientos de escalamiento, comunicaciones, gestión y reporte de eventos de continuidad operacional (alta administración y partes interesadas, incluida CMF).
- Realización de pruebas periódicas para gestionar la continuidad operacional en escenarios tales como un cambio en los activos de información o desastres naturales.
- En caso de servicios de custodia, se deberá disponer de sistemas que:
    - **a.** Registren las posiciones abiertas, así como las modificaciones en los derechos sobre el activo, en nombre cada cliente.
    - **b.** Soporten los medios de acceso y restitución del cliente a sus activos de forma oportuna.
    - **c.** Permitan la segregación de las cuentas y activos de los clientes de los activos del prestador de los servicios de custodia.
- En el caso de enrutadores de órdenes, deberán disponer de sistemas que permitan una pronta transmisión de las órdenes de clientes hacia

sistemas alternativos de transacción, intermediarios de valores u otras entidades.

3. Externalización de servicios.

Contar con una política de externalización de servicios, que considere:

- Definir los servicios críticos para la continuidad de las operaciones de la entidad, el cumplimiento normativo y la calidad de los productos ofrecidos.
- Definir los servicios que solo pueden ser externalizados con la aprobación previa de la alta administración.
- Realizar la debida diligencia en la contratación de proveedores.
- Contenidos mínimos de los contratos con proveedores de servicios externalizados:
    - **a.** Descripción del servicio contratado, plazo de vigencia y obligaciones del proveedor.
    - **b.** Requisitos de seguridad de la información, ciberseguridad y continuidad de negocios que deberá cumplir el proveedor.
    - **c.** Que el proveedor realice periódicamente informes de auditoría interna o revisiones independientes de sus servicios.
    - **d.** Estrategias para el término de la prestación de servicios externalizados sin perjudicar las operaciones de la entidad.
    - **e.** Tratamiento de datos personales asociados al servicio, en cumplimiento con la regulación vigente al respecto.
- Contar con un registro de servicios externalizados. En caso de subcontratación en cadena, detallar cuáles son las entidades a las que el proveedor subcontrata el servicio.
- Monitorear periódicamente que los proveedores cumplan con las condiciones pactadas.

4. Información de incidentes y perdidas operacionales

- Las entidades deberán comunicar a la CMF los incidentes operacionales críticos que afecten o pongan en riesgo la continuidad del negocio, en un plazo máximo de 30 minutos luego de su ocurrencia, entre ellos, fallas en servicios importantes para el negocio, problemas que afecten la seguridad de la información; ataques del ciberespacio y; virus en los activos de información críticos.

- Se deberá elaborar un informe interno con una investigación y análisis de incidente críticos.
- También deberán ser reportadas semestralmente las pérdidas operacionales materializadas por encima de un umbral definido por la CMF.

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 prestan en conjunto con intermediación, custodia y/o enrutamiento de órdenes de forma regular?
- ¿Qué interrelación y/o dependencia tienen con las entidades fiscalizadas por la CMF?