



COMISIÓN  
PARA EL MERCADO  
FINANCIERO

## Mesa Consultiva de Gobierno Corporativo y Gestión de Riesgos

Sistemas Alternativos de Transacción y Plataformas de  
Financiamiento Colectivo

Mayo 2023

[www.CMFChile.cl](http://www.CMFChile.cl)

# Mesa Gobierno Corporativo y Gestión de Riesgos

## Alcance de la Mesa.

Sistemas Alternativos de Transacción y Plataformas de Financiamiento Colectivo de la Ley N° 21.521.

## Definiciones.

**Sistema Alternativo de Transacción (SAT):** lugar físico o virtual que permite a sus participantes cotizar, ofrecer o transar instrumentos financieros o valores de oferta pública, y que no está autorizado para actuar como bolsa de valores de acuerdo con la Ley N° 18.045 o como bolsa de productos de acuerdo con la Ley N°19.220.

*Esta definición solo aplica en el caso en que el sistema "junte puntas" de compra y venta de terceros. Cuando la empresa toma una de las puntas, este servicio deberá considerarse como intermediario de instrumentos financieros.*

**Plataforma de Financiamiento Colectivo:** lugar físico o virtual por medio del cual quienes tienen proyectos de inversión o necesidades de financiamiento difunden, comunican, ofertan o promocionan esos proyectos o necesidades, o las características de éstos, y se contactan u obtienen información de contacto de quienes cuentan con recursos disponibles o la intención de participar en esos proyectos o necesidades o satisfacerlos; a fin de facilitar la materialización de la operación de financiamiento.

*Esta definición se circunscribe a entidades que facilitan el cierre de negocios, pero no aquellas donde éstos tienen lugar. En este último caso, la plataforma deberá inscribirse como SAT.*

## Propuesta de Norma de Gobierno Corporativo y Gestión Integral de Riesgos

El desarrollo de las actividades de sistemas alternativos de transacción y plataformas de financiamiento colectivo llevan a las entidades que prestan dichos servicios a asumir distintos riesgos, los que pueden llegar a afectar el patrimonio de sus clientes.

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, que se puede resumir en los lineamientos expuestos a continuación.

## **1. Alta administración (o 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; prevención del lavado de activos y financiamiento del terrorismo, incluyendo operaciones transfronterizas, conservación y manejo de información confidencial, divulgación de información veraz y oportuna en el interés de los clientes y otras partes interesadas, idoneidad y conocimientos del personal de la entidad, procedimientos de selección de instrumentos a los oferentes, contratación del personal y cumplimiento regulatorio.

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 otra estructura acorde que permite una gestión eficiente de la organización. Sin perjuicio de ello, deberá contar con un comité o encargado de gestión de riesgo integrado al menos por un miembro de la alta administración.
- Aprobar los niveles de tolerancia a los riesgos identificados.
- Aprobar y monitorear el cumplimiento de planes 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 un mecanismo efectivo para la recepción, gestión y resolución de reclamos internos o 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 servicios. La entidad debe procurar que los servicios ofrecidos al cliente sean entendidos por él, incluidos los riesgos derivados.

## **2. Políticas, procedimientos y controles de riesgos.**

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

- Integridad de las prácticas de la entidad en materia de transacción de instrumentos financieros y oferta de proyectos de inversión, que garanticen que las transacciones se realicen en el interés y la protección de sus clientes, en forma transparente y considerando todos

los riesgos asociados a cada tipo de instrumento o proyecto, y privilegiando el acceso directo a la negociación.

- Gestión de conductas de abuso de mercado, incluyendo el manejo de información privilegiada y distorsión del mecanismo de fijación de precios.
- Políticas de aceptación de proyectos de inversión, clientes e instrumentos en sus plataformas (incluyendo la publicación de prospectos o "libros blancos").
- 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.
- 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 de remuneraciones de la entidad y en los contratos de prestación de servicios. Dicha política deberá ser divulgada en el sitio web del prestador en un lugar de fácil acceso, con un nivel de detalle que permita a cada cliente tomar una decisión informada respecto de los potenciales conflictos para los servicios ofrecidos.
- Protección de los activos financieros y de información, tanto de la entidad como de sus clientes.
- Sistemas que permitan el mantenimiento apropiado de registros exigidos por la normativa vigente, considerando la integridad, disponibilidad y confiabilidad de la información.
- Segregación apropiada de los deberes y de las funciones claves.
- Políticas y procedimientos para la continuidad operacional de la entidad.
- Procedimientos de control para el cumplimiento de leyes y normativas aplicables a la entidad, incluyendo la prevención del lavado de activos y financiamiento del terrorismo entre otros.

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 due diligence e información continua de proyectos, acceso a negociación, formación de precios y manejo de incumplimientos de contraparte establecidos en la normativa de Autorización de Plataformas de Financiamiento Colectivo y Sistemas Alternativos de Transacción que debe dictar esta Comisión.

### **3. 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 (financieros, operacionales, mercado, legal, conducta, reputacional, según corresponda)
- Establece una metodología para la medición, control y monitoreo de riesgos, la que debiera incluir un mapeo de los distintos procesos del negocio, determinación de los riesgos de cada proceso, medición de exposición a dichos riesgos y establecimiento de controles mitigantes.
- 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 y niveles de exposición al riesgo de la entidad.
- Reevalúa los riesgos ante distintos escenarios, por ejemplo:
  - a. Cambios en condiciones del entorno económico y mercados en que opera la entidad.
  - 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 la alta administración y otras instancias responsables.

### **4. 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.
- 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 para monitorear la oportuna corrección de las observaciones por deficiencias en la gestión de riesgos.

## GESTIÓN DE RIESGO OPERACIONAL

La gestión de riesgo operacional de los servicios de SAT y plataforma de financiamiento incluida en la norma de gestión de riesgo operacional de entidades de valores<sup>1</sup>.

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, de manera que sea consciente de los riesgos de seguridad de la información y ciberseguridad y contribuya a su adecuada gestión.
- Clasificar los activos de información e implementar un inventario, 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.
- Contar con herramientas de registro y control de actividad de usuarios de sistemas.
- Implementar controles que permitan mitigar los riesgos en el uso de dispositivos móviles y del acceso remoto realizado por el personal.
- Gestionar las condiciones para la localización segura para los equipos.
- Contar con procedimientos de respuesta y recuperación ante incidentes, que consideren la recuperación oportuna de las funciones críticas, los procesos de respaldo y soporte, los 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, 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 normas y procedimientos que establecen la información que requiere ser protegida a través de técnicas de cifrado, entre otras.

---

<sup>1</sup> Se encuentra en proceso de publicación por la CMF.

- 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.
- Procedimientos de gestión de capacidad para la prestación continua del servicio a través de sus plataformas, incluyendo la disponibilidad de un sitio secundario y el uso de indicadores de provisión del servicio.
- 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). En términos globales, deberá existir un *uptime* de la provisión de servicios (establecido por producto por la entidad), el que no podrá ser 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.
- Los Sistemas Alternativos de Transacción (SAT) deberán disponer de sistemas que permitan:
  - a. Rechazar ordenes de negociación que excedan umbrales predefinidos de precio y cantidad que pudieran ser erróneos.
  - b. El acceso de forma periódica por parte de los clientes a la información de precios, volumen, profundidad de mercado, y hora de las ordenes transadas en el SAT a lo largo del ciclo de negociación diario.
  - c. Tener capacidad suficiente para garantizar una negociación ordenada en condiciones de fuerte tensión en el mercado.
  - d. Que las transacciones sean realizadas a los precios informados al cliente al momento de su ejecución.

## **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.
- Contar con un registro de servicios externalizados, incluidos los servicios en cadena.
- Monitorear periódicamente que los proveedores cumplan con las condiciones pactadas.

#### **4. Información de incidentes y pérdidas operacionales.**

- Deber de 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.
- Elaborar un informe interno con investigación y análisis de incidentes críticos.
- También deberán ser reportadas semestralmente las pérdidas operacionales materializadas por encima de 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?
- ¿Prestan servicios adicionales en conjunto con plataformas de financiamiento colectivo y/o SAT de forma regular?
- ¿Qué interrelación y/o dependencia tienen con las entidades fiscalizadas por la CMF?