Gestión de Riesgo Operacional - Lineamientos

1. Introducción

El propósito de ComDer es asumir el doble rol de a) Operador del Sistema de Contraparte Central (SCC) y b) de una Entidad de Contraparte Central (ECC).

Las contrapartes de la ECC son los denominados Participantes Directos, quienes adhieren a las Normas de funcionamiento de Comder, a través de la suscripción de un Contrato de servicio.

Rol como Operador del Sistema de Contraparte Central (SCC)

El propósito en su rol de operador del SCC es reducir y gestionar los riesgos generales del negocio, los riesgos operacionales, de custodia e inversión, legales, de cumplimiento, reputacionales y el riesgo sistémico que ComDer podría provocar en el sistema financiero chileno, en el caso que interrumpiera sus servicios.

Estos riesgos se refieren a los riesgos y pérdidas potenciales que surgen de la administración y operación como empresa, que no están relacionados con el incumplimiento de un Participante ni con los recursos financieros destinados a mitigar los riesgos de su rol de Entidad de Contraparte Central.

Los riesgos generales del negocio tienen que ver con cualquier deficiencia potencial de su posición financiera como consecuencia del incremento de sus gastos operacionales o reducción de sus ingresos. Lo que incluye los riesgos de la información que provee especialmente en sus informes financieros (balances, estados de resultados, etc.) e informes de gestión de riesgos.

Los riesgos operacionales, que son propios en la operación de servicios altamente automatizados como es el caso de ComDer, son los riesgos de seguridad de la información / ciber seguridad, continuidad de negocios, fraude, calidad y ciber riesgos.

Los riesgos de custodia e inversión se refieren al riesgo financiero de las inversiones propias de ComDer y donde se custodian.

El riesgo legal comprende los cambios en la legislación que afecten adversamente la posición de la compañía.

El riesgo de cumplimiento se refiere a las pérdidas debido al incumplimiento de la legislación o normativa vigente.

El riesgo reputacional refiere al peligro de que, por causa de algún evento interno o externo, una opinión pública negativa impida o disminuya la capacidad de la compañía para hacer negocios.

Por todo lo anterior, ComDer debe contar con sistemas de gestión y de control interno robustos para identificar, analizar, evaluar, mitigar, monitorear y comunicar estos riesgos.

Rol como una Entidad de Contraparte Central (ECC)

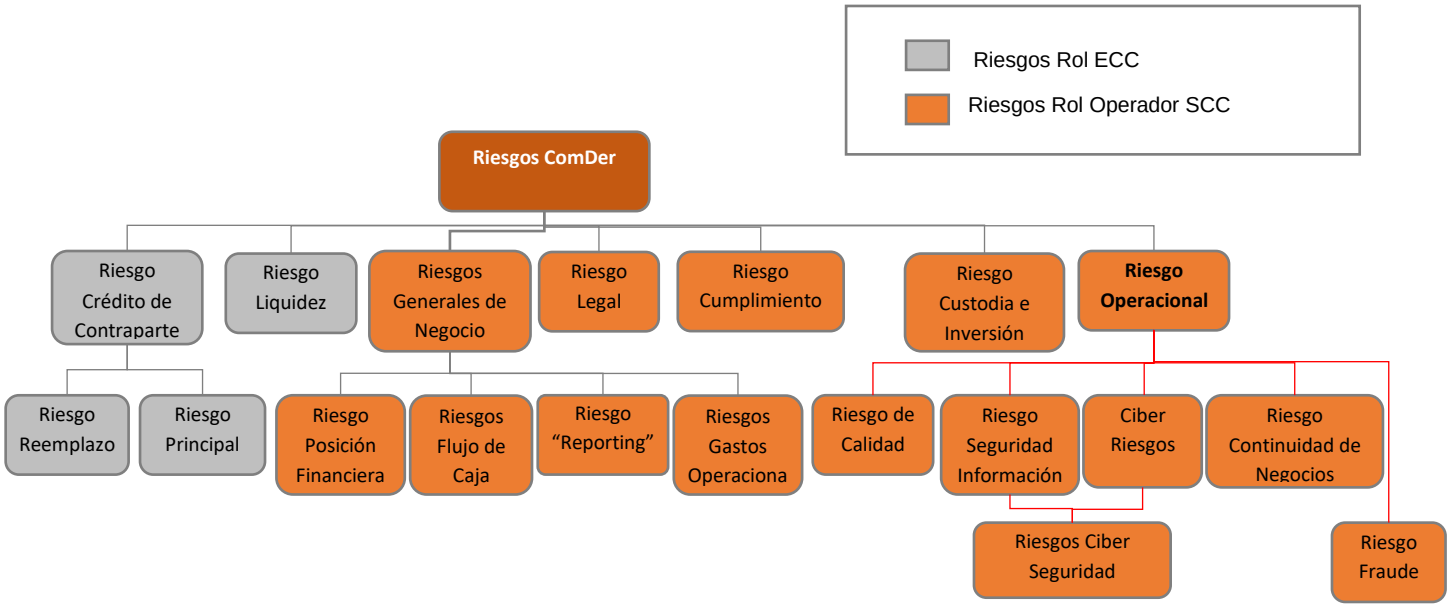
El propósito en su rol como ECC, es reducir y gestionar el riesgo de contraparte en el mercado financiero, previniendo la acumulación de una red de exposiciones entre Participantes del mercado bilateral (Riesgo Sistémico, contagio) y asegurando que, si un Participante Directo de la ECC falla o incumple, las otras contrapartes son protegidas por un procedimiento de gestión de incumplimiento previamente establecido, permitiendo al mercado continuar su operación.

Un Participante que compensa y liquida sus transacciones financieras en una ECC, sustituye sus numerosas exposiciones bilaterales por una única exposición neta con la ECC, debido a que la ECC se constituye en acreedora y deudora de los derechos y obligaciones que provengan de tales transacciones.

Las ECC realizan la mitigación del riesgo de contraparte a través de herramientas robustas de gestión de riesgos de contraparte, tales como, compensación multilateral, exigencia de garantías, liquidación diaria del margen de variación y un conjunto de reglas legales y operacionales pre acordadas (Normas de Funcionamiento) en caso que una contraparte incumpla.

Además, en este rol se debe mitigar el riesgo de liquidez que se puede ver enfrentada la ECC, en caso de un Evento de Retardo de un Participante (no pago oportuno de su Margen de Variación).

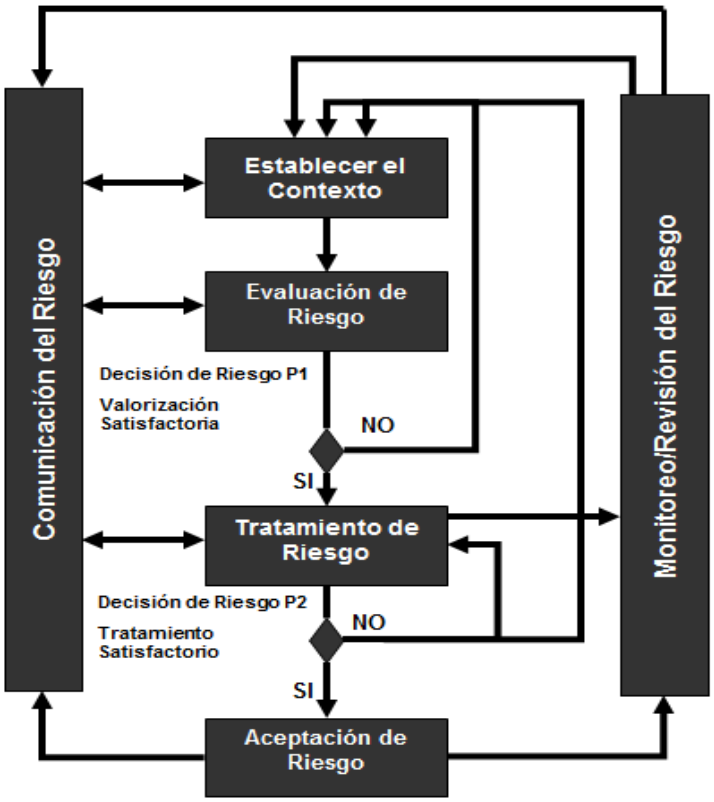
Der acuerdo a lo anterior, se ha establecido el siguiente Mapa de Riesgos para Comder Central de Contraparte SA.



2. Gestión de Riesgo Operacional

Para llevar a cabo una adecuada gestión de Riesgos, ComDer ha adoptado el estándar ISO31000:2009 "Risk Management - Principles and Guidelines" como estructura para todas las categorías de riesgos declarados en el Mapa de Riesgos. En particular, la categoría Riesgo Operacional, se encuentra en el ámbito de ComDer en su rol de Operador del Sistema de Contraparte Central.

La estructura definida para la gestión de todos los riesgos y por ende del riesgo operacional se muestra en la figura siguiente.



2.1 Definiciones

Riesgo Operacional:
ComDer hace suya la definición de Riesgo Operacional de CPMI-IOSCO, que lo define como: "el riesgo que las deficiencias en los sistemas de información, los procesos internos y el personal, o las alteraciones provocadas por acontecimientos externos deriven en la **reducción, el deterioro o la interrupción** de los servicios prestados por una Infraestructura de Mercado Financiero (IMF)".

De la misma forma, también toma en consideración la definición de Riesgo Operacional de la SVS, que lo define como: "el riesgo de **pérdida** debido a la inadecuación o a la falla de los procesos, del

personal y de los sistemas internos y/o controles internos aplicables, o bien a la causa de acontecimientos externos".

Las fallas Operacionales pueden dañar la reputación o confiabilidad percibida, traer consecuencias legales y resultar en pérdidas financieras incurridas por la IMFs, los participantes y otras partes.

De acuerdo a las definiciones anteriores y tomando en consideración la categorización de la "ERM Wheel" del GARP, los tipos de riesgos que se incluyen en la categoría riesgo operacional son:

- Riesgo de Continuidad de Negocios
- Riesgo de Seguridad de la Información
- Riesgo de Calidad
- Riesgo de Fraude
- Riesgo de Ciberseguridad
- Ciber Riesgos

Apetito por Riesgo:
El apetito por riesgo se define como la cuantía y tipología (clasificación) de los riesgos que se considera razonable asumir en la ejecución de la estrategia del negocio.

2.2 Objetivos en la Gestión de Riesgo Operacional.

El objetivo de la gestión del riesgo operacional es identificar, evaluar, controlar y mitigar el riesgo operacional dentro de ComDer e implementar un framework basado en el estándar ISO 31000 en toda la Organización, con el objetivo de asegurar la consistencia y completitud en su aplicación.

El Riesgo Operacional es parte importante del universo de gestión de riesgos de ComDer, el cual se gestiona en el Sistema Gestión Integral – Riesgos SGI-R.

2.3 Directrices en la Gestión de Riesgo Operacional.

1. ComDer cualitativamente tiene un bajo apetito al riesgo operacional, por ende, tiene una baja tolerancia a las interrupciones y deterioro del servicio, y a las pérdidas ocasionadas por ellas. Por lo anterior, evitará cuando sea posible los riesgos que afecten la entrega de sus servicios, o en su defecto, tomará las acciones de control apropiadas para reducirlos o compartirlos.

2. Los procesos de gestión de Riesgo Operacional, que forman parte del framework son: Establecer el Contexto, Valorización del Riesgo, Tratamiento de Riesgos, Aceptación del Riesgo y Monitoreo/Revisión del Riesgos. Estos procesos de gestión serán auditados periódicamente y por un ente independiente a Operaciones y TI.

3. El Comité de Gestión Operacional del Sistema de Contraparte Central (SCC), aprueba la evaluación del riesgo inherente en todos los servicios y procesos de negocios. Además, asegura que se mantengan actualizado el inventario de eventos y los mapas de riesgos de riesgo operacional, que se confeccionaran teniendo en cuenta el impacto y probabilidad de ocurrencia del evento de riesgo.

4. Los planes de tratamiento de los riesgos Operacionales deberán ser revisados y aprobados al menos una vez al año por el Comité de Gestión Operacional del SCC. Al igual que los planes de contingencia TIC y de continuidad de negocios, los que además deberán ser probados periódicamente.

5. Las Actividades de Control (políticas, procedimientos y controles) deben estar orientados a reducir o mitigar los riesgos identificados y a prevenir, detectar y corregir las fallas o problemas que puedan surgir.

6. De la Política General de Riesgo Operacional, se desprende un conjunto de Políticas Específicas en los ámbitos de la gestión del riesgo operacional, la seguridad de la información, continuidad del negocio, calidad de los procesos, outsourcing y recursos humanos.

7. El diseño organizacional (funciones y procesos) debe asegurar la segregación de funciones. Por lo tanto, no se asignarán a una misma persona funciones con intereses contrapuestos y ningún proceso de ComDer podrá ser ejecutado sólo por una persona, debiendo intervenir como mínimo dos.

8. ComDer declara su decisión de cumplir con la normativa y legislación vigente de los Organismos Reguladores y Fiscalizadores, relacionadas con el riesgo operacional, outsourcing, continuidad del negocio y seguridad de la información.

9. Los Riesgos relacionados a fallas en componentes tecnológicos como hardware, configuración base, y redes se monitorean en forma automática. Los riesgos relacionados a los ámbitos de procesos se monitorean mediante indicadores de riesgo y los riesgos de recursos humanos a través de controles independientes que aseguren la segregación de funciones y la adherencia a las actividades de control implementadas.

10. Para la cuantificación del impacto de las perdidas asociadas al riesgo operacional y así realizar prudencialmente las mitigaciones necesarias, se adoptará preferentemente la metodología Factor Análisis for Information Risk (FAIR).

2.4 Criterios de Evaluación y Tratamiento de riesgo

Análisis de Riesgos

ComDer utiliza una metodología de análisis semi cuantitativa en la cual se le asignan valores a la probabilidad de ocurrencia y al impacto del riesgo de acuerdo Criterios de Probabilidad de Ocurrencia y Criterios de Impacto.

En la valoración de los riesgos, se utiliza como base una Matriz General de 5 x 5 y la fórmula Clasificación de Riesgo= nivel de probabilidad + nivel de impacto -1.

Los criterios de probabilidad e impacto son válidos para las categorías de los riesgos de ComDer en su rol de operador de la Entidad de Contraparte Central, entre los que se encuentran los tipos de Riesgo Operacional (Riesgo de Continuidad de Negocios, Riesgo de Seguridad de la Información, Fraude y Riesgo de Calidad).

Evaluación de Riesgo

Se evalúa el riesgo estimado y clasificado comparándolo con el siguiente criterio de aceptación del riesgo:

1. La aceptación de riesgos en cada categoría se lleva a cabo de acuerdo a las estrategias de mitigación para cada una de ellas.
2. En general en ComDer se aceptan riesgos de nivel 3 e inferior de la Matriz de General de Clasificación de Riesgo Impacto-Probabilidad (descrita arriba)

Tratamiento de Riesgos

En caso de que el nivel del riesgo estimado sea mayor al nivel de aceptación del mismo, se debe tomar la primera decisión de riesgos, que consiste en elegir una opción de tratamiento de riesgos.

Las opciones de tratamiento de riesgos son:

1. Reducción o mitigación del riesgo
2. Retención del riesgo
3. Evitar el riesgo
4. Transferir el riesgo

Todos los riesgos con clasificación de alto impacto y alta probabilidad de ocurrencia, deben contar con respuestas al riesgo y, en caso de asumir el riesgo, se debe contar con acciones mitigadoras explícitas que reduzcan el riesgo residual lo más posible. Esta misma definición aplica para los riesgos con alto impacto y baja probabilidad de ocurrencia, los que deben además contar con el respectivo Plan de Contingencia en caso de ocurrir.

Si se escoge como opción reducir o mitigar el riesgo, se debe confeccionar un Plan de Tratamiento de Riesgos (PTR) para cada categoría de riesgos.

El PTR del Riesgo Operacional es el agregado de los riesgos relacionados a los sistemas (tecnología), procesos, persona y eventos externos que pueden producir una falla o interrupción de los servicios de ComDer, riesgos que son tratados en las categorías de Seguridad de la Información, Fraude, Continuidad y Calidad.

El PTR se debe confeccionar:

1. Seleccionando los controles específicos ejecutados en los procesos, que mitiguen los riesgos identificados.
2. Estimando en cuánto se disminuye la probabilidad y el impacto del riesgo con la acción de los controles seleccionados, de manera de reducir el riesgo a los niveles de aceptación.
3. Si los controles ya establecidos no son suficientes, se deben crear controles adicionales que aseguren el nivel de aceptación.
4. Finalmente, se monitorea la ejecución de los controles en la frecuencia definida para prevenir los riesgos.

Una vez confeccionados los PTR éstos deben obtener su aprobación por parte del Comité de Riesgo No Financiero, el cual aceptará o rechazará, los riesgos residuales propuestos.

Una vez elegida la opción de tratamiento de riesgos se debe tomar la segunda decisión de riesgos, que es aceptar o no el riesgo después de realizado su tratamiento.

Las estrategias de tratamiento de riesgos son propias de cada categoría de riesgos, así las estrategias de tratamiento de los riesgos de Seguridad de la información son distintas a las estrategias de Continuidad de Negocios, Cumplimiento, etc.

Gerencia General

ComDer Contraparte Central S.A.