1. Introducción

El propósito de ComDer es asegurar el cumplimiento de las obligaciones de los Participantes que operan en la Entidad de Contraparte Central regida por la Ley 22.345. Para ello, ComDer asume un 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)

Los objetivos de este rol son operar el SCC de acuerdo a la regulación vigente y bajo altos estándares de calidad, seguridad, ciber seguridad y continuidad de negocio. Para ello, debe gestionar y mitigar los riesgos generales del negocio, los riesgos operacionales, de custodia e inversión, legales, de cumplimiento, reputacionales y reducir el riesgo sistémico que el Operador del SCC podría provocar en el sistema financiero chileno, en el caso que interrumpiera sus servicios.

Estos riesgos se refieren a las pérdidas potenciales que surgen de la administración y operación del SCC, conocidas internacionalmente como Non Default Losses (NDL), las cuales no están relacionadas con el incumplimiento de un Participante (Default Losses, DL) ni con los recursos financieros destinados a garantizar las obligaciones de los Participantes 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. Dentro de este grupo también se encuentran los riesgos TI, que corresponden a aquellos asociados con el uso, propiedad, operación, involucramiento, influencia y adopción de TIC dentro de una empresa.

Los riesgos operacionales, que son propios en la operación de servicios altamente automatizados como es el caso de ComDer, son tipificados en 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 objetivo de este Rol es asegurar el cumplimiento de las obligaciones de los Participantes, utilizando todas las herramientas que provee la Gestión de Riesgos de Crédito de Contraparte y Liquidez.

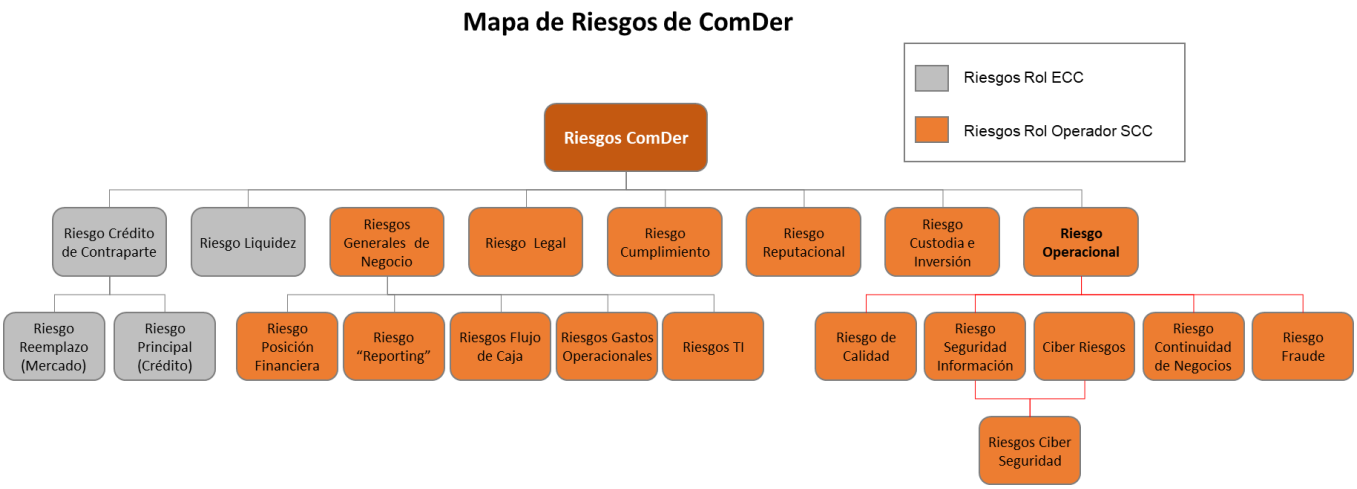
Para lograr su objetivo, la ECC debe reducir y gestionar el riesgo de contraparte en el mercado financiero, previniendo la acumulación de una red de exposiciones entre Participantes del mercado bilateral (Riesgo Sistémico, contagio) y asegurando que, si una contraparte de la ECC falla o incumple, las otras contrapartes son protegidas por un procedimiento de gestión de incumplimiento previamente establecido, que dispone de las garantías entregadas por los Participantes a través de los Márgenes Iniciales y Márgenes de Variación enterados en la operación diaria de la cámara, permitiendo la continuación de 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) para enfrentar la eventualidad 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 (pago en forma no oportuna 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, la organización adopta un enfoque por niveles propuesto por NIST 800-39. El enfoque tiene como objetivo integrar de manera más eficiente los riesgos en toda la organización para así mejorar la comunicación de los riesgos.

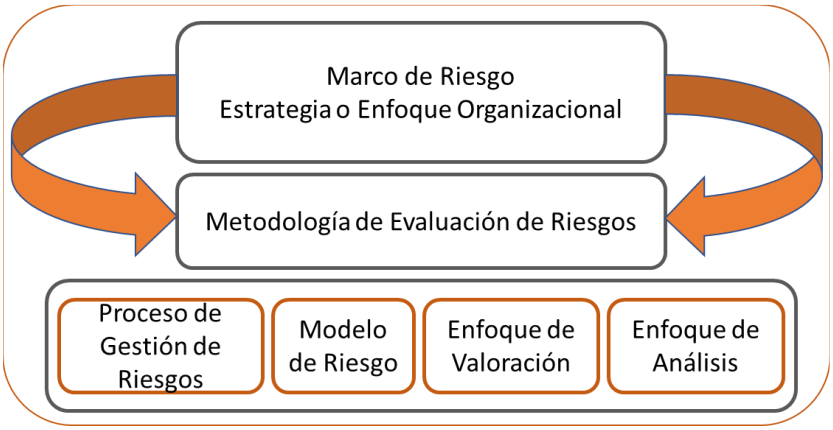
Nivel 1 – Organizacional/Ejecutivo: Aborda el riesgo desde una perspectiva de activos organizacionales. El Nivel 1 implementa el primer componente de la gestión de riesgos (es decir, el marco de riesgos), proporcionando el contexto para todas las actividades de gestión de riesgos realizadas. El Nivel 1 es el que comunica las prioridades de la misión, estrategia de riesgo, los recursos disponibles, apetito y la tolerancia al riesgo general al Nivel 2.

Nivel 2 – Misión/Procesos: Aborda el riesgo desde una perspectiva de proceso de negocio y está informado por el contexto de riesgo, las decisiones de riesgo y las actividades de riesgo en el Nivel 1. El Nivel 2 utiliza la información como entradas en el proceso de gestión de riesgos, y luego colabora con el Nivel 3 de implementación u operaciones para comunicar las necesidades del negocio y crear un Perfil de riesgo. Mediante este nivel se determina el RTO y la tolerancia de impacto de los procesos de negocio.

Nivel 3 - Sistemas de Información/Operacional: Aborda el riesgo desde la perspectiva del sistema de información o componentes del proceso, y se guía por el contexto de riesgo, las decisiones de riesgo y las actividades de riesgo en los Niveles 1 y 2. El Nivel 3 comunica el progreso de la implementación, el estado de la infraestructura, estado de controles y el Perfil de riesgo al nivel empresarial o de proceso.

La relación entre el Nivel 2 (Procesos de Negocio) y Nivel 3 se realiza por medio del BIA.

Adicionalmente, ComDer ha decidido adoptar la propuesta metodológica del estándar NIST 800-30 Guide for Conducting Risk Assessments, para complementar las normas ISO. En esta metodología se establecen cuatro componentes esenciales para la gestión de riesgos, que se conforman en base a un enfoque organizacional.



Los componentes de la metodología de evaluación de riesgos son los siguientes:

Procesos de gestión de riesgos: Establecen las actividades necesarias para enmarcar el riesgo dentro del contexto de la organización, evaluar el riesgo, responder al riesgo, y realizar seguimiento del riesgo.

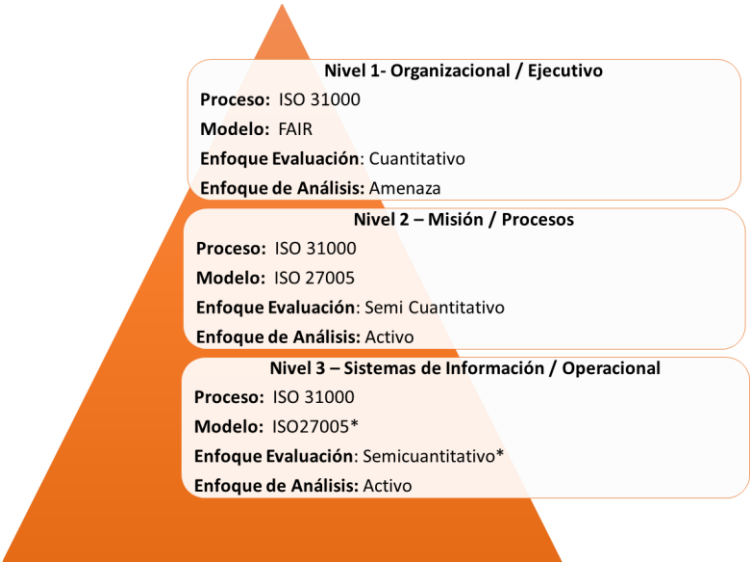
Modelo de riesgo: Definen los factores de riesgo a ser evaluados y las relaciones entre esos factores. Los factores de riesgo son características utilizadas en los modelos de riesgo como insumos para determinar los niveles de riesgo en las evaluaciones de riesgos. La organización ha adoptado dos modelos de riesgo, el primero se encuentra basado en la ISO 27005, considerando directamente los factores de impacto y probabilidad, también adoptará el modelo propuesto por FAIR o Factor Analysis of Information Risk, una metodología de medición cuantitativa del riesgo en el cual el impacto y probabilidad se puede definir en doce factores.

Enfoque de valoración: Los factores de riesgo definidos en el modelo de riesgo se pueden valorizar de varias maneras, que incluyen cuantitativa, cualitativa o semicuantitativa. La organización ha adoptado un enfoque de valoración cuantitativo y semicuantitativo, dependiendo del nivel de activo que se evalúe.

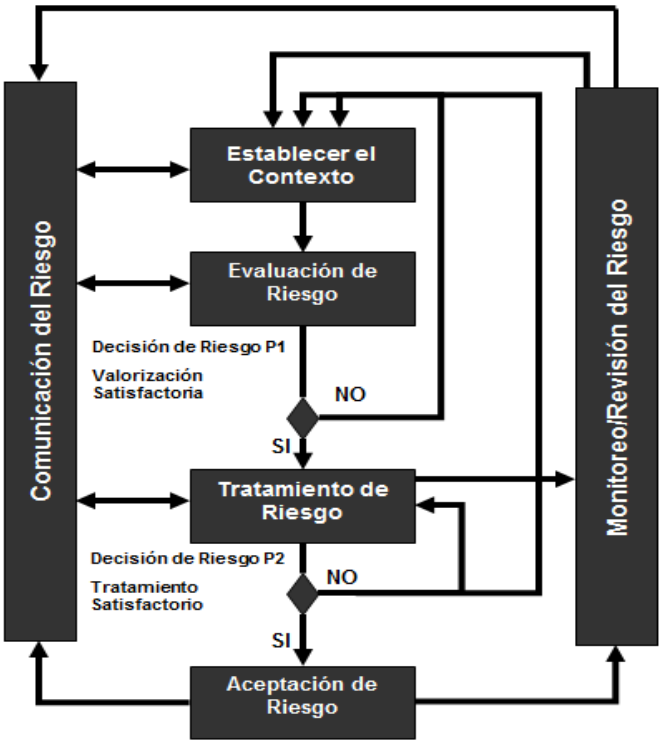
Enfoque de análisis: Se refieren al punto de partida de la identificación de riesgos, donde los enfoques pueden ser orientados a amenazas, a activos u orientado a la vulnerabilidad. La

organización ha adoptado dos enfoques de análisis, un enfoque en la amenaza y un enfoque en el activo, lo anterior dependiendo del nivel de activos que se evalúe.

Dependiendo del tipo y nivel del activo cuyo riesgo se quiere gestionar, se ha adoptado una metodología distinta. Por lo anterior se han definido las siguientes metodologías por cada nivel:



Los procesos de gestión de riesgos adoptados por la Organización, como parte de las normas ISO 31000:2009 e ISO 27005:2011, y que se encuentran integrados en la gestión integral de la Organización, se muestran en la siguiente figura:



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 CMF, 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 (FAIR):

Es el nivel de exposición de pérdidas que una organización ve como aceptable de asumir, dado los objetivos estratégicos del negocio y sus recursos.

Tolerancia al Riesgo (FAIR):

Es el grado de varianza del apetito al riesgo de la organización que la organización está dispuesta a tolerar.

Riesgo Aceptado:

Es el criterio de aceptación (semi cuantitativo o cuantitativo) que fija un nivel sobre el cual, en general, no se requieren más acciones de mitigación.

2.2 Objetivos en la Gestión de Riesgo Operacional.

El objetivo de la gestión de riesgo es poder definir las actividades que permitan identificar riesgos, para poder evaluarlos y tomar decisiones, con foco en el apetito por riesgo y riesgo aceptado definidos de forma estratégica por la Organización.

El objetivo de la Gestión de Riesgo Operacional y Operador es asegurar que la exposición al riesgo permanece dentro del apetito de riesgo definido por la organización.

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 (mitigarlos) o compartirlos. ComDer establecerá el nivel cuantitativo de riesgo aceptado y de tolerancia de acuerdo con lo aprobado por el Comité de Riesgo Operacional.

2. Para llevar a cabo una adecuada gestión de los Riesgos Operacionales, La Organización adoptará el estándar ISO 31000:2009 Risk Management - Principles and Guidelines como framework, que le permitirá la gestión de sus distintos tipos de riesgos, y cumplir con lo estipulado en la normativa de la CMF. Además, se realizará una gestión de riesgos por niveles basados en el estándar NIST 800-30, con la finalidad de integrar la gestión de riesgos en la organización.

3. Las actividades de gestión de Riesgo Operacional, que forman parte del Proceso de Gestión de Riesgo son: Establecer el Contexto, Valorización del Riesgo, Tratamiento de Riesgos, Aceptación del Riesgo y Monitoreo/Revisión del Riesgos. Este proceso de gestión será realizado al menos anualmente y auditado periódicamente por un ente independiente a Operaciones y TI.

4. El Comité de Gestión Operacional (conformado por la Alta Administración de ComDer) evaluará el riesgo inherente en todos los servicios y procesos de negocios. Además, mantendrá 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.

5. Los planes de tratamiento de los riesgos Operacionales deberán ser revisados y aprobados al menos una vez al año por el Comité de Riesgo Operacional (conformado por tres miembros, dos de ellos elegidos por los Participantes Directos y un miembro designado por el Directorio de ComDer), o en su defecto por el Directorio. Mientras que los planes de contingencia TIC y de continuidad de negocios deberán ser probados periódicamente y aprobados por el Comité de Gestión Operacional.

6. 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.

7. De la Política General de Riesgo Operacional, se desprende un conjunto de políticas específicas/propias de los ámbitos de la gestión del riesgo operacional, la seguridad de la información, continuidad del negocio, calidad de los procesos, fraude y ciber riesgo.

8. 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.

9. 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.

10. Los Riesgos relacionados a fallas en componentes tecnológicos como hardware, configuración base, aplicaciones 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.

11. La Organización promoverá una cultura de riesgos en materia de riesgos operacionales, lo que incluye a los riesgos de Seguridad de la Información / Ciberseguridad, continuidad de negocios, ciber riesgos, calidad y fraudes, dando especial atención a los procesos de gestión de toma de conciencia de los respectivos sistemas de gestión.

12. 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 Analysis of Information Risk (FAIR).

2.4 Criterios de Evaluación y Tratamiento de riesgo

Análisis de Riesgos

ComDer utiliza una metodología de análisis cuantitativa para los activos nivel 1 y una semi cuantitativa para los niveles 2 y 3.

En el caso de la metodología cuantitativa se utilizará la metodología FAIR, para lo cual se debe definir las variables a utilizar dentro de los doce factores del árbol FAIR (de acuerdo a la información que se tenga disponible para la realización del análisis), las que posteriormente deben ser valoradas a través de una simulación, a partir de la cual se obtiene la pérdida esperada.

En el caso de la metodología semi cuantitativa, se 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 se compara los resultados con los criterios de aceptación de riesgo:

- Nivel 1: Se realiza en base al riesgo cuantificado y agregado comparado con el definido por la organización como riesgo aceptado.

- Nivel 2 y 3: Nivel 3 o inferior de la matriz de Clasificación de Riesgo Impacto-Probabilidad.

El riesgo aceptado por la Organización corresponde al 30% del Capital Regulatorio requerido por los PFMI asociado a gastos operacionales.

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. Compartir o transferir el riesgo

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

La opción de retención se tomará cada vez que el nivel de riesgo inherente sea igual o inferior al nivel de riesgo aceptado. Para esta opción no es necesario incluir un Plan de Tratamiento de Riesgos.

En caso de que se opte por la opción de evitar o compartir el riesgo, se debe plantear la opción al Comité de Gestión Operacional, para que este determine si la opción puede ser realizada, o en su defecto determinar qué acciones deben ser realizadas.

El PTR del Riesgo Operacional es el agregado de los riesgos relacionados a los sistemas (tecnología), procesos, personas y eventos externos que pueden producir una falla o interrupción de los servicios de ComDer.

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. Finalmente, se monitorea la ejecución de los controles en la frecuencia definida para prevenir los riesgos.

Una vez confeccionados los PTR, los riesgos son evaluados nuevamente para obtener su evaluación residual, es decir, su riesgo remanente una vez aplicado su plan de tratamiento, y se vuelve a comparar con los criterios de aceptación definidos.

En este punto, se debe tomar la segunda decisión de riesgos, que es aceptar o no el riesgo después de realizado su tratamiento.

En caso que el nivel de riesgo residual sea superior a su nivel de aceptación se deben determinar nuevas opciones de Tratamiento del Riesgo, lo que involucra generar un plan de acción.

El análisis, evaluación y valoración de los riesgos, sus respectivos planes de tratamiento y planes de acción deben ser validados por el Comité de Gestión Operacional y posteriormente aprobado por el Comité de Riesgo Operacional.

Gerencia General

ComDer Contraparte Central S.A.