ComDer es una Entidad de Contraparte Central constituida de conformidad con la ley 20.345 y es filial de Servicios de Infraestructura de Mercado OTC S.A

Servicios de Infraestructura de Mercado OTC S.A., es una sociedad de apoyo al giro bancario, que tiene como principal activo su participación de un 99,92% de la propiedad de Comder Contraparte Central.

En línea con lo anterior, a fin de generar sinergias y con el objetivo de garantizar la integridad y consistencia de los lineamientos para elementos comunes, se ha establecido, que aquellas definiciones y/o actividades que consideren la gestión de recursos compartidos o materias comunes, podrán ser descritas bajo el término "Organización", cuyo alcance considere elementos tanto de Comder como de su matriz IMERC.

La presente política es aplicable a nivel de Organización

I.- PROPÓSITO GENERAL DE LA ORGANIZACIÓN

El propósito de la organización es asumir los roles de: a) Operador del Sistema de Contraparte Central (SCC) y de Entidad de Contraparte Central (ECC) con el vehículo legal Comder y b) Operador de Infraestructuras (tecnológicas) de Mercado con el vehículo legal IMERC.

a) Rol Operador, como Operador del Sistema de Contraparte Central (SCC) y Operador de Infraestructura (tecnológicas) de Mercado

   El propósito en este rol es reducir y gestionar los riesgos generales del negocio, los riesgos operacionales, de custodia e inversión, legales, de cumplimiento, reputacionales, y en consecuencia el riesgo sistémico que la Organización 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 Organización, 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. 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 la Organización, estos son tipificados en riesgos de seguridad de la información / ciber seguridad, continuidad de negocios, ciber riesgos, fraude y calidad.

Los riesgos de custodia e inversión se refieren al riesgo financiero de las inversiones propias de la Organización 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 se 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, la organización debe contar con sistemas de gestión y de control interno robusto para identificar, analizar, evaluar, mitigar, monitorear y comunicar estos riesgos.

b) 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 una contraparte 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.

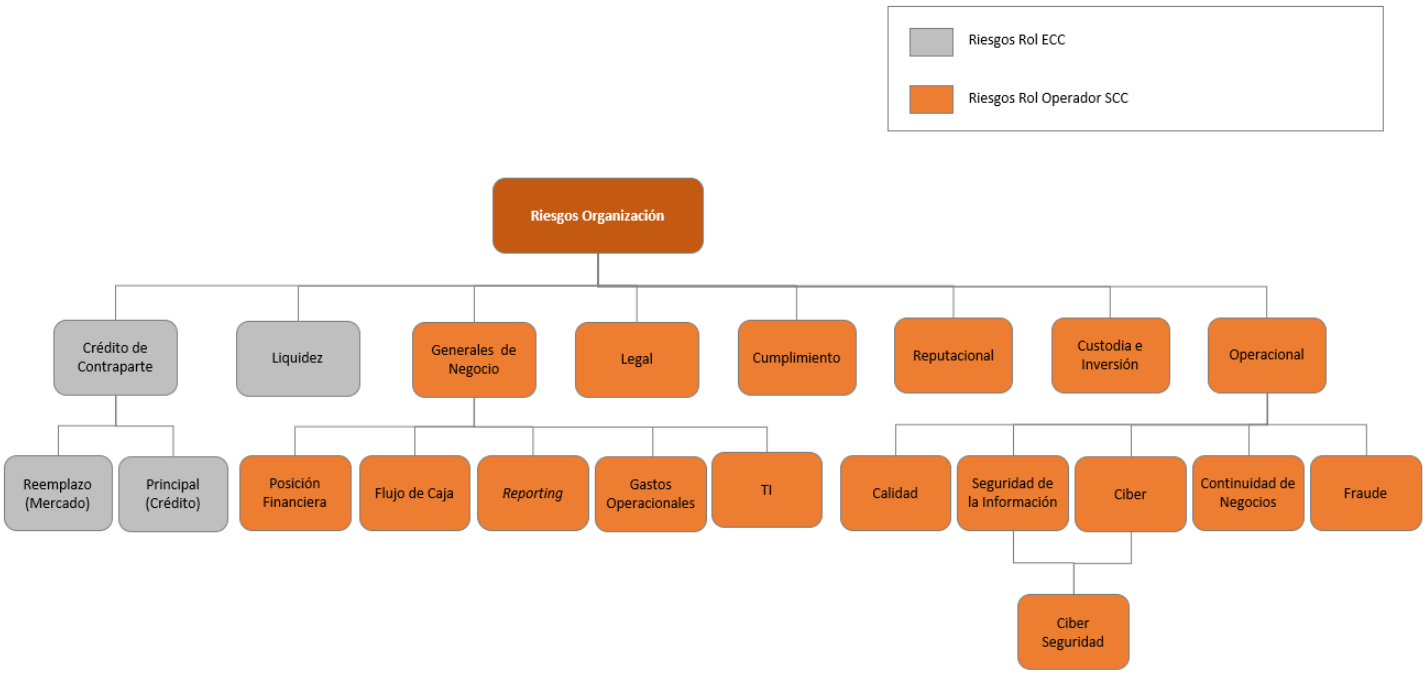
Un Participante que compensa y liquida sus transacciones financieras en una ECC, sustituye sus numerosas exposiciones bilaterales por una única exposición neta con la ECC, debido a que la ECC se constituye en acreedora y deudora de los derechos y obligaciones que provengan de tales transacciones.

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) para enfrentar la eventualidad de 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).

II.- ALCANCE

Esta Política General de Riesgos aplica a todas las actividades de la organización, y es el Marco General para la gestión de todos los tipos de riesgos que afectan a la Organización. Dichos riesgos son: Crédito de contraparte, Liquidez, Generales del Negocio, Legal, Cumplimiento, Reputacional, Operacional, Custodia, Inversión y, en consecuencia, sistémico por el incumplimiento de un participante y/o por incumplimiento propio. Lo anterior, se ve graficado en el siguiente mapa de riesgos.



III.- OBJETIVOS

El primer objetivo de esta Política es declarar las intenciones y orientaciones con respecto a la gestión de los riesgos a los cuales está expuesta la Organización, tanto en su rol de Operador del SCC e Infraestructura, como en su rol de Entidad de Contraparte Central.

El segundo objetivo es dar los lineamientos para el mantenimiento y desarrollo del sistema de gestión de Riesgo que la organización ha implementado en toda la Organización y como componente de su Sistema de Gestión Integral (SGI).

IV.- DEFINICIONES

Riesgo (Definición general)
La probable frecuencia y magnitud de una pérdida futura esperada e inesperada.

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

La Organización hace suya la clasificación y definiciones de Riesgo de CPMI-IOSCO.

Riesgo sistémico ECC (contagio)*: El riesgo sistémico de una Entidad Central de Contraparte (contagio) es que la incapacidad de uno o más participantes para cumplir sus obligaciones conforme a lo previsto, implique que otros participantes tampoco sean capaces de cumplir sus obligaciones cuando venzan.
*Riesgo Gestionado por la autoridad monetaria (BCCh).

Riesgo sistémico Operador SCC: El riesgo sistémico de un Operador que opera y administra el SCC, es que interrumpa sus servicios y no sea capaz de continuar su operación, provocando que uno o más de los participantes tampoco sean capaces de cumplir sus obligaciones cuando venzan.

Riesgo de crédito: El riesgo de que una contraparte, ya sea un participante u otra entidad, no pueda cumplir íntegramente sus obligaciones financieras cuando estas venzan o en cualquier momento del futuro.

Riesgo de liquidez: El riesgo de que una contraparte, ya sea un participante u otra entidad, no disponga de fondos suficientes para cumplir sus obligaciones financieras cuando estas venzan, aunque pueda hacerlo en el futuro.

Riesgo general del negocio: El riesgo general de negocio hace referencia a los riesgos y pérdidas potenciales que se derivan de la administración y funcionamiento de una FMI. Así como también cualquier potencial deterioro de valor de la posición financiera (como empresa en funcionamiento) de una FMI como resultado de la caída de sus ingresos o del crecimiento de sus gastos, de tal manera que los gastos superen a los ingresos y deriven en una pérdida que deba ser cargada contra el capital.

Riesgo legal: El riesgo de aplicación imprevista de una ley o regulación, que normalmente deriva en una pérdida.
Riesgo operacional: El riesgo de que las deficiencias que puedan producirse en los sistemas de información o procesos internos, errores humanos, fallos de gestión o alteraciones provocadas por acontecimientos externos deriven en la reducción, deterioro o interrupción de los servicios prestados por la Organización.

Riesgo de custodia: El riesgo de pérdida con respecto a los activos mantenidos en custodia en caso de insolvencia, negligencia, fraude, mala administración o mantenimiento inadecuado de archivos de un custodio (o subcustodio).

Riesgo de inversión: El riesgo de inversión es el riesgo de pérdida al que se enfrenta la Organización cuando invierte sus propios recursos u otros recursos como las garantías depositadas por sus participantes en instrumentos con riesgos de mercado, de crédito y de liquidez.

Riesgo reputacional: El riesgo reputacional es el 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.

Riesgo de Cumplimiento: El riesgo de cumplimiento se define como la probabilidad de ocurrencia y el impacto económico del incumplimiento de las obligaciones legales y normativas de la organización.

Riesgo de Reporting: Es el riesgo de errores no intencionales en los estados financieros.

V.- APETITO POR RIESGO

La Organización declara tener la intención y el deber, de siempre poder cumplir las obligaciones que tiene con sus participantes, descritas en las Normas de Funcionamiento y contratos, y de esa forma, lograr uno de los objetivos principales, reducir el riesgo de contraparte (Rol ECC). Además, la Organización asume su condición de Infraestructura de Mercado Financiero y entiende la responsabilidad que una mala gestión de ésta puede contribuir a una crisis sistémica y agravarla si los riesgos no se gestionan adecuadamente.

La Organización ha definido su apetito por cada tipo de riesgo de acuerdo con el Mapa de Riesgos en las respectivas políticas generales de cada uno de ellos. En los casos en que Categorías o Tipos de Riesgos no tengan una Política General, como es el caso de los Riesgos Generales del Negocio (excepto Riesgo TI), Legal y Reputacional el apetito se definirá en este documento.

Para llevar a cabo los procesos anteriormente mencionados, la Organización se compromete a proveer los recursos humanos y tecnológicos necesarios para cubrir las necesidades de la gestión de riesgos de su responsabilidad.

VI.- REGLAS

1. Para llevar a cabo una adecuada gestión de Riesgos, la Organización adoptó el estándar ISO31000:2009 "Risk Management - Principles and Guidelines" como "framework" para todos los riesgos declarados en las secciones anteriores.

2. Los riesgos identificados como rol operador del SCC e Infraestructura, en el mapa de riesgo deben ser gestionados utilizando los procesos de gestión de Riesgo que forman parte del framework, estos son: Establecimiento del Contexto, Evaluación –que incluye la Identificación, Análisis, y Valoración del Riesgo-, Tratamiento de Riesgos, Aceptación del Riesgo, Monitoreo y Comunicación del Riesgo. Estos procesos de gestión serán auditados periódicamente y por un ente independiente.

3. En línea con el punto anterior, se establecerán para los riesgos del mapa de riesgos, los criterios de evaluación y tratamiento de riesgos, utilizando la metodología de evaluación de riesgos semi cuantitativa de los mapas de calor (criterios de Impacto y Probabilidad de Ocurrencia para cada tipo de riesgos, ver Anexo A de esta política), la cual se complementará con una metodología de evaluación de riesgos cuantitativa, utilizando preferentemente la metodología FAIR.

4. Las actividades asociadas a la administración del riesgo -políticas, procedimientos y controles- deben estar orientadas a reducir o mitigar los riesgos identificados y a prevenir, detectar y corregir las fallas o problemas que puedan surgir, las cuales deben ser revisadas al menos anualmente.

5. 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 gestión de riesgos podrá ser ejecutado sólo por una persona, debiendo intervenir como mínimo dos.

6. La organización declara su decisión de cumplir con la normativa y legislación vigente de los Organismos Reguladores y Fiscalizadores, relacionadas con los riesgos que ha declarado asumir.

7. De acuerdo con la definición de riesgo legal establecida por los PFMI, la Organización en su rol de ECC, considera que es un riesgo inherente al negocio, el cual es regido, en el caso de ComDer, por la Ley 20.345 y que cambios o la aplicación de dicha ley que perjudiquen a la Organización son de baja probabilidad de ocurrencia, por lo que declara que la opción de tratamiento de riesgos (ISO 27005) para los riesgos de tipo legal es la de "retención" , es decir de aceptación del riesgo sin realizar más acciones en

lo referente a la aplicación imprevista de cambios legales y litigando en tribunales en caso de divergencias en la aplicación de las leyes.
La Organización declara que su apetito al Riesgo Legal en todos sus roles es bajo, en línea con el apetito al Riesgo Operacional.

8. El Riesgo Reputacional se tratará como una propiedad emergente de los riesgos identificados por la organización, es decir, surge de otros tipos de riesgos materializados de la organización. Dado lo anterior, la estrategia para la gestión de los riesgos reputacionales será la mitigación de riesgos de los otros tipos, que pueden generar un daño reputacional como, por ejemplo: multas de la CMF, fraudes, incumplimiento de SLAs, etc.
Dado que el Riesgo Reputacional es consecuencia de la materialización de otros riesgos, el apetito a este riesgo es bajo en línea con el apetito al Riesgo Operacional.

9. Los Riesgos Generales del Negocio hacen referencia a cualquier potencial deterioro de valor de la posición financiera (como empresa en funcionamiento) de la Organización como resultado de la caída de sus ingresos (riesgo de Flujo de Caja) o del crecimiento de sus gastos (riesgo de Gastos Operacionales), de tal manera que los gastos superen a los ingresos y deriven en una pérdida que deba ser cargada contra el capital.
La Organización declara que su apetito a los Riesgos Generales del Negocio es bajo, en línea con el apetito al Riesgo Operacional.

10. El incumplimiento de esta política constituye una falta y será sancionado como tal.

11. Las Categorías de Riesgos Generales del Negocio, Cumplimiento y Custodia e Inversión seguirán las reglas y lineamientos de la gestión de Riesgo Operacional. No así las Categorías de riesgo Legal (riesgo retenido) y Reputacional (riesgo emergente).

12. Dado el alcance estratégico / organizacional de los Riesgos Generales del Negocio y de Custodia e Inversión, todos estos riesgos serán evaluados sólo mediante la metodología de cuantitativa.

VII.- ROLES Y RESPONSABILIDADES

Los roles y responsabilidades se encuentran definidos de acuerdo con la siguiente relación de rol y documento:

Rol	**Documento**
Directorio	Manual de Gobierno
Comités de Gobierno	Estatutos de Comité
Organización	Estructura Organizacional

VIII.- CIRCUITO DE APROBACIÓN E HISTORIAL DE CAMBIOS

El Directorio es el dueño y aprobador de este documento. El Gerente General es el responsable revisor, y es el encargado de asegurar que la Política sea revisada al menos anualmente por el Directorio. El Rol Modificador corresponde al Subgerente de Riesgo quien es el responsable de asegurar que la versión vigente de esta política se encuentre disponible, y también es responsable de realizar el proceso de revisión con partes involucradas que identifiquen la necesidad de cambios en la Política. Esta Política es de Nivel 1, por lo tanto, debe ser aprobada por el Directorio."

La versión de esta política fue aprobada por el Directorio de Comder según consta en Acta de sesión n°110, con fecha 18/10/2022 y por Directorio de Imerc en Acta de sesión n°112 en igual fecha. Esta política es emitida en base a versiones controladas bajo la autorización del Gerente General

La versión vigente de este documento está disponible para el personal en el Portal de Gestión del Conocimiento.

HISTORIAL DE CAMBIO

N° Versión	Fecha	Descripción
1.0	17/03/2015	Emisión Inicial, aprobada en el Acta N° 19 de Directorio
1.1	19/01/2016	Cambio del Mapa de Riesgos, en el que se explicitan los riesgos en distintos roles de ComDer, por lo que se identifican los siguientes riesgos: Reporting, gastos operacionales, flujo de caja, sistémico rol operador, fraude y reputacional. Aprobada en el Acta N° 29 de Directorio.
1.2	02/02/2016	Corrige error en mapa de riesgos (se incluyó riesgo sistémico como operador del SCC)
1.3	19/04/2016	Se incluye definición de apetito por riesgos y se cambia formato de roles y responsabilidades.
1.4	18/04/2017	Se incluye regla para la metodología de evaluación de riesgos, junto con los criterios de impacto y probabilidad
1.5	17/04/2018	Revisión sin modificaciones
1.6	22/05/2019	Se incorpora la tipificación de Ciberseguridad en los riesgos Operacionales. Se actualiza el mapa de riesgo. Se incorpora definición de Riesgo (definición general) y de Tolerancia al Riesgo, y se modifica la de Apetito por Riesgo. Se excluye riesgo de inversión y custodia del proceso de gestión de riesgo Se incorpora como complemento a la metodología de evaluación de riesgos cualitativa, la metodología cuantitativa FAIR. Se incorpora rol de Comité de Riesgo Operacional. Se modifica responsabilidad de Auditoría Interna Se incorpora rol y responsabilidad de Colaboradores
1.7	19/05/2020	Se incorpora definición del riesgo reputacional. Se incorpora definición del riesgo de cumplimiento Se indica que definiciones de Apetito por Riesgo se llevarán en este documento Se especifica que la metodología de evaluación es cuantitativa para todos los riesgos de la CCP en su rol de contraparte central. Se actualiza Mapa de Riesgos, separando el Riesgo reputacional, legal y de cumplimiento. Se elimina la referencia de que el riesgo de inversión financiera y custodia no será gestionado basado en la ISO 31000. Se corrige el numeral 3 del cap VI, explicitando que la evaluación de los riesgos de la SCC es semi cuantitativa.

		En roles y responsabilidades del Gerente de Riesgo se agrega que éste debe mantener informado de la gestión de riesgo al Directorio y al Comité de Riesgo. Se incluyen reglas 7, 8 con las opciones de tratamiento de riesgos legal y reputacional. Se incorpora el apetito por riesgo. Se incorpora regla 9 con definición de apetito para los riesgos Generales del Negocio. Se incluye regla 10 sobre incumplimiento de la política En el capítulo de roles y responsabilidades se agregan las que corresponden al Subgerente de Riesgo Operacional como responsable de la gestión de todos los riesgos de Comder en su rol de Operador del SCC. Se eliminan las referencias al Comité de Riesgo Operacional y se referencia al "Comité de Gestión Operacional del Sistema de Contraparte Central" (CGOS). Se incorporan criterios de impacto para Ciber Riesgos Se modifica el nivel de impacto en pérdidas de confidencialidad. Se elimina nivel de impacto para el riesgo legal dada la nueva regla 7
1.8	18/05/2021	Se incorpora regla 11 en relación con las reglas y lineamientos de las categorías de riesgo general del negocio, cumplimiento y custodia e inversión. Se incorporan responsabilidades al Comité de Gestión Operacional. Se incorpora rol del Comité de Riesgo Operacional. Se incorporan modificaciones en el capítulo de roles y responsabilidades y capítulo de historia de cambio.
1.9	20/07/2021	Se incorporan modificaciones que surgieron a partir de la identificación y evaluación de los Riesgos Generales del Negocio y Custodia e Inversión, las cuales fueron presentadas y aprobadas por el Comité de Riesgo Operacional: - En la sección IV.- Definiciones, se incorpora de definición de Riesgo de Reporting. - En la sección VI. Reglas: ▪ En la regla 9, se incorpora observaciones indicando el riesgo de Flujo de Caja y de Gastos Operacionales. ▪ Se incorpora regla 12.

		- En el Anexo A / a), se eliminan criterios de impacto de Riesgos Generales del Negocio (alineado a lo indicado en la regla 12).
2.0	22/02/2022	Se incorporan modificaciones en el capítulo de roles y responsabilidades tanto para el Comité de Gestión Operacional como para el de Riesgo Operacional y Riesgos Operador. Esta modificación fue aprobada por el Directorio en el Acta N°102, con fecha 01 de marzo de 2022.
2.1	22/06/2022	Se incluye Rol Operador de Infraestructuras (tecnológicas) de Mercado. Se modifica la política a un nivel organizacional.
2.2	18/10/2022	Se incorpora el Riesgo TI dentro de los Riesgos Generales del Negocio. Se modifica definición de riesgos Generales del Negocio.

ANEXO A
Criterios de Impacto y Probabilidad de Ocurrencia de los Riesgos de ComDer en su rol de Operador del SCC y de Operador de Infraestructuras (tecnológicas) de Mercado.

a) Niveles de Impacto semi cuantitativo para Riesgos como Operador del Sistema de Contraparte Central SCC y de Operador de Infraestructuras (tecnológicas) de Mercado

Nivel de Impacto	Continuidad de negocios	Seguridad de la Información	Ciber Riesgo	Calidad	Fraude
1	**Despreciable**	**Despreciable**	**Despreciable**	**Despreciable**	**Despreciable**
2	**Leve:** El impacto es menor, no afecta a la continuidad de negocios	**Leve:** Pérdida de disponibilidad, que no alcanzan a crear molestias a los Participantes y no afectan el Ciclo de Negocios descrito en las Normas de Funcionamiento y/o contratos.	Pérdida de disponibilidad, que no alcanzan a crear molestias a los Participantes y no afectan el Ciclo de Negocios descrito en las Normas de Funcionamiento o especificaciones del contrato. Monto de pérdida es inmaterial (menos 10 UF)	**Leve:** La falla o error, no alcanza a afectar las características de los servicios prestados a los Participantes.	**Leve:** Monto defraudado es inmaterial (menos 10 UF)
3	**Moderado:** el impacto es importante y se debe realizar seguimiento ya que se podría provocar una interrupción en los servicios con el paso del tiempo	**Moderado:** Genera pérdidas de disponibilidad de los servicios críticos TIC, que no afecta los horarios límites establecidos en las Normas de Funcionamiento (Rol SCC). Afectan los SLA con los Participantes. Pérdidas de integridad de datos de uno o dos Participantes, que obliga a enviar comunicación a los Participantes, explicando la situación para que puedan realizar sus cuadraturas de fin de día" -Perdida de confidencialidad, filtración de información definida como confidencial.	**Moderado:** -Genera pérdidas de disponibilidad de los servicios críticos TIC, que no afecta los horarios límites establecidos en las Normas de Funcionamiento o contratos Pero afectan los SLA con los Participantes. -Perdidas de integridad de datos de uno o dos Participantes, que obliga a enviar comunicación a los Participantes explicando la situación para que puedan realizar sus cuadraturas de fin de día" -Monto en pérdidas es > 10UF y < 200 UF	**Moderado:** Fallas o errores afectan algunas de las características de los servicios que cumplen los requerimientos de los Participantes. Ej. Errores en información estadística,	**Moderado:** Monto defraudado es > 10UF y < 200 UF
4	**Grave:** el impacto es alto, podría provocar la interrupción de uno de los servicios	**Grave**: -Falta de disponibilidad de los servicios críticos TIC que afectan los horarios del Ciclo de Negocios. -Errores de integridad de datos en las OC compensadas u operaciones de dos o más Bancos, que puedan implicar pérdidas financieras a los Participantes involucrados.	**Grave** -Falta de disponibilidad de los servicios críticos TIC que afectan los horarios del Ciclo de Negocios. -Errores de integridad de datos en las OC compensadas u Operaciones de dos o más Bancos, que puedan implicar pérdidas financieras a los Participantes involucrados. -Monto en pérdidas es >200 UF y < 25.000 UF. -Perdida de confidencialidad, filtración de detalles de las OC compensadas por los	**Grave:** -Errores o fallas que afectan los servicios de compensación y liquidación de las Ordenes de Compensación enviadas.. -Errores o fallas que afectan los servicios Ej -Errores o fallas que ocasionen pérdidas financieras a los Participantes	**Grave:** Monto defraudado es >200 UF y < 25.000 UF o en el fraude hay más de una persona involucrada (independiente del monto defraudado)

			Participantes y datos de participantes y clientes -Perdida de confidencialidad, filtración de detalles de los contratos		
5 (Alto Impacto)	**CN**: **Gravísimo:** el impacto es desastroso, se han interrumpido los servicios de Compensación, Liquidación y Registro o de infraestructura. **Fraude**.	**Gravísimo**: Afecta la Continuidad de Negocios -Perdidas de disponibilidad de los Servicios Críticos TIC que no permiten el cierre de las operaciones del día. -Perdida de Integridad de Datos que no hace posible las conciliaciones de las cuentas de margen efectivo y/o margen instrumentos.	**Gravísimo**: Afecta la Continuidad de Negocios -Perdidas de disponibilidad de los Servicios Críticos TIC que no permiten el cierre de las operaciones del día. -Perdida de Integridad de Datos que no hace posible las conciliaciones de las cuentas de margen efectivo y/o margen instrumentos Afecta la Continuidad de Negocios -Perdida de Integridad de Datos que afecta la Continuidad de Negocios -Cualquier pérdida que afecte a: los Participantes, los EEFF -Pérdida excede el Patrimonio Mínimo (150.000 UF) definido por la CMF NG 266 será considerado como un desastre.	**Gravísimo**: Afecta la Continuidad de Negocios. Información incompleta o errónea Información incompleta o errónea de las posiciones, saldos cuentas de margen, nivel de Fondo de Garantía., que imposibilitan continuar con la operación del sistema SCC.	**Gravísimo**: Afecta la Continuidad de Negocios Cualquier fraude que afecte a: los Participantes, los EEFF, actos ilegales y de corrupción independientemente del monto defraudado será considerado como un desastre reputacional y si el monto defraudado excede el Patrimonio Mínimo (150.000 UF) definido por la SVS NG 266 será considerado como un desastre financiero.

Nivel de Impacto	Cumplimiento
1	**Despreciable**
2	**Leve:** No alcanza a afectar el cumplimiento de las normas de la CMF, leyes atingentes a ComDer, leyes laborales y tributarias en tiempo y forma.
3	**Moderado:** Genera atrasos en la presentación de pagos previsionales y/o tributarios, pero sin aplicación de multas Genera incumplimientos a las Normas Funcionamiento, originan un Oficio de amonestación de la CMF.
4	**Grave:** -Genera atrasos y/o errores de cálculo en la presentación de pagos previsionales y/o tributarios, con aplicación de multas. -Implica solicitar la suspensión de los servicios de Compensación y Liquidación.
5 (Alto Impacto)	**Gravísimo**: Afecta la Continuidad de Negocios Errores graves en el pago de obligaciones tributarias y/o previsionales, que significan una multa, llegando a la cancelación del Giro del negocio. -Imposibilidad de subir al sistema SEIL la información requerida por la CMF.

b) Niveles semi cuantitativos de Probabilidad de Ocurrencia

	Nivel	Descripción	Criterio
Frecuencia de ocurrencia: Tiempo transcurrido entre dos eventos.	1	Raro	>5 años
	2	Improbable	>1 año < 5 años
	3	Posible	>6 meses < 1 año
	4	Probable	>1 mes < 6meses
	5	Casi cierto	< 1mes