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.- OBJETIVOS

Asegurar que la Organización tenga un entendimiento actualizado, claro y correcto de los riesgos de seguridad de la información, de manera que sean evaluados y tratados para contribuir al cumplimiento de los objetivos de la Organización.

Los objetivos en los ámbitos de la Seguridad de la Información son:

a) Ámbito de la confidencialidad: prevenir la divulgación no autorizada de la información.
b) Ámbito de la integridad: prevenir modificaciones no autorizadas de la información.
c) Ámbito de la disponibilidad: prevenir interrupciones no autorizadas/controladas de los recursos informáticos.

II.- ALCANCE

Esta Política General se aplica a toda la información generada en la Organización, con especial énfasis en la información relacionada con los Participantes y los Entes Reguladores.

III.- DEFINICIONES

Seguridad de la Información: es entendida como la preservación y protección de la confidencialidad, integridad y disponibilidad de la información, de una amplia gama de amenazas. Su propósito es minimizar el daño, garantizar la integridad, confidencialidad y disponibilidad de la información y los servicios, resguardando la imagen y reputación de la Organización.

Ciberseguridad: Preservación de la confidencialidad, integridad y disponibilidad de la información en el Ciberespacio.

Ciberespacio: Ambiente complejo resultado de la interacción de personas, software y servicios en la internet por medio de aparatos tecnológicos y redes conectados a ellos, el cual no existe en ninguna forma física.

IV.- REGLAS

1. La Información es un bien valioso para la Organización que, al igual que los bienes asociados a su tratamiento, debe ser administrado con la debida atención. La seguridad de la información es un atributo necesario en los procesos de negocios y procesos TI ejecutados, como en los servicios ofrecidos por la Organización.

2. La Seguridad de la Información y de los bienes asociados a su manejo, es responsabilidad de todos los funcionarios, independientemente del cargo que desempeñen.

3. La información es clasificada de acuerdo con criterios de valoración, que dependen de la importancia que posee esta para el negocio y su impacto vía: destrucción, filtración no autorizada, disponibilidad e integridad y niveles de autorización. La información debe ser protegida en función de esa clasificación.

4. La información confidencial de la organización y la de los Participantes no debe quedar disponible a personas o entidades externas a la empresa, salvo en las situaciones y formas expresamente establecidas en la legislación y normas vigentes y con los controles que garanticen su protección y confidencialidad.

5. La organización declara su decisión de cumplir con la legislación vigente y la normativa de los Organismos Reguladores y Fiscalizadores, relacionadas con aspectos de reserva, privacidad de

la información de sus clientes, trabajadores y accionistas y derechos de propiedad intelectual.

6. 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 operacional, ni modificación de parámetros de los sistemas críticos deberá ser ejecutado sin el complemento de un procedimiento que dé las garantías requeridas y con los controles correspondientes.

7. Todo empleado, así como el personal de un proveedor clasificado como Crítico de Outsourcing, el cual posea acceso a la información de la Organización, debe estar en conocimiento de esta Política y debe acceder exclusivamente a la información que le sea estrictamente necesaria para cumplir las funciones que la empresa le ha encargado.

8. Todo empleado o colaborador tiene la obligación de notificar cualquier evento, incidente o situación que afecte o pueda afectar la Seguridad de los Activos de Información.

9. La Organización contará con actividades de monitoreo con el fin de detectar e investigar eventos e incidentes y generar acciones de mitigación, a modo de resguardar la confidencialidad, disponibilidad e integridad de sus activos de información en materia de Seguridad de Información y Ciberseguridad. Esto incluye la gestión y supervisión de cuentas privilegiadas.

10. La Organización reconoce que la sensibilización, capacitación y entrenamiento adecuados a su personal en las materias de Seguridad de la Información y Ciberseguridad son tareas prioritarias.

11. De esta Política General se desprende un conjunto de Políticas de Seguridad de materias específicas y sus respectivas herramientas de implantación.

12. Las Políticas de Seguridad de Información regirán independiente de cómo se presente o almacene la información, los sistemas que la procesen o los métodos de transporte utilizados, acorde a la evaluación de riesgo del contexto

13. Las disposiciones relacionadas con las Políticas referidas a la Seguridad de la Información serán debidamente controladas en su cumplimiento por los estamentos definidos por la Organización.

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

15. Políticas relacionadas al Sistema de Gestión de Seguridad de la Información (SGSI):

    a) La Planificación Estratégica vigente, la Política General de Riesgo Operacional y el Proceso de Gestión de Riesgos del Operador proveen el contexto para identificar, valorar, evaluar y controlar los riesgos relacionados a la información a través del establecimiento y mantención de un Sistema de Gestión de Seguridad de la Información (SGSI).

    b) La Evaluación de Riesgos, la Declaración de Aplicabilidad (SOA) según norma ISO 27001 y el Plan de Tratamiento de Riesgos indican cómo son mitigados y controlados los riesgos relacionados a la seguridad de la información en la Organización.

    c) El Dueño del SGSI es responsable de velar que los dueños de activos mantengan un proceso de evaluación y registro de vulnerabilidades de los mismos y la mantención del plan de tratamiento de riesgos de la seguridad de la información correspondientes.

    d) Se podrán realizar evaluaciones de riesgos adicionales, cuando sea necesario, para determinar los controles apropiados para un riesgo específico.

    e) La organización mantendrá un inventario de sus activos de información, identificando y caracterizando los mismos de forma suficiente para la adecuada gestión de los riesgos asociados, teniendo en cuenta atributos tales como ubicación física, función que presta, entre otros datos, incluyendo versión, cuando aplique.

    f) Las siguientes actividades de control (políticas, procedimientos y controles específicos) son fundamentales para implementar esta política:

        - Planes de Continuidad acorde a la Política General Corporativa de Continuidad de Negocios, basada en la norma ISO 22301, a fin de recuperar las operaciones o procesos críticos en forma oportuna y eficaz.
        - Las protecciones contra virus, software malicioso y ataques de ciberdelincuentes.
        - Los controles para prevenir fraudes.

- Registro y reporte de los incidentes de seguridad de la información y ciberseguridad.
- Política de Clasificación de la Información.

g) Los objetivos de control para cada una de estas áreas están contenidos en el manual del SGSI y estarán soportados por políticas y procedimientos específicos debidamente documentados.

h) El personal de la Organización será debidamente capacitado en las materias relacionadas a la seguridad de la información y ciberseguridad, de acuerdo con sus funciones y tiempo de permanencia en la Organización, con una periodicidad establecida y oportuna.

i) La gestión de la Seguridad de la Información se medirá y evaluará a través de la fase Evaluación del Rendimiento según lo establecido en la norma ISO 27001, la cual incluye revisiones realizadas por Auditoría Interna. La evaluación se realizará al menos anualmente.

j) Esta política se aprobará por el Directorio, al menos anualmente y cuando se produzcan cambios significativos en la organización, en el personal, en la arquitectura tecnológica, en los sites de procesamiento, en los proveedores estratégicos y cambios de oficinas. En caso de existir modificaciones, éstas se someterán a la aprobación del Directorio.

k) La mejora continua es parte integral de la Gestión de la Seguridad de la Información de la Organización. Por lo tanto, los incidentes de Seguridad de la Información producidos en la ejecución de un proceso y/o sistema de información y los hallazgos o no conformidades observados o detectados en la ejecución de los controles específicos, en las auditorías internas o externas deben ser registrados, monitoreados y solucionados oportunamente.

l) Los riesgos de Seguridad de la Información asociados a información de la Organización son definidos como Riesgos Operacionales y, por lo tanto, deben cumplir con la Política de Riesgo Operacional de la Organización.

m) De existir desviaciones al cumplimiento de reglas de esta Política General de Seguridad de la Información, deberán ser aprobadas por el Gerente de Operaciones o el Gerente de Tecnología y Proyectos.

16. La Ciber Seguridad es un subconjunto de la Seguridad de la Información y será tratada de acuerdo a la norma ISO 27100 Information Technology – Cybersecurity, complementando con elementos de los marcos de mejores prácticas NIST CSF (Cybersecurity Framework) y CIS Controls (de Center for Internet Security). Por lo que se identificarán explícitamente la evaluación y tratamiento de los ciber riesgos y por ende las Ciber Amenazas.

17. Como estrategia para la gestión de la Ciber seguridad de los próximos 3 años[1], se adoptarán los conceptos y atributos de la normas ISO 27110 (directrices marco ciberseguridad), ISO 27002 (controles seguridad de información) y función de controles FAIR-CAM (modelo analítico de controles). En base a estos marcos se seguirán las siguientes etapas de trabajo:
    - Análisis de las brechas de Planes de Tratamiento de Riesgo (PTR, controles) existentes, relacionado con la estrategia TI.
    - Evaluación de implementación de PTR (controles), relacionado con la estrategia TI.
    - Profundización en atributos de respuesta y recuperación, relacionado con la estrategia de negocio.

    La priorización de las inversiones en Ciber seguridad deberán ser consistentes con las estrategias TI y Seguridad de la Información-Ciber seguridad.

18. La Organización realizará regularmente pruebas para detectar las amenazas y vulnerabilidades que pudieran existir sobre su sistema de gestión de seguridad de la información en el ciberespacio. El análisis de vulnerabilidades se realizará al menos semestralmente, en tanto que pruebas de intrusión y/o ethical hacking se llevarán a cabo al menos cada 2 años. Estos análisis y sus resultados serán gestionados por las áreas relacionadas con seguridad de la información.

V.- 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

[1] A contar de enero 2023

Organización	Estructura Organizacional

VI Control de Versión

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 Oficial de Seguridad de Información 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 vigente de este documento está disponible al personal en el Portal de Gestión del Conocimiento.

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

VII.- HISTORIA DE CAMBIO

N° Versión	Fecha	Descripción
1.0	17/03/2015	Emisión Inicial
1.1	19/04/2016	Inclusión de cláusula 14k) que relaciona explícitamente esta política con la política de Riesgo Operacional. Cambios de Forma como: Nombre del Comité de Riesgos y Cumplimiento por Comité de Gestión Operacional del SCC y Reemplazo del diagrama de Roles y Responsabilidades.
1.2	17/05/2016	Cambio en código de encabezado
1.3	18/04/2017	Revisión sin modificaciones
1.4	12/09/2017	Incorporación de definiciones de Ciber Seguridad y Ciber Espacio y regla 15 sobre ciber riesgos.
1.5	17/04/2018	Revisión sin modificaciones

1.6	22/05/2019	Cambios de redacción (sin cambios de fondo): - Regla 4: se agrega adjetivo confidencial. - Regla 14e: se utiliza redacción con términos similares a RAN 1-13. - Regla 14g: se agrega de acuerdo a sus funciones y tiempo de permanencia. - Se adiciona Regla 16.- sobre realizar regularmente pruebas para detectar las amenazas y vulnerabilidades. Adicionalmente, se separa el rol del Comité de Gestión Operacional y el del Comité de Gestión Integral.
1.7	19/05/2020	Regla 14 l: se incorpora para indicar que de existir desviaciones al cumplimiento de reglas de esta política, deberán ser aprobadas por el Gerente de Operaciones o el Gerente de Tecnología y Proyectos. Regla 15: Se modifica ISO 27032 por CIS Controls como marco de mejores prácticas en ciberseguridad Eliminación de referencia a Comité de Gestión Integral Incorporación de responsabilidad del Oficial de Seguridad de Información para el mantenimiento de la política.
1.8	18/05/2021	Regla 6: se agrega "sin el complemento" como mejora de redacción Regla 7: se acota tipo de personal de proveedor que debe estar en conocimiento de esta política Regla 12: se agrega "acorde a la evaluación de riesgo del contexto" Regla 14 a): se reemplaza "manual de sistema de gestión integral" por "proceso de gestión de riesgos del operador" Regla 14 c) se modifica responsabilidad del dueño del SGSI en términos de velar por las responsabilidades de los dueños de activos. Regla 15: Se incorpora norma ISO 27100:2020 y marco NIST CSF 1.1. En punto V.- Roles y responsabilidades: Se cambia la responsabilidad del Directorio de establecer y mantener, a ser dueño y aprobador de la presente política. Se incorpora responsabilidad de informar a Comité de Auditoría por parte de Auditoría. Al Gerente General se le incorpora que es responsable revisor y encargado de asegurar que la Política sea revisada al menos anualmente por el Directorio. Al Comité de Gestión Operacional se agrega nota sobre que las otras responsabilidades propias de la gestión de describen en la Estructura Organizacional. Se incorpora el Comité de Riesgo Operacional y su rol.

		En la sección al final sobre control de versión, se modifican las responsabilidades con este documento.
1.9	22/06/2022	Se incorpora regla 9, con lineamientos sobre monitoreo de eventos, gestión y supervisión de cuentas privilegiadas. Se incorpora en regla 15, punto e, acerca del inventario de activos de información. Se generaliza referencia a marcos como ISO 27001 y otros para independizar de versión específica. Se define política a nivel organizacional.
1.10	18/10/2022	Se incorpora regla 17, con lineamientos sobre estrategias para la gestión de la Ciber seguridad. Se complementa título de esta política con Ciber Seguridad