# POLITICA GENERAL CORPORATIVA DE CONTINUIDAD DE NEGOCIOS

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

Los principales objetivos de esta política son:

a) Comunicar a todas las Partes Interesadas (internas y externas) el compromiso de la Organización con la Gestión de la Continuidad de Negocios.
b) Reflejar el compromiso gerencial con el desarrollo, implementación y mantención de un Sistema de Gestión de Continuidad de Negocios.
c) Asegurar la protección de las personas, activos, información y la reputación de la Organización.
d) Asegurar el cumplimiento de los requerimientos regulatorios después de un incidente.
e) La Gestión de Continuidad de Negocios será implementada en cumplimiento con el siguiente Estándar Internacional:
ISO 22301:2019 "Seguridad y Resiliencia – Requerimientos de un Sistema de Gestión de Continuidad de Negocios"

## II.- DEFINICIONES

**Continuidad de Negocio** (ISO 22301:2019 Seguridad y Resiliencia – Requerimientos de un Sistema de Gestión de Continuidad de Negocios): Capacidad de la Organización de continuar la entrega de sus servicios dentro de plazos aceptables a una capacidad predefinida durante una disrupción.

**Incidente** (ISO 22301:2019 Seguridad y Resiliencia – Requerimientos de un Sistema de Gestión de Continuidad de Negocios)**:** Evento que puede ser, o podría llevar a, una disrupción, pérdida, emergencia o crisis.

**Disrupción** (ISO 22301:2019 Seguridad y Resiliencia – Requerimientos de un Sistema de Gestión de Continuidad de Negocios): Incidente, ya sea anticipado o no, que causa una desviación negativa no planificada de la entrega esperada de servicios de acuerdo con los objetivos de una organización.

**Mejora Continua** (ISO 22301:2019 Seguridad y Resiliencia – Requerimientos de un Sistema de Gestión de Continuidad de Negocios)**:** Actividad recurrente para mejorar el rendimiento (resultado medible).

## III.- ALCANCE

El Sistema de Gestión de la Continuidad de Negocios (SGCN), en relación con los servicios entregados a sus participantes, cubre todas las actividades relacionadas con la gestión de las tecnologías de la información, procedimientos, infraestructura, instalaciones y recursos humanos en la Oficina Principal, apoyada por un Escritorio Remoto de Operaciones (ERO).

## IV.- REGLAS

1. La Organización se compromete con el cumplimiento de la legislación vigente y requerimientos regulatorios relativos a la Continuidad de Negocios.

2. La Organización designará a un dueño del Sistema de Gestión de Continuidad de Negocios (SGCN) dentro de la Organización, encargado de velar por los resultados de la gestión de continuidad de negocios y de proveer soporte y dirección cuando sea necesario.

3. La Organización se compromete a establecer y mantener un Sistema de Gestión de Continuidad de Negocios (SGCN).

4. La Organización se compromete a realizar en forma periódica (al menos anualmente) un Análisis de Impacto al Negocio (BIA), que considera los criterios necesarios para identificar los procesos de mayor criticidad y determinar los tiempos de recuperación objetivo (RTO), punto objetivo de recuperación (RPO) y período máximo tolerable de interrupción (MTPD), definidos por la Organización. Los resultados del Análisis de

Impacto al Negocio (BIA), serán informados por medio del Informe Anual de Riesgo Operacional al Directorio para su revisión y aprobación.

5. La Organización se compromete a realizar en forma periódica (al menos anualmente) una Evaluación de Riesgos de Continuidad de Negocios de los procesos de mayor criticidad a fin de mitigar su impacto o disminuir su probabilidad de ocurrencia.

6. Antes de introducir nuevos servicios, procesos, actividades o sistemas, la Organización se compromete a evaluar los riesgos de continuidad de negocios que se podrían estar asumiendo.

7. La Organización establecerá planes de continuidad de negocio y recuperación tecnológica, que permitan recuperarse ante interrupciones que afecten la continuidad de los servicios críticos.

8. Los planes deberán ser probados y revisados al menos anualmente. Dependiendo del resultado de estas pruebas, los planes deberán ser modificados cuando sea necesario.

9. Los resultados de estas pruebas deben ser reflejados en un informe que defina el alcance, condiciones en que se realizan, y los planes de acción si corresponde.

10. La Organización proveerá una estructura organizacional de alto nivel que tenga la responsabilidad de gestionar los incidentes y las crisis operacionales, junto con la invocación de estrategias (continuidad y comunicacional) y planes.

11. La Organización debe considerar un proceso formal para la gestión de incidentes que pudieran interrumpir o afectar la provisión de los servicios críticos. Este proceso considera la generación de información suficiente, adecuada y oportuna de los riesgos vinculados con esta materia, los cuales son reportados a las instancias que toman decisiones en caso de ser necesario.

12. Todo el personal de la Organización deberá ser concientizado en los planes de continuidad de negocio y recuperación tecnológica para responder a todos los escenarios definidos y estar capacitado para ejercer sus roles y responsabilidades frente a la invocación de uno de estos planes.

13. La Organización debe contar con programas de capacitación y entrenamiento que permitan que todos los niveles del personal asuman y comprendan sus responsabilidades dentro del sistema de gestión de continuidad de negocios. Para estos fines, se privilegiará el entrenamiento interno y cursos impartidos por especialistas en la materia.

14. La Organización mantendrá operativa una infraestructura tecnológica redundante, de manera de minimizar los tiempos de recuperación ante cualquier falla de un componente.

15. La Organización mantendrá sitios de procesamiento de datos e infraestructura tecnológica robusta resultante de una adecuada gestión, con las siguientes características:

    - Los sitios de procesamiento de datos, ya sea principal o de contingencia, se encuentran permanentemente homologados en la infraestructura tecnológica y versiones de software, y operando en modalidad activo-pasivo.
    - El diseño, la construcción y la operación de los sitios de procesamiento de datos, se encuentran certificados por una entidad especializada e independiente.
    - La infraestructura de los sitios de procesamiento de datos tiene la capacidad, en cuanto a energía, refrigeración y mantenimiento, para alcanzar una disponibilidad de operación de al menos 99,98% o downtime de 1,6 horas anuales.
    - La configuración de los sitios permite disponer de una infraestructura de telecomunicaciones y de equipamiento computacional con la redundancia necesaria para evitar puntos únicos de falla; con medios de comunicación distintos en sus trayectorias; y gestionado por especialistas, de manera de proporcionar soporte técnico que funcione de acuerdo con las necesidades del negocio y operando preferentemente en modalidad 24x7.
    - Los sitios (principal y de contingencia) han sido dispuestos de tal forma que no queden expuestos a los mismos riesgos, considerando, entre otros, factores como la ubicación y distancia entre las instalaciones.
    - La Organización cuenta con infraestructura y procedimientos de respaldo que permiten recuperar los datos, software básico y aplicativos, ante una contingencia o corrupción de la información de acuerdo con los RPO y RTO establecidos.

16. La Organización mantendrá planes actualizados de continuidad de infraestructura tecnológica, los que incluyen planes de recuperación ante desastres (DRP).

17. Los riesgos de Continuidad de Negocios asociados a los Servicios de la Organización y sus dependencias son definidos como Riesgos Operacionales y, por lo tanto, deben cumplir con la Política de Riesgo Operacional de la Organización.

18. La Organización se compromete con la mejora continua en el Sistema de Gestión de la Continuidad de Negocios y sus procesos.

19. La Organización realiza auditorías independientes al Sistema de Gestión de Continuidad de Negocios, con la profundidad y alcance necesario y suficiente.

20. La Organización se compromete a informar al Directorio por medio de su Gerente General, al menos anualmente, sobre la gestión de Continuidad de Negocios por medio del Informe Anual de Riesgo Operacional.

21. Esta política se aprobará por el Directorio, al menos anualmente y cuando ocurran cambios significativos en la Organización, en el personal, en la arquitectura tecnológica, en los sites de procesamiento, en los proveedores estratégicos y/o cambios de oficinas.

22. La Política General de Continuidad de Negocios se encontrará disponible:

    a. Para el personal de la Organización, a través del Portal de Gestión del Conocimiento.
    b. Para las Partes Interesadas Externas, a través del sitio web de la Organización.

23. En el contexto de una contingencia de carácter sistémica que afecte a varias entidades simultáneamente, es necesario que la Organización cuente con planes para mitigar el efecto que se pueda producir en el sistema financiero:

    - Se debe contar con un plan comunicacional para informar de manera efectiva la materialización de algún escenario de contingencia a las partes interesadas definidas.

    - Se debe contar con equipos humanos altamente capacitados y/o entrenados para las labores de coordinación, tanto en el plano interno

como con las autoridades competentes y otras instituciones públicas y privadas.

- Se debe contar con procedimientos para ubicar y contactar al personal dentro de las zonas afectadas, considerando además la provisión de transporte para facilitar la logística y el traslado del personal.

- Se debe contar con medios de comunicación alternativos como contingencia a los medios tradicionales de comunicación (teléfono, correo electrónico y aplicación de mensajería instantánea, principalmente).

## 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 |
| Organización | Estructura Organizacional |

## VI.- CONTROL DE VERSIONES

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 Encargado de Continuidad de Negocios 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 para el personal en el Portal de Gestión del Conocimiento.

Esta política fue aprobada por el Directorio de ComDer en la sesión n°127, de fecha 19/03/2024 y por el Directorio de Imerc en la sesión n°129 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 | Cambios de forma como: Reemplazo de Roles y Responsabilidades. |
| 1.2 | 24/08/2016 | Se traspasa a pdf. |
| 1.3 | 18/04/2017 | Se verifica que a la fecha el documento no ha sufrido cambios. |
| 1.4 | 17/04/2018 | Revisión sin modificaciones. |
| 1.5 | 22/05/2019 | Los puntos contenidos en el Objetivo f) se traspasan a Reglas.<br>El alcance de la Política ha sido modificado por el alcance que estará declarado en el certificado BSI.<br>El orden de las Reglas se modifica tras la incorporación de las Reglas N°5, 6, 8, 10, 11, 12, 16, 17, 20, 21 y 24.<br>Se incorpora nuevo rol al Gerente General.<br>Se incorpora nuevo rol al Comité de Gestión Operacional.<br>Se incorpora el Comité de Gestión Integral. |
| 1.6 | 19/05/2020 | Se elimina regla 8 que hacía referencia a algunos escenarios. Regla redundante respecto a la elaboración de planes de continuidad.<br>Se elimina Comité de Gestión Integral de Roles y Responsabilidades y su rol se asigna al Comité de Gestión Operacional.<br>Se modifica sección final de este documento respecto a la responsabilidad del Oficial de Continuidad de Negocios con la política. |
| 1.7 | 18/05/2021 | Se modifica regla N°4, incorporando "Los resultados del Análisis de Impacto al Negocio (BIA), serán informados por medio del Informe Anual de Riesgo Operacional al Directorio para su revisión y aprobación." |

| N° Versión | Fecha | Descripción |
|---|---|---|
| | | Se modifica Regla N°20 indicando que la Gestión de Continuidad de Negocios será informada al Directorio por medio de Informe Anual de Riesgo Operacional.<br><br>Se modifica cuarto párrafo de la Regla N°23, donde decía que se debe contar con telefonía satelital como contingencia a medios de comunicación, se reemplaza indicando que "Se debe contar con medios de comunicación alternativos como contingencia a los medios tradicionales de comunicación (teléfonos, correo electrónico)."<br><br>Punto V de Roles y Responsabilidades:<br>Se cambia la responsabilidad del Directorio de establecer y mantener a ser dueño y aprobador de la política de Continuidad de Negocios.<br><br>Al Gerente General se incorpora ser "responsable revisor, y es el encargado de asegurar que la Política sea revisada al menos anualmente por el Directorio."<br><br>En Comité de Gestión Operacional se modifica primer punto en relación con la aprobación de BIA para la Continuidad de Negocios, incorporando la Continuidad Tecnológica<br><br>En Comité de Gestión Operacional se incorpora nota "Las otras responsabilidades propias de la gestión de describen en la Estructura Organizacional."<br><br>Se incorpora Comité de Riesgo Operacional y su rol.<br><br>En Auditoría Interna se incorpora rol "Informar de su labor directamente al Comité de Auditoría y Directorio"<br><br>Se eliminan referencias a Oficial de Continuidad de Negocios.<br><br>Sección final de la Política, se modifica respecto a responsabilidades con este documento. |

| N° Versión | Fecha | Descripción |
|---|---|---|
| 1.8 | 01/03/2022 | Se modifica la regla N°15 indicando que los sitios de procesamiento de datos operan en modalidad activo – pasivo.<br>Esta modificación fue aprobada por el Directorio en el Acta N°102, con fecha 01 de marzo de 2022. |
| 1.9 | 22/06/2022 | Se actualiza la versión de la norma ISO 22301, pasando de la 2012 a la 2019.<br>Se define política a nivel Organizacional.<br>Se realizan modificaciones menores de redacción.<br>Estas modificaciones fueron aprobadas por el Directorio en el Acta N°106, con fecha 22 de junio de 2022. |
| 2.0 | 20/06/2023 | Para las definiciones incidente disruptivo y mejora continua, se referencian las normas ISO 22300:2018 y 22301:2019, respectivamente.<br>En la regla n°4, se incorpora el punto objetivo de recuperación (RPO) y el período máximo tolerable de interrupción (MTPD).<br>En la regla n°9, se reemplaza planes de corrección por planes de acción.<br>En la regla n°10, se extienden los planes de continuidad de negocio a continuidad tecnológica, y se reemplaza planes de comunicación por estrategias de comunicación.<br>En la regla n°16, se indica que los planes de continuidad de infraestructura tecnológica incluyen planes de recuperación ante desastres.<br>En la regla n°23, se incorpora la aplicación de mensajería instantánea como medio tradicional de comunicación.<br>Se realizan correcciones menores de redacción.<br>Estas modificaciones fueron aprobadas por el Directorio en el Acta N°118, con fecha 20 de junio de 2023. |
| 2.1 | 19/03/2024 | Se actualizan las definiciones "Continuidad de Negocio", "Incidente Disruptivo" y "Mejora Continua", de acuerdo con la ISO 22301:2019.<br>La definición de "Incidente Disruptivo" se desglosa en "Incidente" y "Disrupción".<br>Cuando se mencionan los planes de continuidad de negocio, también se hace referencia a los de recuperación tecnológica. |

| N° Versión | Fecha | Descripción |
|---|---|---|
| | | Se realizan precisiones en algunas reglas y cambios menores en redacción.<br>Estas modificaciones fueron aprobadas por el Directorio en la sesión N°127, con fecha 19 de marzo de 2024. |