BIOMETRICS

POLÍTICA DE CONTINUIDAD DEL NEGOCIO

Política

V 1.0

15/12/2020

Identificación del Documento

Identificación del documento	PO-02-00 Política de Continuidad del Negocio
Registro(s) relacionado(s)	Minuta del Comité de gestión de riesgo, continuidad y seguridad de la información. Minuta del Comité de gestión de RCS.
Documento(s) relacionado(s)	Plan Sin Agua Potable Plan Sin Energía Eléctrica Plan Sin Instalaciones Plan Sin personas Plan Sin proveedores Plan Sin Sistemas Evaluación plan de contingencia Evaluación plan de continuidad
Responsable de aprobación	Gerente General
Dueño funcional	Seguridad y Acreditaciones
Puesto(s) implicado(s)	Responsable del SGI, OSI, CEO, Gerente General, Líder de Proceso, Responsables de proceso.

Control de Versiones

Motivo:
Cambio del diseño del documento
Actualizar la documentación base para adaptarse a las normas de certificación

Responsable	Versión	Consultados/Revisión	Informados	Aprobación
Ingeniero de Procesos Analista Procesos	1.0	OSI PMO	Gerente de (TI) Gerente BI Gerente de Finanza y Administración Gerente Internacional Gerente I + D	Gerente General
Dic 2020		Dic 2020	Dic 2020	Dic 2020

I. Primera Parte: Aspectos Generales

1. Alcance:

Esta política se aplica en forma transversal a todos los procesos de negocio de TOC.

Considera la identificación de los procesos del negocio, el nivel de criticidad asociado a cada uno, definición de sitios de contingencia, plan de pruebas, procedimientos de activación, escalamientos y responsables, ante los siguientes escenarios de contingencia:

a) Sin sistemas
b) Sin instalaciones
c) Sin personal crítico
d) Sin proveedores
e) Sin servicios básicos

2. Objetivos:

La presente política tiene como objetivos:

a) Asegurar la continuidad operativa de TOC y mantener la integridad y disponibilidad de los activos de información o minimizar su pérdida ante la ocurrencia de eventos como falla de servidores, aplicaciones, equipos de comunicaciones, enlaces o proveedores, indisponibilidad de oficinas centrales, indisponibilidad de datacenter.
b) Salvaguardar la integridad física del personal de TOC.

c) Establecer medidas que mitiguen las interrupciones de las actividades de TOC debido a los efectos de desastres o de situaciones que afectan su normal operación.

La continuidad del negocio es materia y preocupación de todos los colaboradores de TOC, áreas de negocio, comerciales, operativas y de apoyo.

a) Todas las áreas del negocio, en las materias que le aplican a cada una, deben
participar activamente en la elaboración, actualización y prueba de los planes de Continuidad del Negocio, de forma tal que éstos provean efectivas acciones
alternativas para la continuidad operativa de la organización, en el caso de que se produzca una interrupción de las actividades regulares consideradas como críticas.

b) Las acciones frente a escenarios de contingencia deben resguardar, en todo momento, la seguridad de las personas y los principios y estándares en la seguridad de la información.

c) El Plan de Contingencia está basado en los siguientes componentes:

- Sistemas de información distribuidos en dos Data Centers, siendo cada uno de ellos capaz de asumir el procesamiento del total de las aplicaciones críticas de TOC y si es que fallara el otro.
- Oficinas de contingencia para el personal de los procesos críticos de TOC determinados según análisis de impacto para el negocio (BIA).
- Esquema de reemplazo para el personal crítico. (esquema de Backups)

d) Los planes de continuidad del negocio están insertos en el concepto de riesgo operacional.

3. Estructura y Responsabilidades

a) Comité de continuidad del negocio

El comité de continuidad del negocio se conformará de los siguientes cargos:

- Gerente General
- Gerente de Seguridad
- Gerente de Finanzas
- Gerente Comercial
- Gerente BI / Marketing
- Gerente Nvos Productos
- Gerente de Tecnologías
- Gerente de I+D
- Control de Gestión

b) Grupo Continuidad de Negocios

Es una instancia para la toma de decisiones y de orientación estratégica para la gestión de continuidad del negocio, que consideran entre otros la planificación, implementación y mantenimiento de la Continuidad del Negocio.

Entre las responsabilidades del grupo de continuidad de continuidad de negocios se encuentran:

- Identificar y acordar todas las responsabilidades y roles, definidas en los planes de Continuidad del Negocio.
- Proveer a TOC de un marco único y homogéneo, en el que se basan los planes de continuidad.
- Identificar la pérdida aceptable de la información y los servicios.
- Aprobar los escenarios, metodologías y periodicidad de pruebas.
- Controlar el cumplimiento de los planes aprobados.
- Proveer de recursos para la capacitación y educación del personal en los procedimientos y procesos acordados.
- Controlar una vez al año la actualización de los planes de continuidad.
- Reportar mensualmente los incidentes al directorio o en casos excepcionales reportar en cuanto una falla se materialice.
- Creación, actualización y control de los planes de continuidad
- Planificar y coordinar la ejecución de las pruebas de los planes y asegurar la capacitación correspondiente del personal involucrado
- Desarrollar e implementar planes de continuidad operativa, que permitan restaurar la operación del negocio, frente a contingencias o fallas tecnológicas, como así también en escenarios de problemas humanos u operacionales (inhabilitación del acceso de personas a las instalaciones, huelgas etc.), que afecten sus respectivos procesos comerciales críticos.
- Identificar los eventos operacionales o tecnológicos que pueden causar interrupciones a los procesos comerciales, junto con la probabilidad y el impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.
- Incluir controles que permitan identificar y disminuir los riesgos, además de limitarlas consecuencias de daños de incidentes y asegurar que se podrá reanudar a tiempo las operaciones esenciales.
- Establecer controles preventivos y recuperativos que ayuden a mantener la Continuidad del Negocio.
- Considerar la contratación de seguros que formen parte del proceso de Continuidad del Negocio.
- Manejar estándares para desarrollar, mantener y documentar los planes de Continuidad del Negocio y los planes de contingencia tecnológica.
- Identificar los procesos críticos del negocio para poder establecer el impacto que tendría la ocurrencia de un desastre o falla sobre ellos.
- Documentar los planes de Continuidad de Negocio y de sistemas.

- Que cada plan de Continuidad del Negocio especifique las condiciones para su activación y las responsabilidades del negocio para cada uno de sus componentes, como así también para las condiciones para su desactivación y vuelta atrás.
- Establecer una lista de todos los recursos críticos de TOC para determinar el nivel de prioridad en el restablecimiento de ellos, es decir, que los recursos más críticos sean recuperados en primera instancia.
- Procedimientos de reanudación que describen las acciones a tomarse para regresar a las operaciones comerciales normales.
- Un programa de mantenimiento que especifica cómo y cuándo se va a probar el plan, y el proceso para mantener el plan.
- Las actividades de educación y capacitación diseñadas para crear el entendimiento de los procesos de Continuidad del Negocio y asegurar que los procesos continúen siendo efectivos.
- Las responsabilidades de las personas, describiendo quién es el responsable de ejecutar cuál componente del plan.
- Definir acciones para mantener y/o restaurar los sistemas y aplicaciones de TOC de forma de asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas (SLA) frente a interrupciones o fallas tecnológicas que afecten al centro de procesamiento de datos.

c) Acciones a implementar por el comité

1. Reunir al comité de continuidad de negocio, dicha reunión puede ser presencial o a distancia, dependiendo de la criticidad del incidente.
2. Establecer responsabilidades y lineamientos para el personal que integra el comité, así como un punto focal de comunicación.
3. Comunicar a los organismos competentes de la situación esto en caso de que aplique.
4. Identificar el alcance e impacto del incidente y tomar las acciones competentes para la remediación del mismo, por ejemplo:
    a. Para casos de no contar con la disposición de algún sistema crítico definido por el negocio, se debe seguir lo establecido en el documento identificado como **Plan sin sistemas**.
    b. En caso de no contar con suministro eléctrico en alguna de las instalaciones críticas definidas por el negocio, se debe realizar lo establecido en el documento identificado como **Plan sin energía eléctrica**.

c. Las acciones a seguir para casos donde no se pueda contar con personal especializado se indican en el documento identificado como **Plan sin personas**.
d. Otro escenario posible es la interrupción del servicio por terremoto, para este caso las acciones a seguir para la continuidad operacional se establecen en el documento **Plan de terremoto**

4. Activación de Planes de Continuidad de Negocios y de Comité de Crisis.

En caso de activación de los planes de continuidad de negocio, se procederá de acuerdo al tipo de contingencia que se materialice (Menor – Moderada – Crisis).

5. Pruebas, mantenimientos y evaluaciones de planes de continuidad.

Las realización de pruebas, mantenimiento y evaluaciones de los planes de continuidad se realizarán a través del archivo llamado **Minuta del Comité de gestión de riesgo, continuidad y seguridad de la información** y será en este documento donde se dejará registrado todo lo conversado en la reunión que se realizará 1 vez por semana.

En el caso de que la incidencia sea puntual se realizará un reunión extraordinaria y se llevará a cabo el registro en el siguiente documento **Minuta del Comité de gestión de RCS**

La gestión de continuidad de TOC incluye:

a) Probar regularmente los planes de Continuidad para asegurar que se mantienen actualizados y son verdaderamente efectivos.

b) Revisar y actualizar al menos una vez al año o cuando ocurran cambios significativos los roles y responsabilidades del personal responsable involucrado en la ejecución de las actividades de recuperación en contingencia.

c) Asegurar que todos los miembros del equipo de recuperación y otro personal relevante estén adecuadamente capacitados en los planes, en su

responsabilidad con la continuidad del negocio y la seguridad de la información, y que conozcan su papel cuando se active el plan.

d) Asegurar que los recursos de hardware y software dispuestos en sitios alternativos de procesamiento u operación se encuentren disponibles en su funcionamiento y debidamente actualizados.

Luego de haber pasado el evento y como una actividad posterior se aplicará el documento **Evaluación plan de continuidad,** con la finalidad de determinar si el plan funcionó como estaba previsto.

En el caso de que no se presente un evento disruptivo, se aplicará el documento **Evaluación plan de contingencia,** con la finalidad de realizar un ensayo o simulacro de un posible evento futuro.