Gestión de la Continuidad del Negocio

Isabel Casares San José-Martí
Secretaria General OCOPEN

Ante las situaciones que estamos viviendo en la actualidad, debemos tener en cuenta que el Gobierno Corporativo y de la Gestión Integral de Riesgos de las empresas deben cumplir con una gestión efectiva del **riesgo operacional** y establecer criterios mínimos para la gestión de la continuidad del negocio, obligándose a reportar eventos de interrupción significativa de las operaciones, y el uso de indicadores clave para supervisar la gestión de la continuidad del negocio, siempre bajo el **principio de proporcionalidad** al tamaño, la naturaleza y la complejidad de sus operaciones.

Los estándares y buenas prácticas internacionales sobre la materia, entre los que se encuentran el estándar **ISO 22301,** sobre los sistemas de gestión de la continuidad del negocio, y la **Guía de Buenas Prácticas del Business Continuity Institute.** Asimismo, la empresa debe contar con un sistema de gestión de la seguridad de la información, orientado a garantizar la integridad, confidencialidad y disponibilidad de su información.

Analizando la terminología común en esta materia destacamos:

- Análisis de impacto del negocio: Proceso mediante el cual se evalúan los efectos de un evento de interrupción del negocio para determinar la prioridad con la que se deben recuperar las actividades de la empresa.
- Impacto máximo aceptable: Nivel máximo de impacto que puede ser aceptado por la empresa ante la ocurrencia de un evento de interrupción del negocio sobre diversos aspectos, tales como financiero, regulatorio, reputacional, sobre el público y el cumplimiento de los objetivos estratégicos.
- Objetivo de recuperación de negocio: Nivel mínimo aceptable de operatividad de los productos y servicios a recuperar luego de una interrupción. Puede ser definido en términos de alguna o la combinación de las siguientes variables: canales de atención, volumen de operaciones, volumen de clientes, montos para la atención de operaciones y horarios de atención.
- Periodo máximo tolerable de interrupción (PMTI): Periodo luego del cual una interrupción alcanza alguno de los niveles de impacto máximos aceptables.
- Punto único de falla: Fuente o camino único de un servicio, actividad y/o proceso para el cual no existe una alternativa y cuya pérdida o falla pueda ocasionar una interrupción.
- Punto objetivo de recuperación (POR): Nivel máximo de información que se podría perder como resultado de una interrupción en los servicios de tecnologías de la información. Se representa en unidades de tiempo.
- Tiempo objetivo de recuperación (TOR): Tiempo establecido por la empresa para reanudar operaciones, en caso de ocurrencia de una interrupción. Es menor al PMTI.

El sistema de gestión de la continuidad del negocio, es el componente de la gestión integral de riesgos que busca asegurar la capacidad de la empresa para continuar operando a niveles previamente establecidos, ante la ocurrencia de una interrupción y abarca, al menos, las siguientes fases:

1. Entendimiento de la organización.
2. Diseño de la estrategia de continuidad.
3. Implementación de la estrategia de continuidad.
4. Plan de pruebas.
5. Capacitación.
6. Revisión y actualización.

Las políticas para la gestión de la continuidad del negocio deben ser aprobadas por el Consejo de Administración, revisadas periódicamente y considerar, al menos:

a) Vinculación a los objetivos estratégicos de la empresa.
b) Proveer un marco para establecer y alcanzar los objetivos de la gestión de la continuidad del negocio.
c) Establecer los impactos máximos aceptables ante la ocurrencia de una interrupción, los cuales deben ser considerados para el análisis de impacto del negocio.

La gestión de la continuidad de negocio puede ser **desempeñada** por una unidad especializada o asignada a otra unidad de la empresa, atendiendo al tamaño, la naturaleza y la complejidad de sus operaciones, estableciendo las siguientes responsabilidades respecto a dicha gestión:

a) Proponer políticas.
b) Desarrollar procedimientos y metodologías apropiados.
c) Apoyar y asistir a las unidades de la empresa en la implementación de las políticas, procedimientos y metodología desarrollados.
d) Asegurar que la gestión se integre a la gestión de riesgos de la empresa.
e) Asegurar que el Consejo de Administración, la gerencia general y el comité de riesgos tomen conocimiento de los aspectos relevantes de la gestión, para una oportuna toma de decisiones.
f) Asegurar que el desarrollo de las actividades referidas a la gestión sea aprobado por las instancias correspondientes.
g) Identificar las necesidades de capacitación y difusión para una adecuada gestión.

1. Entendimiento de la organización

La empresa debe efectuar un análisis de impacto del negocio y una evaluación de riesgos que podrían causar una interrupción del negocio, cuyos resultados deben ser aprobados por **el comité de riesgos e informados al Consejo de Administración**, debiendo incluir:

a) Un inventario de los productos o servicios entregados a personas (físicas o jurídicas) o entes jurídicos, que puedan verse afectados por la interrupción de las actividades de la empresa, incluyendo en dicho inventario a las obligaciones que se mantengan con dichas personas o entes.
b) Una evaluación, a través del tiempo, de los **impactos financiero, regulatorio y reputacional**, en el público y en el cumplimiento de los objetivos estratégicos que podrían generarse como resultado de interrumpir la entrega de los productos y servicios, con el objetivo de determinar el PMTI y el TOR.
c) La definición de los productos y servicios priorizados, en atención al PMTI y TOR correspondientes, así como la identificación de los procesos que los soportan.
d) La estimación de los recursos propios y/o provistos por terceros, necesarios para la ejecución de los productos y servicios priorizados, y que incluyen al personal con capacidades técnicas, los procedimientos, información, tecnología e infraestructura.

La **evaluación de riesgos** que podrían causar una interrupción del negocio debe incluir, al menos:

a) Identificación de los puntos críticos de falla.
b) Escenario en los que los recursos necesarios, propios y/o provistos por terceros, no se encuentren disponibles.
c) La exposición a riesgos relacionada a la ubicación geográfica de sus instalaciones y la de aquellos proveedores cuya falla o indisponibilidad podría afectar la continuidad de las operaciones de la empresa.

Las metodologías para desarrollar el análisis de impacto del negocio y la evaluación de riesgos que podrían causar una interrupción del negocio deben ser consistentes con aquellas usadas para la gestión del riesgo operacional.

2. Diseño de la estrategia de continuidad

La empresa debería diseñar estrategias que permitan asegurar la continuidad en la entrega de los productos y servicios, aprobadas por el Consejo de Administración e incluyendo:

1. La factibilidad técnica, los TORs y los recursos necesarios para su implementación.
2. Un análisis de escenarios que incluya la falla o indisponibilidad de los bienes o servicios brindados por terceros.
3. Contar con más de un centro de procesamiento de datos con perfiles de riesgo distintos, de modo que posibles eventos de interrupción no los afecten de manera simultánea.
4. La información de las operaciones de los productos de inversiones.
5. Las instalaciones destinadas a la recuperación de los procesos que soportan los productos y servicios priorizados deben cumplir con las políticas y los protocolos de seguridad establecidos por la empresa.
6. Contar con un análisis realizado por un tercero independiente y especializado, en donde se analice si los centros de procesamiento de datos se verán o no afectados por un mismo evento de interrupción, considerando la ubicación geográfica, el suelo, la infraestructura y la accesibilidad de cada centro, debiendo actualizarse periódicamente o ante cambios en alguna de las características señaladas.

3. Implementación de la estrategia de continuidad

La empresa debe implementar las estrategias de continuidad aprobadas, desarrollando planes de gestión de crisis, de continuidad de los productos y servicios priorizados, de recuperación de los servicios de tecnología de información y de emergencia.

El plan de gestión de crisis describirá la estructura organizativa y los procedimientos aplicables en situación de crisis, incluyendo:

a) Criterios de activación y desactivación.
b) Conformación del comité de crisis de nivel estratégico.
c) Lineamientos para la toma de decisiones.
d) Roles y responsabilidades durante la crisis.
e) Esquema de comunicación entre los miembros del comité de crisis.
f) Lineamientos para la comunicación con aquellas personas (físicas o jurídicas) y entes jurídicos, que pudieran verse afectados por la interrupción de las actividades de la empresa.

El plan de continuidad de los productos y servicios priorizados describiendo los aspectos necesarios para el despliegue de las estrategias que permitan asegurar la continuidad en la entrega de dichos productos y servicios, y debe incluir lo siguiente:

1. Criterios de activación y desactivación.
2. Roles y responsabilidades de los involucrados.
3. Descripción de los procedimientos y recursos necesarios para recuperar los productos y servicios.
4. Descripción de los procedimientos y recursos necesarios para realizar el retorno a la operación normal de los productos y servicios.

El plan de recuperación de los servicios de tecnología de información (TI) describiendo los aspectos necesarios para el despliegue de las estrategias aprobadas para recuperar los servicios de TI. Dicho plan debe contemplar los siguientes aspectos:

a) Criterios de activación y desactivación.
b) Conformación del equipo a cargo de la recuperación de los servicios de TI, los cuales deben incluir a los proveedores que soporten dichos servicios de TI.
c) Roles y responsabilidades.
d) Descripción de los procedimientos y recursos necesarios para recuperar los servicios de TI.
e) Descripción de los procedimientos y recursos necesarios para realizar el retorno a la operación normal de los servicios de TI.

El plan de emergencia describiendo los aspectos necesarios para salvaguardar la integridad física del personal y público en general en las instalaciones de la empresa.

4. Plan de pruebas de continuidad

Las pruebas de continuidad deben asegurar el cumplimiento de los objetivos de la gestión de la continuidad del negocio. La empresa debe planificar y ejecutar anualmente pruebas de los planes de gestión de crisis, de la continuidad del negocio, de recuperación de los servicios de tecnología de información, y de emergencia.

En caso de contar con múltiples estrategias para asegurar la continuidad de los productos y servicios priorizados, la empresa debe probar todas ellas en un periodo no mayor a tres años y elaborar informes sobre la ejecución de pruebas que incluyan la siguiente información:

- Los objetivos y metas de la prueba.
- Características, alcance y escenario.
- Resultados obtenidos y oportunidades de mejora.
- Planes de acción a implementar.

5. Capacitación y cultura organizacional

La empresa debe asegurar el conocimiento necesario y el compromiso con la gestión de la continuidad del negocio en todos los niveles de la organización, al menos:

a) Diseñando e implementando programas de capacitación dirigidos a los diferentes niveles organizacionales, de acuerdo a las funciones y responsabilidades asignadas dentro del sistema de gestión de la continuidad del negocio.
b) Diseñando y ejecutando actividades que integren la gestión de la continuidad del negocio a la cultura organizacional de la empresa.

6. Revisión y actualización

La empresa debe revisar el sistema de gestión de la continuidad del negocio periódicamente o ante nuevos productos o cambios importantes en el ambiente de negocios, operativo o informático. Para dicho efecto, debe establecer políticas para su revisión periódica y lineamientos que permitan identificar situaciones que ameriten su actualización.

Se debe informar de la ocurrencia de un evento de interrupción significativa de operaciones, en cuanto se tenga conocimiento, entendido como tal el que implique cualquiera de las siguientes situaciones:

a) La suspensión en la entrega de los productos y servicios priorizados por un tiempo mayor a los respectivos TOR.
b) La indisponibilidad del 25% o más de un canal de atención en una determinada región geográfica o a nivel nacional, por un periodo mayor a un número de horas (normalmente cuatro horas) o al TOR definido por la empresa, el que sea menor.
c) La activación del plan de gestión de crisis.