Cómo asegurar la continuidad del negocio en una organización en caso de incidente disruptivo

Ante el incremento de incidentes disruptivos que pueden afectar gravemente a las organizaciones, la gestión de la continuidad del negocio está adquiriendo una relevancia creciente dentro de los planes estratégicos empresariales.

La **gestión de la continuidad del negocio** es un proceso que **ayuda a las organizaciones a identificar las amenazas potenciales y el impacto que podría tener en las funciones críticas del negocio,** y establece un **marco para garantizar que esas operaciones puedan continuar o restablecerse rápidamente** durante y después de un incidente disruptivo.

El lunes, 28 de abril de 2025, se produjo en España un corte de energía sin precedentes, que dio lugar a una crisis nacional, afectando a millones de personas y empresas en todo el país. Horas después del corte de energía, se constató que numerosas empresas —incluidas algunas consideradas “esenciales”— se vieron obligadas a cerrar sus puertas ante la imposibilidad de mantener sus operaciones y servicios. En contraste, otras, como hospitales públicos y privados; ciertos grupos hoteleros, supermercados, centros comerciales, y cierto número de industrias, lograron sostener al menos los servicios mínimos, evidenciando diferencias significativas en su capacidad de respuesta ante la emergencia.

La rápida respuesta y la minimización de interrupciones se lograron gracias a la disponibilidad de generadores y sistemas SAI en múltiples ubicaciones; la certificación ISO 22301, por ejemplo, en numerosos hospitales; la migración de información crítica a la nube con acceso remoto garantizado; y la implantación y revisión periódica de simulacros y planes de crisis que aseguraron una preparación efectiva ante contingencias.

Un sistema y plan de “Continuidad de Negocio (CN)” permite a las empresas anticiparse y responder de manera eficaz a situaciones imprevistas, como un corte prolongado de energía, garantizando la continuidad de las operaciones y servicios esenciales, en esos momentos críticos.

¿Qué se entiende por “continuidad de Negocio”, “Sistema de Gestión de Continuidad de Negocio (SGCN)” y “Plan de Continuidad de Negocio (PCN)?

Según la ISO 22301:2020 (Norma Internacional que establece los requisitos para un Sistema de Gestión de Continuidad del Negocio (SGCN)):

- **“Continuidad de Negocio”** (Business Continuity, BC): Capacidad de una organización para continuar proporcionando productos y servicios dentro de plazos aceptables, con una capacidad predefinida durante una disrupción.

- **"Sistema de Gestión de Continuidad del Negocio"** (Business Continuity Management System, BCMS): Marco de trabajo que ayuda a una organización a identificar las amenazas potenciales, gestionar su impacto y asegurar que puede operar de forma continua, o recuperarse rápidamente, tras un incidente disruptivo.
- Un **"Plan de Continuidad de Negocio"** (Business Continuity Plan, BCP): Consiste en una serie de procedimientos documentados y estrategias destinadas a garantizar que una organización pueda mantener sus operaciones esenciales durante una contingencia y recuperarse cuanto antes, reduciendo las pérdidas que se puedan ocasionar por dicha disrupción.

¿Cómo se ven afectadas las empresas ante un incidente?

Las organizaciones pueden verse afectada, entre otros, por:

- Daños directos o indirectos a los activos.
- Reducción o paralización de la actividad y la consecuente pérdida financiera.
- Dificultad para la recuperación, pudiendo incluso llevar al cese de la actividad.
- Daño a la reputación y pérdida de confianza de los suministradores y los clientes.
- Incumplimiento de regulaciones y, como consecuencia, posibles sanciones.

¿Por qué implantar un Sistema y Plan de Continuidad de Negocio? Objetivo del Plan de Continuidad de Negocio

Entre el objetivo y los beneficios de implantar un **"Sistema de Gestión de Continuidad de Negocio"** se encuentran una mayor resiliencia de la organización, mediante la elaboración y el mantenimiento de planes que aseguren la continuidad de las operaciones críticas; la reducción de las pérdidas económicas y los costos asociados a las interrupciones; la protección de la reputación, manteniendo la confianza de clientes y partes interesadas; ventajas competitivas, ya que permite a la organización destacar frente a la competencia al demostrar su capacidad de gestionar crisis; y cumplimiento normativo que ayuda a cumplir con los requisitos y contratos, evitando penalizaciones.

El **"Plan de Continuidad de Negocio"** no pretende restaurar de inmediato el 100 % de la capacidad productiva y financiera de la empresa. Su **objetivo principal** es **garantizar la supervivencia del negocio en "condiciones mínimas aceptables",** asegurando que las operaciones críticas continúen, y evitando que la organización se vea gravemente comprometida, mientras se encuentra en fase de recuperación de forma gradual.

Componentes claves para la implantación del Sistema y el plan de Gestión de Continuidad del Negocio.

A la hora de implementar un sistema de gestión de continuidad de negocio se proponen 5 fases

principales:

- **Integración** dentro de la organización. Considerar la cultura empresarial, establecer la política de la empresa, alcances, roles asociados al proceso y responsabilidades, autoridades/gobernanza, los objetivos, etc.
- **Análisis y valoración** de los riesgos inherentes a los procesos y organizaciones. Identificación de las posibles amenazas potenciales que podrían interrumpir la actividad de la organización y los posibles impactos.
- **Diseño** de las soluciones según los riesgos encontrados y priorizados. Planificación de la respuesta / Respuesta a incidentes / Recuperación ante desastres.
- **Implementación** de los planes para la reducción de las pérdidas. Formación y concienciación.
- **Validación y mantenimiento** del sistema y el plan de continuidad de negocio Pruebas, validación y mantenimiento.

Existen diferentes enfoques a la hora de implantar el sistema de gestión de continuidad de negocio, entre los que se encuentran la UNE-EN ISO 22313:2020 “Seguridad y resiliencia. Sistemas de gestión de la continuidad del negocio. Directrices para la aplicación de la norma ISO 22301 (Norma Internacional que establece los requisitos para un Sistema de Gestión de Continuidad del Negocio)” y guías de buenas prácticas, cómo, por ejemplo, la guía elaborada por el Instituto de Continuidad de Negocio (Business Continuity Institute (BCI) de Londres).

A continuación, se presenta una tabla general que muestra, a modo de ejemplo, los procedimientos y estrategias que conforman un sistema y plan de gestión de continuidad del negocio:

Tipos de amenazas dentro de una organización y sus posibles impactos

Los tipos de incidentes que pueden afectar a una organización son diversos y deben analizarse individualmente. Este análisis dependerá, entre otros factores, del tipo de actividad, área de negocio/mercado, el tamaño de la empresa, su ubicación geográfica, así como de las características de sus proveedores y clientes.

En general, entre los incidentes que pueden afectar a una empresa se encuentran los siguientes:

- **Incendios**/explosiones/caída de rayos/avería de maquinaria.
- **Desastres naturales,** como terremotos, inundación por fuertes lluvias torrenciales o escorrentías, áreas inundables o próximas a ríos o al mar, granizo, etc.
- **Inestabilidad geopolítica** (conflictos armados, tensiones diplomáticas, cambios abruptos en políticas exteriores, sanciones económicas, o movimientos sociales).
- **Crisis financieras** globales.

- **Interrupciones** del suministro eléctrico durante uno o varios días.
- **Incidentes** de la cadena de suministro: fallos en la cadena de suministro
- **Incidentes** Tecnológicos y Cibernéticos
- **Accidente** laboral, un brote infeccioso o una intoxicación alimentaria de una persona o varias personas con tareas exclusivas.
- **Derivados** de riesgos sociales, como interrupción organizada o deliberada (huelgas, motín), sabotajes, terrorismo, etc.

Desde el punto de vista del "negocio", una vez identificados los incidentes, es conveniente **clasificar** estos en distintos niveles **según su impacto:** aquellos que ocasionan paradas o pérdidas menores, los que generan efectos disruptivos significativos, los que comprometen la continuidad operativa y los que provocan daños de carácter destructivo."

Para ello se utilizan dos técnicas de análisis: el "**Análisis del Impacto del Negocio" (BIA Business Impact Analysis) y la "Valoración del Riesgo" (RA Risk Assesment).**

- El "Análisis del Impacto del Negocio" estima los impactos de la interrupción a lo largo del tiempo para determinar la respuesta de la organización, las prioridades de recuperación y los requisitos de recursos.
- La "Valoración del Riesgo" identifica el nivel de Riesgos de interrupción de las actividades prioritarias de la organización.

El resultado del BIA y el RA se utiliza como input para la fase de diseño de soluciones del BCMS. Por lo tanto, la calidad y los resultados del proceso de BIA y RA y sus resultados son extremadamente importantes.

"Planes de Actuación" frente a una amenaza que pueda afectar a la continuidad de negocio

Los planes de actuación, para el caso de la ocurrencia de un evento disruptivo (amenaza) que afecte a la continuidad del negocio de una empresa u organización, son documentos estratégicos que definen procedimientos, recursos y responsables para reaccionar ante eventos inesperados (daños de los activos, desastres naturales, ciberataques, fallos tecnológicos, crisis reputacionales). Se centran en la respuesta inmediata y en la recuperación rápida para minimizar el impacto en el negocio. Estos planes de actuación dan una respuesta estructurada y evitan la improvisación en momentos críticos en los que se haya producido un evento disruptivo.

Entre los planes de actuación, en caso de un incidente disruptivo que afecte a la continuidad de negocio, se encuentran:

En ocasiones, se habla indistintamente de plan de emergencia (PE), plan de contingencia (PC) y plan de continuidad de negocio (PCN), aunque no son lo mismo. A continuación, se incluye un ejemplo general y simple sobre la diferencia entre ellos.

- **“Plan de emergencia”:** serie de acciones contempladas para reducir o eliminar el incidente.
  Por ejemplo: En caso de incendio del transformador principal de una planta; actuación en la extinción de este mediante medios manuales y/o automáticos para limitar los daños.
- **“Plan de Contingencia”:** acciones específicas para minimizar el impacto de un incidente adverso. Se centra en “qué hacer si ocurre X”.
  Por ejemplo: En caso de incendio del transformador principal de la planta, con los daños totales de este y la consecuente parada parcial o total de la actividad; Reposición del trasformador por uno nuevo y en buen estado. Así se ganarían como mínimo unas horas y como máximo varios días.
- El **“Plan de Continuidad de Negocio”** garantiza que la organización pueda seguir operando (aunque sea parcialmente) durante y después de una incidencia grave. Define cómo mantener servicios los esenciales; incluye estrategias como trabajo remoto, proveedores alternativos, redundancia tecnológica; se activa ante eventos prolongados (desastres naturales, ciberataques, fallos masivos);

Por ejemplo: En caso de incendio del transformador principal de la planta, con los daños totales de este y la consecuente parada parcial o total de la actividad; Plan de continuidad del negocio que contemple la existencia de un transformador de repuesto (plan de contingencia) en buen estado y bien mantenido, que pueda reemplazar al existente, y no afecte a la pérdida de beneficios de la planta.

Conclusión

Disponer de un sistema y un plan de continuidad de negocio es clave para garantizar la resiliencia y estabilidad operativa de una organización. Ambos permiten anticipar riesgos, minimizar el impacto de interrupciones, proteger activos críticos y asegurar la rápida recuperación de servicios esenciales. Esta combinación fortalece la confianza de clientes y socios, cumple con normativas y asegura la competitividad ante cualquier contingencia.

Autoría del texto:

María Teresa Queralt

Ingeniera de Riesgos Senior en MAPFRE Global Risks