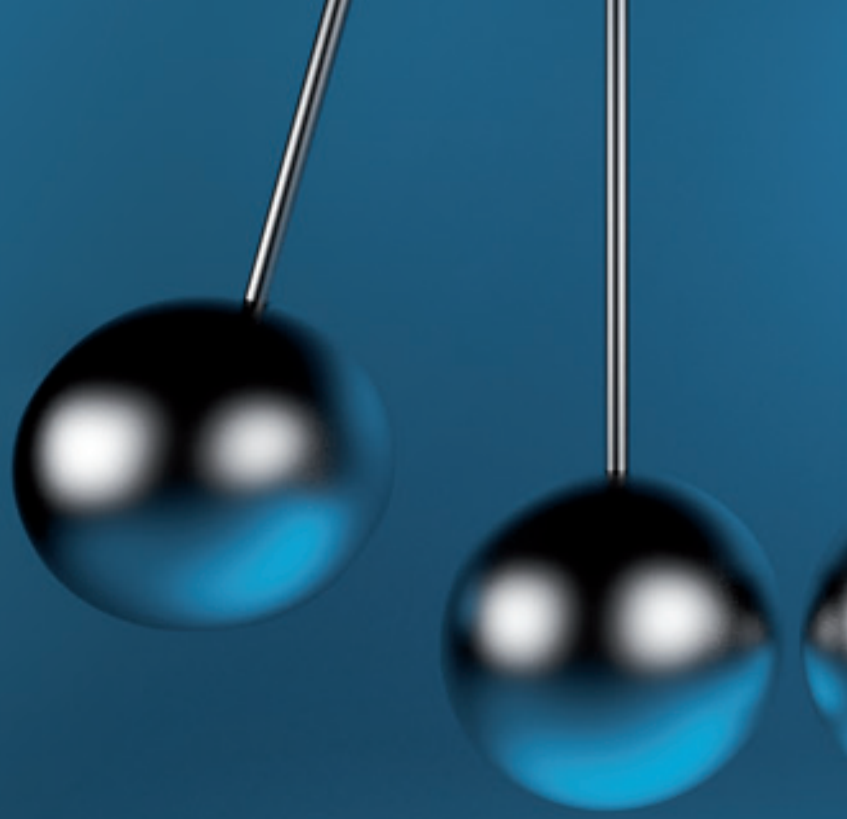
UNE-EN ISO 22301
Y UNE-EN ISO 22313

Según la Cámara de Comercio de Londres, un 43% de las organizaciones después de un accidente no podrán continuar sus operaciones, viéndose obligadas a cerrar. Las Normas UNE-EN ISO 22301 y UNE-EN ISO 22313 especifican los requisitos para implantar con éxito un Sistema de Gestión de Continuidad de Negocio en cualquier tipo de organización. Este sistema permite afrontar y superar, de la mejor manera posible, situaciones de incertidumbre, crisis y cambios que acompañan al entorno actual empresarial.



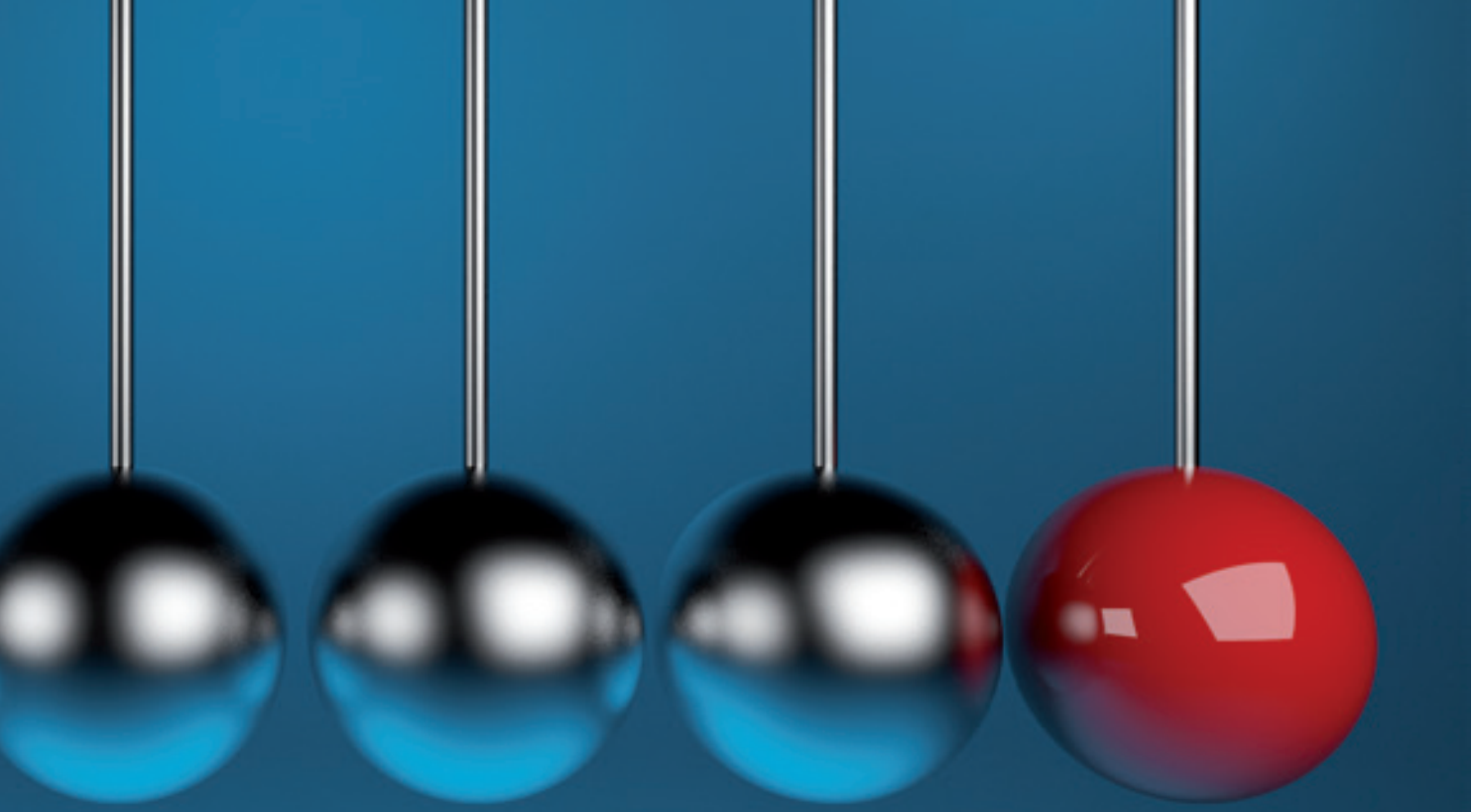
Cómo garantizar la continuidad del negocio

Paloma García y Ana María Mariblanca
Dirección de Normalización AENOR

La continuidad del negocio se ha convertido en un área cada vez más común de preocupación desde el atentado del *World Trade Center* de Nueva York en septiembre de 2011, incidente completamente imprevisto que creó una amenaza grave y repentina para las funciones esenciales de varias empresas. En este sentido, las Normas ISO 22301:2012 *Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Requisitos* e ISO 22313:2012 *Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Directrices* ayudan a las organizaciones a gestionar este aspecto.

Han transcurrido algo más de dos años desde la publicación de estas normas internacionales, durante los que ha ido creciendo su importancia en el ámbito mundial tanto en empresas de Tecnologías de la Información y Comunicaciones (TIC) como en todas aquellas que dependen, en mayor o menor medida, de dichas tecnologías; la banca es un buen ejemplo de ellas. De hecho el Banco de España ya ha emitido varias Recomendaciones relativas a la continuidad del negocio, instando a que ésta debe formar parte de la gestión del riesgo operacional de una entidad de crédito. Este aumento de la concienciación ha derivado en la decisión del comité europeo CEN/TC 391 *Protección y seguridad de los ciudadanos* de adoptar ambas normas ISO como normas europeas. A su vez, todos los organismos nacionales de normalización miembros de CEN las han adoptado en sus países respectivos. Es el caso de España, que ha publicado, en enero de 2015, las Normas UNE-EN ISO 22301 y UNE-EN ISO 22313. Disponer de estas normas en el ámbito europeo y nacional acercará los Sistemas de Gestión de la Continuidad del Negocio (SGCN) a las organizaciones, y en especial a las pymes.

Tradicionalmente, los Planes de Continuidad -que complementan a los antiguos Planes de Contingencia Tecnológica- se han asociado a grandes compañías que necesitan



Disponer de las Normas UNE-EN ISO 22301 y UNE-EN ISO 22313 en el ámbito europeo y nacional acercará los Sistemas de Gestión de la Continuidad del Negocio (SGCN) a las organizaciones, y en especial a las pymes

reaccionar de forma inmediata ante cualquier evento que interrumpa sus servicios. La realidad es que cualquier organización puede sufrir un incidente que afecte a su continuidad y, dependiendo de la forma en que se gestione dicho incidente, las consecuencias pueden ser más o menos graves. Últimamente se ha popularizado el término *resiliencia* para referirse a la capacidad de recuperación ante desastres conseguida por una organización gracias a su SGCN.

No sólo las catástrofes ambientales, tales como incendios o inundaciones, pueden causar daños adversos a una organización. También pueden causar grandes daños incidentes serios de seguridad en los sistemas, como delitos cibernéticos, robo de información sensible, daños en las infraestructuras y en los servicios, o fallos en el suministro eléctrico. Los desastres pueden ocurrir en cualquier momento y sus consecuencias sobre las organizaciones que no tienen un Plan de Continuidad de Negocio pueden llegar a ocasionar incluso el cierre de las mismas.

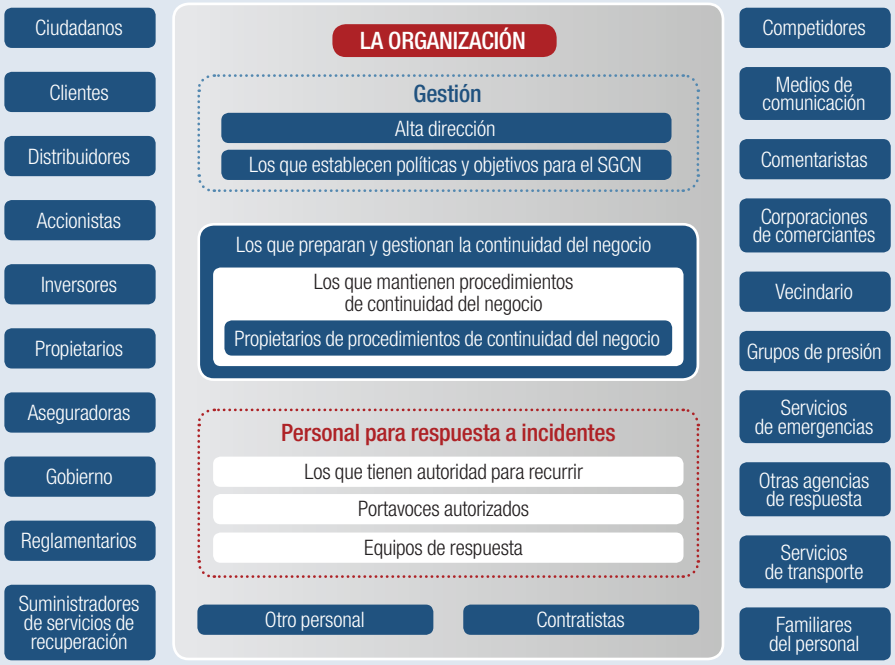
Según la Cámara de Comercio de Londres, un 43% de las organizaciones después de un accidente no podrán continuar sus operaciones, viéndose obligadas a cerrar; el 80% tendrán que hacerlo en menos de 13 meses; un 50% se verán forzadas a cerrar antes de cinco años después del desastre y un 53% de los clientes de estas organizaciones no recuperarán las pérdidas causadas por los daños derivados. Aunque los efectos inmediatos parecen ser la pérdida de beneficios, hay otros efectos derivados que pueden causar un gran impacto en la compañía. Es el caso del impacto en la reputación o la pérdida de ventaja competitiva frente a otras compañías.

Pero no hay que centrarse exclusivamente en el sector TIC. Cualquier organización, independientemente de su dimensión y el sector al que pertenezca, encontrará valor en la implantación y mantenimiento de un SGCN. Cualquier negocio, y cualquier área dentro de él, puede ser objeto de aplicación de un SGCN, desglosando adecuadamente las actividades y estudiando su implantación a cada una de las partes y a todo el conjunto. Por ejemplo, en el área de Recursos Humanos, podrían identificarse varias actividades como administración de personal, gestión de nóminas, control de presencia, etc.; y en ventas, la comercialización de productos, gestión de impagos, facturación, etc.

Para desarrollar todo el potencial que proponen estas nuevas normas en la mejora de procesos de una organización, es preciso no quedarse solamente en los impactos de tipo operativo. Es decir, en aquellas actividades para las que resulta relativamente sencilla la evaluación de los costes económicos causados por la interrupción de sus actividades, bien sean directos, como el coste de las horas de trabajo perdidas por los empleados, o indirectos. Se

Figura 1

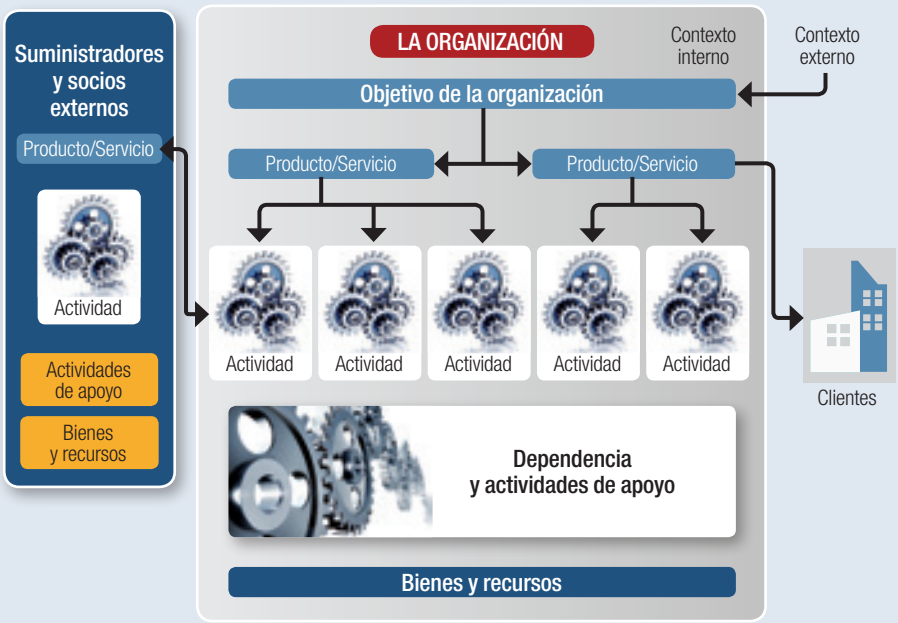
Ejemplos de partes interesadas que hay que considerar en sectores públicos y privados



Fuente: Figura 4 (Norma UNE-EN ISO 22313: 2015)

Figura 2

Entendimiento de la organización



Fuente: Figura 6 (Norma UNE-EN ISO 22313:2015)

deben tener en cuenta otros impactos que no hay que minusvalorar, como los legales o contractuales, y otros más intangibles como la imagen y reputación. Estos impactos pueden tener consecuencias a largo plazo mucho mayores que las pérdidas inmediatas causadas por una interrupción.

Cada una de las partes que conforman el modelo "Planificar-Hacer-Verificar-Actuar" son indispensables para garantizar la eficacia de un SGCN.

Planificar

Para una planificación óptima, es esencial el entendimiento de la organización y de su contexto, de las necesidades y expectativas de las partes interesadas. Así, podrá tomarse una decisión razonada sobre el campo de aplicación del SGCN; esto es, qué partes de la organización deben incluirse en el sistema.

Otro pilar de la planificación es la implicación de la alta dirección, que debe asegurar que se establecen los objetivos de continuidad del negocio y se comunican a las funciones y niveles aplicables. Estos objetivos de continuidad deben ser coherentes con la política de continuidad de negocio, teniendo en cuenta el nivel mínimo de productos y servicios que es aceptable para que la organización consiga sus objetivos; deben ser mensurables, y estar supervisados y actualizados según sea apropiado.

Hacer

Se trata de establecer criterios para los procesos, realizar el control de procesos de acuerdo con los criterios y mantener la información documentada para tener la seguridad de que los procesos se realizan según lo planificado. Esta información debe incluir los requisitos legales, las prioridades de los tratamientos de riesgos, el resultado del análisis de impacto en el negocio y de la apreciación del riesgo, y los requisitos de actualización y de confidencialidad de esta información.

CURSOS DE AENOR RELACIONADOS

- Fundamentos de continuidad según la Norma ISO 22301
- Implantación de un SGCN según la Norma ISO 22301
- Auditoría de la Norma ISO 22301

Verificar

Los dos primeros vértices del cuadrado PDCA no tienen sentido sin la supervisión de lo que se ha planificado e implantado. La organización debe determinar qué se debe supervisar y medir, los métodos y plazos que deben preverse para ello, y los análisis y evaluaciones. Cuando sea necesario debe actuar para solventar los resultados adversos antes de que se produzca una no conformidad y conservar la información documentada como evidencia. En última instancia, la verificación es responsabilidad de la alta dirección.

Actuar

Está íntimamente relacionado con la mejora continua. La organización debe mejorar de manera continua la idoneidad, adecuación y eficacia del SGCN, utilizando para ello procesos del propio sistema como el de liderazgo, planificación o evaluación del rendimiento.

El modelo PDCA descrito en detalle en la Norma UNE-EN ISO 22301 se apoya en la UNE-EN ISO 22313, que proporciona directrices sobre los requisitos especificados en la primera. De hecho, su estructura editorial es idéntica, presentando los mismos encabezados, pero sin repetir los requisitos, términos y definiciones. En el capítulo 4 sobre la *Planificación*, se incluye una figura que abarca todas las posibles partes interesadas (ver figura 1)

En el capítulo 8, que se corresponde con "Hacer" del modelo PDCA, se muestra una figura sobre el entendimiento de la organización, que puede ayudar al análisis de impacto en el negocio y la valoración del riesgo. (Ver figura 2). En el mismo capítulo se trata la estrategia de continuidad del negocio y posibles acciones para determinarla, protegiendo las actividades prioritarias, estabilizando, continuando, reanudando las mismas, y mitigando, respondiendo y gestionando los impactos. Así, ambas normas utilizadas como un tándem proporcionan un marco sólido para la puesta en marcha y correcta implantación de un SGCN.

El modelo de Gestión de la Continuidad del Negocio está alineado con otros como el de Seguridad de la información (UNE-ISO/IEC 27001), Gestión del Servicio de TI (UNE-ISO/IEC 20000-1) o Gestión de la Calidad (UNE-EN ISO 9001) con el objeto de facilitar la consistencia necesaria y permitir la sinergia en la implantación y operación de cada aspecto degestión. Concretamente, la Norma UNE-ISO/IEC 27001 contempla la continuidad del negocio como un elemento clave dentro de la gestión de la seguridad de la información. ◗

OPINIÓN

César Pérez-Chirinos
Presidente
AEN/CTN 196/SC 1

La resiliencia no se improvisa

Las fuertes nevadas que interrumpieron en enero y febrero la vida cotidiana en la zona norte de España, aislando pueblos durante varios días, deberían servir para entender la importancia de una gestión integral de la capacidad de reanudación de suministros y servicios imprescindibles.

Aunque otros acontecimientos crean la apariencia de que las mayores amenazas a la protección de los ciudadanos provengan de acciones deliberadas de gran impacto (terrorismo y sabotaje informático), lo cierto es que lo que ahora denominamos "continuidad de negocio" tiene mucho más que ver con lo que históricamente se ha venido denominando en España "protección civil" y la capacidad de reanudar el abastecimiento de recursos vitales ante cualquier interrupción circunstancial.

Esta capacidad de reanudación (que ahora se denomina *resiliencia*) no se puede improvisar. Requiere que las organizaciones proveedoras se doten de medios alternativos que sustituyan a los que habitualmente proporcionan estos suministros o servicios y que puedan haberse perdido, temporal o definitivamente, ante circunstancias extraordinarias. Además, deben comprobar regularmente que estos medios alternativos están listos para ser utilizados en cualquier momento bajo la dirección de los equipos de gestión de crisis encargados de reanudar los suministros o servicios interrumpidos; posiblemente, en coordinación con las autoridades e, incluso, con competidores en circunstancias normales pero que son los únicos que pueden aportar medios muy especializados ante un incidente grave.

La privatización de muchos suministros y servicios esenciales para la población hace imprescindible la existencia de sistemas de gestión de la continuidad de negocio, potencialmente auditables por terceros independientes, tanto en el ámbito público como en la empresa privada, que garanticen que los proveedores más *resilientes* no son injustamente comparados con otros que, ante circunstancias excepcionales, no tienen la misma capacidad de compromiso con sus beneficiarios o clientes.