ISOTools EXCELLENCE

La norma ISO 22301

Cómo asegurar la continuidad del negocio

Índice

1. El Sistema de Gestión de la Continuidad del Negocio

¿En qué consiste un Sistema de Gestión la Continuidad del Negocio?

Disponer de un Sistema de Gestión de la Continuidad del Negocio (SGCN) **se ha convertido en toda una exigencia para las organizaciones** puesto que, en un entorno cada vez más globalizado y exigente, ninguna empresa que pretenda mantener su ventaja competitiva **puede permitirse el lujo de tener interrupciones considerables en su cadena de producción o de negocio.**

Con las nuevas reglas de los mercados internacionales, las empresas tienen la obligación de poder demostrar que son proveedores en los que se puede confiar. Ante la presencia de cualquier evento alterador, disponer de un SGCN bien diseñado y correctamente implantado es una garantía, para la propia empresa y ante terceros, de que dentro de un tiempo estimado, **la organización podrá reanudar sus operaciones y servicios.**

Un SGCN consiste en la **preparación proactiva de la organización frente a contingencias de todo tipo** que puedan suponer una interrupción de la actividad de una empresa, suponiendo **perjuicios de diferente gravedad** según la importancia del ámbito donde se ha producido el paro y el tiempo de inactividad.

El SGCN puede considerarse, por lo tanto, como l**a capacidad estratégica y táctica de una organización para planificar y responder ante incidentes o interrupciones de negocio**, con el fin de continuar las operaciones a un nivel aceptable de servicio, que debe definirse previamente.

En los casos más graves, la interrupción de la continuidad del negocio **puede suponer la propia desaparición de la empresa**, al producirse daños irreparables, pérdidas económicas inasumibles o la imposibilidad de hacer frente a pedidos o compromisos claves con los clientes.

EL PRINCIPAL OBJETIVO DE UN SGCN ES PERMITIR LA ADMINISTRACIÓN, PLANIFICACIÓN, SEGUIMIENTO, CONTROL Y MEJORAMIENTO PERMANENTE DE LA ESTRATEGIA DE CONTINUIDAD DEL NEGOCIO DE LA COMPAÑÍA PARA GARANTIZAR SU OPERACIÓN CRÍTICA EN CASO DE UNA CONTINGENCIA.

¿Principales beneficios de un SGCN?

- Garantizar el cumplimiento de los objetivos prioritarios del negocio en caso de contingencia.
- Brindar seguridad y confianza a las partes interesadas.
- Reducir los efectos adversos en los servicios de la organización por una interrupción inesperada.
- Identificar amenazas y vulnerabilidades sobre las operaciones críticas de la compañía, para su tratamiento y control de manera proactiva.
- Integrar la estandarización, innovación y el liderazgo en la gestión del riesgo operativo.
- Reducir al mínimo las posibilidades de que una contingencia llegue a provocar que la empresa deje de operar el tiempo suficiente como para que no pueda suministrar a tiempo sus productos o servicios.

El estándar ISO 22301:2012

Un SGCN se basa en la **norma ISO 22301**, la cual **enfatiza ciertos aspectos de la organización y de la sustentabilidad** del negocio como: la información, las aplicaciones informáticas, las cuestiones financieras, contables y legales, así como también los procesos productivos y operativos.

Se trata de una norma **enfocada en la organización general de las empresas**, cuyo fin es determinar los requisitos necesarios para la implementación de controles que ayuden a evitar o minimizar las amenazas y sus consecuencias. El segundo punto es establecer o analizar las causas que han motivado este problema.

El estándar ISO 22301:2012, cuya denominación completa es "Seguridad de la Sociedad: Sistemas de Continuidad del Negocio-Requisitos" aplica el ciclo Plan-Do-Check-Act (PDCA por sus siglas en inglés), cuyo fin es la **mejora continua de la calidad** en los distintos aspectos o fases del programa:

- **Planificación.**
- **Establecimiento.**
- **Implementación.**
- **Operación.**
- **Monitoreo.**
- **Revisión.**
- **Mantenimiento.**

LA ISO 22301:2012 ESTÁ MUY RELACIONADA CON OTROS ESTÁNDARES DE GESTIÓN COMO: ISO 9001, ISO 27001, ISO 20000-1, ISO 14001 E ISO 28000.

2. La metodología AMEF

Muchos SGCN, sobre todos los implantados por organizaciones del sector industrial, **se basan en el Análisis del Modo y Efectos de Fallo (AMEF)**, que es una herramienta que permite determinar acciones de prevención a partir de la identificación de riesgos en el análisis de potenciales fallas en: productos, servicios, procesos o sistemas, con el fin de establecer los controles adecuados que eviten la ocurrencia de las mismas.

Con el AMEF es posible reconocer o identificar errores o fallas potenciales, principalmente en los procesos de producción, con el propósito de eliminarlos o de minimizar el riesgo asociado a las mismas.

Principales beneficios del AMEF

Los beneficios de la implantación del AMEF en un sistema son:

- Identificar fallas o defectos antes de que estos ocurran.
- Incrementar la confiabilidad de los productos/servicios.
- Conseguir procesos de desarrollo más cortos.
- Documentar los conocimientos sobre los procesos.
- Incrementar la satisfacción del cliente.
- Mantener el Know-How en la compañía.

Además de estudiar e identificar los posibles fallos que puedan comprometer la continuidad de una cadena de producción o de un negocio, mediante el AMEF lo que se hace es **clasificar esos riesgos según su importancia**.

A partir de ahí, es posible obtener una lista detallada que servirá **para priorizar cuáles son los modos de fallo más relevantes** que son importante solventar por uno o varios de los siguientes motivos:

- Son los errores más peligrosos para la continuidad de los procesos productivos.
- Pueden resultar muy molestos o perjudiciales para terceros: clientes, proveedores y otros grupos de interés.
- Tienen muchas posibilidades de que se produzcan, es decir, su frecuencia es alta.

EL AMEF ES UN MÉTODO DE ANÁLISIS MUY VERSÁTIL, LO QUE PERMITE APLICARLO EN DISTINTOS SECTORES Y EN TODO TIPO DE PROCESOS PRODUCTIVOS, OPERATIVOS U ORGANIZACIONALES.

Etapas del análisis AMEF

Los **pasos para realizar un análisis AMEF** son los siguientes:

1. Crear un grupo de trabajo

El primer paso consiste en crear un grupo de trabajo de 4 ó 5 personas que tengan conocimientos sobre el producto, servicio o proceso que se está desarrollando. Lo ideal es que el equipo sea multidisciplinar y que incluya varios perfiles diferentes.

2. Enumerar los posibles fallos

La principal función de este equipo es enumerar todos los posibles fallos que pueden llegar a comprometer la fluidez y el funcionamiento normal de un determinado proceso de producción.

3. Establecer un índice de prioridad

Tras detectar las posibles incidencias detectadas, estas deben ser clasificadas según su importancia. Un posible modelo de clasificación en el siguiente:

Nivel de Severidad	A cada incidencia detectada se le asigna un valor entre 1 y 10
Nivel de Incidencia	A cada incidencia detectada se le asigna un valor entre 1 y 10
Nivel de Detección	A cada incidencia detectada se le asigna un valor entre 1 y 10
Se puede obtener un valor entre 1y 100 siguiendo la siguiente fórmula: NPR=S*0*D	

El objetivo final del análisis AMFE es que tengamos todos los posibles fallos controlados, habiendo actuado para disminuir el NPR de los más graves.

3. El plan de contingencia. Los tiempos de recuperación

El plan de contingencia se enmarca dentro del plan de riesgo de la organización y, siguiendo los requisitos de la norma ISO 22301**, se implementa mediante un ciclo de mejora continua basado en un modelo PDCA.**

Elementos del plan de contingencia

Los principales elementos que debe tener un plan de contingencia son los siguientes:

Definición de las situaciones críticas

Es importante definir los activos críticos y la relación de procesos de negocio que afecten a esos activos previamente identificados.

Asignación de responsabilidades

Se deben crear grupos humanos configurados por personal competente como el comité de emergencia, el cual se encargará de ejecutar los procedimientos adecuados en el caso de que se produzca una situación crítica.

Determinar las acciones de respuesta

Esta fase del plan implica tener muy bien definida una hoja de ruta con las siguientes acciones a llevar a cabo:

- Indicadores que marcarán el inicio del plan de contingencia.
- Secuencias de acciones que hay que llevar a cabo en el orden preciso.
- Indicadores que permiten considerar que la situación ha quedado normalizada.
- Determinación de los registros y documentación necesaria para dejar constancia por escrito de las acciones que se han llevado a cabo.

Mantenimiento del plan

Es necesaria la obtención de datos de ejecución del plan con el fin de actualizarse y mejorarse para incrementar su eficiencia en futuras ejecuciones.

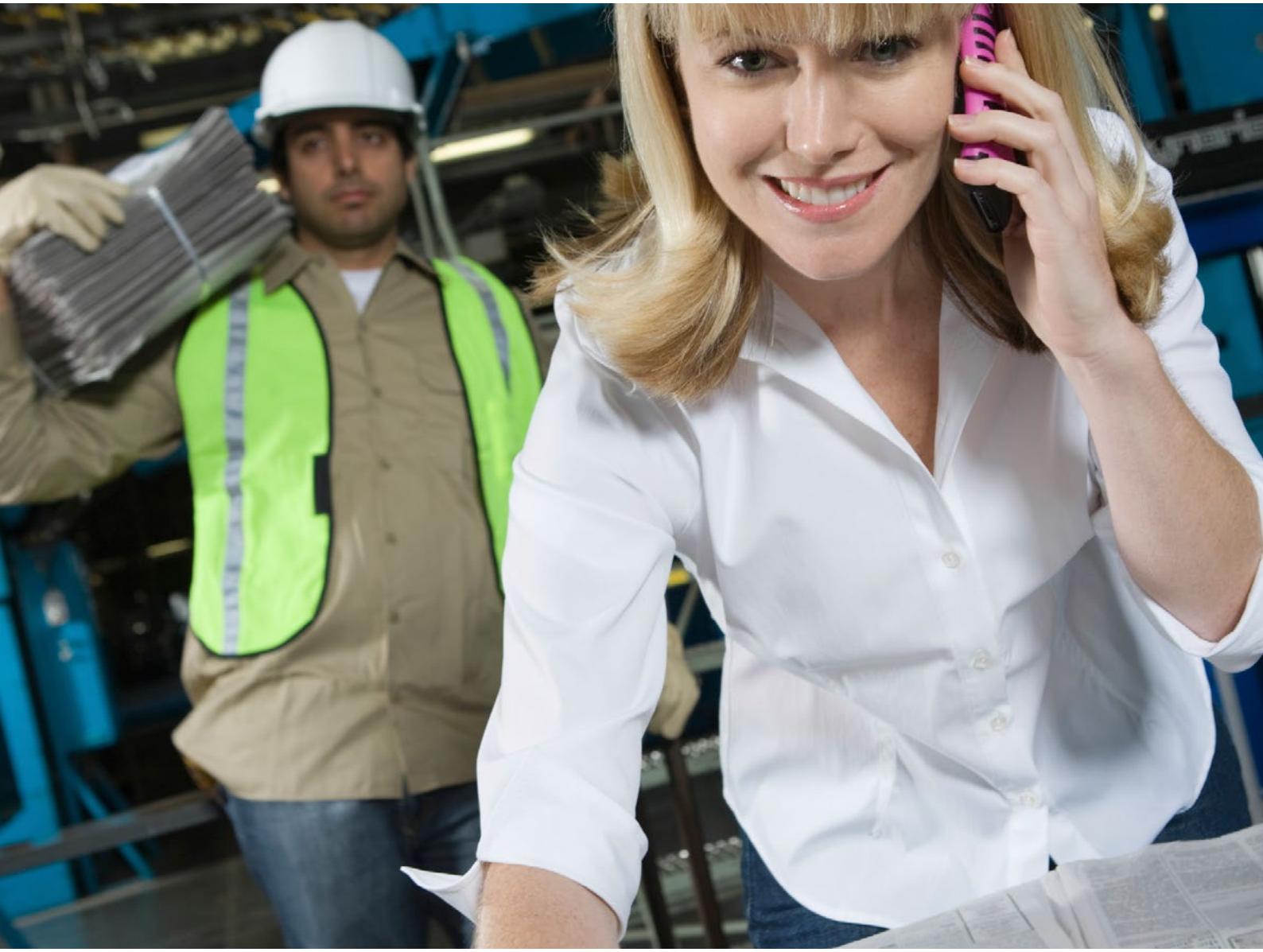
Un **plan de contingencia** suficiente elaborado **permite retomar las actividades dentro de unos tiempos de recuperación adecuados,** previamente definidos.

Esto permite volver a la actividad normal en un tiempo prudencial, antes que se produzcan pérdidas de consideración, una cuestión que no tienen en cuenta ni prevén otros estándares y normas diferentes a la ISO 22301.

PARA QUE PUEDA CALIFICARSE DE SUFICIENTEMENTE ÓPTIMO Y EFECTIVO, UN PLAN DE CONTINGENCIA DEBE OFRECER RESPUESTAS A LA PREGUNTA: ¿QUÉ HACES PARA REVERTIR LA SITUACIÓN DE CRISIS UNA VEZ PRODUCIDA?

Características de los **tiempos de recuperación**:

- ✔ Se deben conocer y definir con exactitud antes de elaborar el plan de contingencia.
- ✔ Los tiempos de recuperación deben encuadrarse en unos mínimos aceptables para poder reanudar la actividad dentro de unos márgenes que impidan que la empresa sufra daños económicos o de logística irreparables o muy importantes.



4. Implantación, mantenimiento y certificación

La ISO 22301 establece como continuidad del negocio la capacidad de la organización para continuar con **la entrega de productos o servicios a unos niveles aceptables.**

Para lograr este objetivo, se hace necesario **implantar una SGCN donde se definan los riesgos y se diseñe un plan de contingencia** en situaciones de crisis que permita, una vez ha tenido lugar un evento negativo, poder restablecer la actividad en el menor tiempo posible, de manera que las pérdidas y riesgos para la empresa sean lo mínimos.

Fases de la implementación de un SGCN

Desde el diseño de la estrategia a la ejecución de un plan de continuidad del negocio definido en un SGCN, y tomando como base el estándar ISO 22301:2012, la implantación y certificación del mismo es un proceso dividido en las siguientes partes:

1) Definición y gestión del riesgo

Se trata de un requisito previo que consiste en la **identificación de los activos críticos y de los riesgos asociados**.

2) Análisis de impacto

Es una de las partes más importantes del proceso y, básicamente, se trata **de relacionar los procesos de negocio identificados con los impactos que se prevé podría provocar una eventual interrupción de cada uno de ellos.**

Para realizar este proceso suele ser necesario llevar a cabo entrevistas en profundidad con profesionales expertos en cada actividad o sector.

Resulta conveniente realizar una **clasificación de los impactos** según su gravedad:

- **Impactos críticos.** Son aquellas interrupciones que pueden provocar un costo no asumible por la organización.
- **Impactos vitales.** Se trata de impactos graves que afectan a procesos importantes, aunque no llegan al nivel de imprescindibilidad de los críticos por existir alternativas paralelas para mantener un cierto nivel de actividad.
- **Impactos sensibles.** Afectaciones sobre procesos que pueden ser desviados o integrados en otros procesos sin que sea necesarios restablecerlos a corto plazo.
- **Impactos no críticos.** Eventos que afectan a actividades de importancia menor, por lo que no suponen un costo elevado para la empresa en el caso de que se interrrumpan.

En el análisis de riesgos es importante detallar:

- El objetivo.
- El alcance.
- La descripción de las situaciones a controlar.

Por otro lado, dicho análisis debe permitir la **definición de los contextos de la evaluación**, así como también los criterios y la evaluación del impacto potencial en relación a un determinado incidente. Otros aspectos a determinar en el análisis son: los requerimientos, legales, contractuales y estatutarios.

EN LO QUE RESPECTA A LA EVALUACIÓN DEL RIESGO, LA ORGANIZACIÓN DEBE IDENTIFICAR Y PRIORIZAR LOS RIESGOS DE EJECUCIÓN, ANALIZAR EL RIESGO DE UNA FORMA SISTEMÁTICA, ASÍ COMO EVALUAR LAS INTERRUPCIONES QUE REQUIEREN TRATAMIENTO.

3) Desarrollo del plan de acción

En primer lugar, se debe realizar una **invocación por parte de la Dirección de las acciones que deben activarse** para continuar con la actividad.

A partir de aquí, ya puede **definirse la estrategia más adecuada** para restablecer la situación al punto de partida, es decir, que el tiempo que pasa desde el inicio del incidente hasta que se recupere la actividad normal sea el mínimo posible.

Una vez tenemos la estrategia, el siguiente paso consiste en **concretar las acciones que sean necesarias** para recuperar la operatividad normal de la organización, con todos los procesos y circuitos funcionando a un nivel óptimo.

Por último, se deben **realizar una serie de ensayos o pruebas** con el fin de garantizar que estas acciones van a funcionar correctamente y cumplirán su objetivo en el momento de ponerlas en práctica en una situación real.

En el plan de acción o plan de contingencias debe constar:

- Los riesgos a controlar y la acción de reposición asociada a cada riesgo.
- Activos involucrados.
- Nivel de servicio exigido.
- Tiempo de respuesta.
- Recursos necesarios.
- Procedimientos y responsables.

ESQUEMA DE PASOS A EJECUTAR UNA VEZ SE HA PRODUCIDO LA INCIDENCIA
1) Restitución de activos, suministros y entorno
2) Arranque de los sistemas y servicios
3) Pruebas de comprobación de los sistemas restaurados
4) Puesta en operación
5) Retirada de los planes de respaldo
6) Registro de las acciones y sus resultados

En cuanto a los **procedimientos utilizados** para poner en marcha las acciones preventivas y activas para asegurar la continuidad del negocio, **la norma ISO 22301 determina los siguientes requisitos**:

- Se deben establecer y documentar los protocolos de comunicación necesarios.
- Los procedimientos han de tener una cierta flexibilidad en lo que respecta a las respuestas.
- Se debe incidir directamente en aquellos procedimientos que sean más críticos en las operaciones.
- Ha de procurarse la disposición de todos los recursos necesarios para ejecutar todas las acciones, tanto preventivas como de reposición de la actividad, una vez se haya producido la interrupción.
- Orientación a la detección de incidentes.
- Disponer de procesos de activación, operación, coordinación y comunicación de respuestas.
- En todo momento debe haber un flujo de comunicación constante.

Por otra parte, la respuesta planteada por los procedimientos se regirán por la **siguiente estructura:**

- ✔ Identificación de los impactos que justifiquen el inicio del plan.
- ✔ Evaluación de la naturaleza y el alcance de un evento dañino.
- ✔ Inicio de las respuestas apropiadas.
- ✔ Establecimiento de un flujo de comunicación con cualquier parte interesada.

4) Monitorización, análisis y evaluación

Deben determinarse los objetivos y herramientas de monitorización, medición, análisis y evaluación, así como los periodos de desempeño y ejecución. Dicha monitorización debe estar basada en métricas que sirvan para evaluar, entre otros, los siguientes factores:

- Desempeño de los procesos.
- Conformidad de los estándares internacionales.
- Registro de los datos obtenidos.

La evaluación se debe llevar a cabo mediante **auditorías internas y auditorías externas.**

Auditorías internas

Las auditorías internas han de estar supervisadas por la Dirección o Gerencia de la organización, y su principal cometido es determinar la conformidad del SGCN con los requerimientos de la organización y de los estándares internacionales, en especial la norma ISO 22301.

A través de estas auditorías y revisiones periódicas, la organización puede lograr **los siguientes beneficios**:

- Comprobar si la estrategia definida es realmente eficaz para garantizar la continuidad del negocio.
- Implantar las correcciones precisas y necesarias para mejorar el alcance y la efectividad del SGCN.
- Comprobar y actualizar los diversos aspectos del SGCN: evaluación de riesgos, análisis del impacto, planes de continuidad y procedimientos relacionados.
- Mejorar la monitorización de todo lo relacionado con el SGCN.

Si se descubre una disconformidad relevante entre los objetivos definidos y la situación real en relación a los planes de acción relativos a la continuidad del negocio, deben **llevarse a cabo los siguientes pasos**:

1. Identificación de la disconformidad.
2. Evaluar la necesidad de poner en macha acciones correctivas.
3. Ejecución de dichas acciones.
4. Revisión de la efectividad de las acciones.
5. Hacer los cambios que sean necesarios en el SGCN.

Auditorías externas

La ISO 22301 es una norma certificable, lo que implica realizar auditorías externas por parte de una empresa autorizada, revisables periódicamente, con el fin de **conseguir y mantener dicha certificación.**

La certificación sirve para demostrar a los clientes, proveedores y partes interesadas que **nuestra empresa considera prioritario proteger los procesos esenciales** que permitan, en todo momento, proveer de los productos o servicios necesarios a sus clientes.

Otras consideraciones del SGCN

El contexto de la organización

La versión del 2012 de la ISO 22301 introduce, en su cláusula número 4, los requerimientos precisos para **establecer el contexto del SGCN a las necesidades de la organización dentro de un alcance determinado**, incluyendo los aspectos legales y regulatorios que se apliquen a la misma.

La ISO 22301 requiere que la organización determine qué será cubierto por la continuidad del negocio y, por el contrario, qué será excluido. Por otro lado, a la organización se le exige que comunique a las partes, tanto internas como externas, el alcance del SGCN.

La cuestión del liderazgo

El estándar de continuidad del negocio es **muy exigente con el rol de la Dirección**, atribuyéndole funciones como:

- Asegurarse que el SGCN es compatible con la dirección estratégica de la organización.

- Integrar los requerimientos del SGCN en los procesos de negocio.
- Comunicar a los empleados y todas las partes interesadas la importancia de una eficaz gestión de la continuidad del negocio.

La planeación

En la cláusula 6 de la ISO 22301:2012 se requiere que la organización defina claramente los objetivos de continuidad del negocio y desarrolle los proyectos adecuados para alcanzarlos.

Dichos objetivos, además de estar relacionados con la política de continuidad del negocio, deben ser conmensurables.

Soporte y documentación

Como toda norma perteneciente a la familia ISO, la norma 22301 otorga una **gran importancia a la gestión documentaria.**

La documentación obligatoria exigida por el estándar ISO 22301:2012 es la siguiente:

1	Lista de requisitos legales, normativos y de otra índole
2	Alcance del SGCN
3	Política de continuidad del negocio
4	Objetivos de la continuidad del negocio
5	Evidencia de competencias del personal
6	Registros de comunicación con las partes interesadas
7	Análisis del impacto en el negocio
8	Evaluación de riesgos, incluido un perfil de riesgo
9	Estructura de respuesta a incidentes
10	Planes de continuidad del negocio
11	Procedimientos de recuperación
12	Resultados de acciones preventivas
13	Resultados de supervisión y medición
14	Resultados de auditoría interna
15	Resultados de la revisión por parte de la Dirección
16	Resultados de acciones correctivas

Simulacros y planes de emergencia

Es necesario también **realizar simulacros y planes con el fin de contemplar las consecuencias de cualquier índole** (costos económicos, problemas de logística) y las mejores acciones para mitigar los riesgos y restablecer la situación ante contingencias de todo tipo. Por ejemplo: un incendio, averías importantes en la maquinaria, una epidemia de gripe o, incluso, que abandone la empresa una profesional importante para la organización y con un perfil difícil de reemplazar.

A través de estos simulacros es posible conocer con exactitud, por ejemplo, cuánto pueden tardar los bomberos ante una llamada de emergencia o el tiempo que se tarda en derivar la energía eléctrica a un generador de emergencia en caso de corte de fluido eléctrico.

El posterior análisis de los resultados del simulacro permite prever **cuáles son las consecuencias asociadas a un determinado evento** pero, sobre todo, posibilita poner en marcha correcciones y acciones de mejora.

5. Objetivos mínimos de la continuidad del negocio (OMCN)

Es fundamental que en el propio SGCN se defina **nivel mínimo de la prestación de servicio o de la producción que es aceptable para que la organización** no entre en quiebra (o tenga unas pérdidas muy importantes) durante la interrupción.

Al establecer los objetivos, se debe **considerar el nivel mínimo de productos y servicios para que la organización pueda alcanzar sus objetivos globales de negocio.**

En la cláusula 8.2.2 del estándar ISO 22301:2012 se define el término “esquemas de tiempo priorizados”, que está relacionado con el OMCN y define el orden y los tiempos para la recuperación de actividades críticas que soportan los productos y servicios claves.

6. Período Máximo Tolerable de Interrupción (MPTB)

En este caso se pretende identificar el **tiempo límite que una empresa puede estar sin el funcionamiento de una maquinaria determinada**, porque en este caso el riesgo operacional se dispara y se puede dar una situación de quiebra técnica. Es decir, se establece un máximo de tiempo para poner en marcha el plan de contingencia.

Este término está definido en las sección 3 del estándar y, aunque no es usado en la norma, la cláusula 8.2.2 (c) plantea que la «organización debe establecer esquemas de tiempo priorizados para reanudar operaciones que apoyan los productos y servicios claves, en un nivel específico aceptables, tomando en consideración el tiempo en el cual, los impactos, de no reanudar operaciones, se convertirían en inaceptables».

7. Objetivo de Tiempo de Recuperación (RTO)

El RTO es el periodo de tiempo seguido tras un incidente dentro del cual la actividad o recursos deben ser reasumida. Está ligado con el tiempo de recuperación y se trata de un tiempo menor que **el tiempo máximo tolerable en el cual se debe restablecer el plan de contingencia para asumir el producto o servicio dentro de la maquinaria.**

Está ligado también al objetivo mínimo de la continuidad del negocio, ya que uno depende directamente del otro

8. Objetivo de Punto de Recuperación (OPT)

Es el punto en que los recursos (humanos, tecnológicos, logísticos...) han quedado restaurados y, por lo tanto se permite la actividad. Es un concepto también muy ligado tanto al período máximo tolerable y al tiempo de recuperación.

9. Cómo automatizar el Sistema de Gestión de Continuidad del Negocio según ISO 22301

En la gestión de la continuidad del negocio, donde el **factor tiempo es absolutamente clave**, resulta fundamental disponer de un **software de automatización** para poder llevar a cabo una **gestión eficaz y exhaustiva de cualquier tipo de riesgo que pueda poner en peligro el funcionamiento normal y fluido de la organización.**

En el caso de catástrofes naturales (inundaciones, atascos, terremotos, epidemias...), acontecidos en la última década, la experiencia ha demostrado que las empresas que han sido capaces de reanudar antes su actividad, con el mínimo de pérdidas posibles, han sido aquellas que tenían implantados **sistemas automatizados de recuperación de información.**

Otro motivo para implantar este sistema es el de la **disponibilidad del personal que tiene que realizar las tareas de recuperación.** En situaciones de desastres naturales, es común que el personal no llegue a tiempo a los centros de trabajo bien por quedar atrapada en los atascos, por la indisponibilidad de trasporte público, etc.

ACTUALMENTE, NO RESULTA OPERATIVO NI EFICAZ DEPENDER DE MANUALES NI EXCESIVA INFORMACIÓN EN PAPEL PARA CONSULTAR PROCESOS HUMANOS NI TECNOLÓGICOS

Algunos **aspectos a tener en cuenta** en este tipo de herramientas que facilitan la **automatización de la gestión de riesgos** son:

- Poner en marcha procesos de identificación automática de los riesgos para la continuidad del negocio a los que está expuesto cada organización.
- Alinear cada riesgo con acciones concretas enmarcadas en un plan de contingencia para eliminar o reducir las pérdidas.
- Poner en marcha un sistema automático del seguimiento del tratamiento de riesgos.
- Realizar simulacros y simulaciones que permitan visualizar los resultados que se podrían obtener con la implantación de las acciones definidas en el plan de contingencia para la continuidad del negocio.
- Se debe tener prevista la posibilidad de fallos en los servidores y aplicaciones informáticas, incluso las que operan en la nube, puesto que por mucho nivel de protección que queramos tener, siempre están sujetas a posibles fallos e indisponibilidades. Por este motivo, el plan de continuidad para las Tecnologías de la Información debe de ser mixto, donde se contemple la copia de seguridad de nuestros servidores virtuales.
- Un buen plan de continuidad, sin duda será imperfecto si no realizamos pruebas de su funcionamiento. Este factor es uno de los más críticos a la hora de enfrentarnos a un sistema que realmente responda cuando lo necesitemos. Las pruebas además de ser planificadas con periodicidades adecuadas, deben contemplar aspectos de fiabilidad en la conmutación a los sistemas de copia de seguridad que nos garanticen la continuidad de los trabajos críticos.
- Es aconsejable plantear una deslocalización de los centros de datos. El primer consejo es establecer una distancia razonable entre la producción y los sitios de recuperación con el fin de mantenerse alejado de los problemas regionales. Sin embargo, muchas pequeñas y medianas empresas poseen un solo centro de datos, por lo que es aconsejable que negocien con sus proveedores de servicios en la nube para disponer de una opción de respaldo en una instalación remota.

- Es fundamental establecer prioridades e implementar una solución económicamente viable, analizando los procesos del negocio en profundidad y establecer cuáles son aquellas aplicaciones que necesitan estar disponibles de inmediato y cuáles pueden esperar unas horas.
- Plantearse la continuidad del negocio podría ser considerado como un servicio más dentro de todos los demás que componen la cartera de Servicios TI. Para ello, debemos aprovechar la experiencia en la selección de proveedores de TI, para seleccionar los sistemas que nos ayudarán en la recuperación ante interrupciones del servicio.

Finalmente, señalar que un óptimo sistema de tratamiento de riesgos debe permitir el **desarrollo del ciclo completo**, es decir: identificación, análisis y evaluación de riesgos, así como la integración y futuras actualizaciones con otras normas ISO.

Software para ISO 22301

La **Plataforma Tecnológica ISOTools** facilita la **implementación**, **automatización** y **mantenimiento** del SGCN según **ISO22301**.

Bajo un enfoque por procesos conforme al **ciclo PHVA (Planear – Hacer – Verificar – Actuar)**, ISOTools permite a las organizaciones estar preparadas ante posibles incidentes tecnológicos, naturales, o de cualquier otra naturaleza que puedan poner en riesgo la continuidad de su actividad.

ISOTools garantiza la **continuidad de negocio**, ya que identifica y gestiona fácilmente los riesgos, disminuyendo así los tiempos de inactividad, la probabilidad de ocurrencia y costos, de este modo la organización está preparada para actuar en caso de que se sucedan.

Este software permite la integración del estándar **ISO 22301** con otras normas, tales como ISO 9001, ISO 14001 y OHSAS 18001, de forma sencilla gracias a su estructura modular.


ISOTools
EXCELLENCE