

Continu  
negocio



 **cero**

Guía para gestionar un plan  
de continuidad de negocio,  
según la **ISO 22301**





<b><u>01</u></b>	¿Qué es la continuidad de la información?.....	4
<b><u>02</u></b>	Gestión de la continuidad de negocio .....	6
<b><u>03</u></b>	Tipos de proyectos de continuidad.....	8
<b><u>04</u></b>	Norma ISO 22301.....	9
<b><u>05</u></b>	Plan de continuidad de negocio, según la ISO 22301.....	15

# 01 Introducción

Cuando hablamos de continuidad de negocio nos referimos a la capacidad que tienen las empresas para sobrevivir ante un riesgo que se pueda presentar de manera interna o externa, afectando el normal desarrollo de las actividades. Sin embargo, las compañías deben tener la habilidad para reaccionar de manera inmediata frente a una amenaza y continuar prestando sus servicios de manera “habitual” con el fin de evitar la interrupción y el desarrollo normal de sus labores cotidianas.

La ISO 22301 reúne todos los requisitos para llevar a cabo la correcta y adecuada implementación de un Sistema de Gestión de Continuidad de Negocio, el cual deberá **identificar las capacidades que tiene una organización para enfrentar algún tipo de incidente** que se pueda presentar y, además, ofrece diferentes claves que permiten mejorar el negocio internamente y realizar una correcta planificación para garantizar la continuidad de este.

En el siguiente eBook usted encontrará los **parámetros que debe seguir para implementar de manera adecuada un plan de continuidad de negocio** que se ajuste a su organización teniendo en cuenta sus objetivos, estructura y alcance. También la importancia de implementarlo y cuál es la forma correcta para hacerlo.

# 01 ¿Qué es continuidad de negocio?

"La gestión de la continuidad de negocio (GCN) busca **sostener en niveles previamente definidos y aceptados, los productos y servicios críticos del negocio** a través de la estructuración de procedimientos, tecnología e información, los cuales son desarrollados, compilados y mantenidos en preparación para su uso durante y después de una interrupción o desastre, con el fin de proteger los intereses de las partes interesadas, la reputación, las finanzas, los activos críticos y otros aspectos generadores de valor". Así lo da a entender Rodrigo Ferrer, en su documento "Metodología para la Gestión de la Continuidad del Negocio", publicado en 2015.

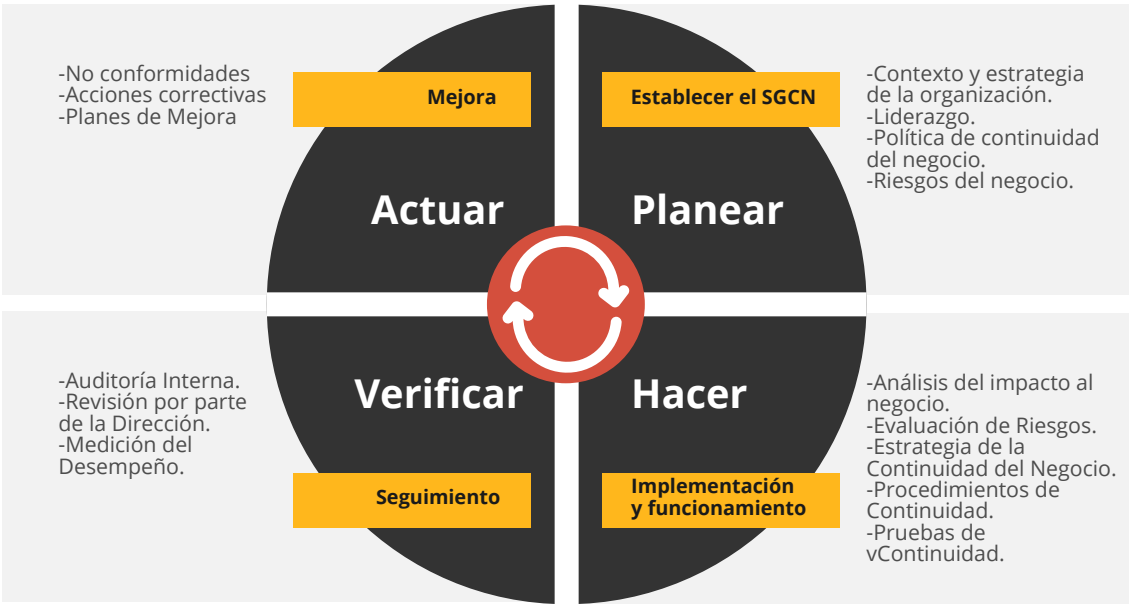
Es un concepto el cual está relacionado con la **planeación para sobrevivir ante un desastre o riesgo** materializado y a su vez con la planeación para restablecer las actividades de la compañía.

Esto se puede definir como la manera más adecuada de **actuar de manera rápida y eficaz ante una eventualidad** que pone en riesgo la operación normal de las actividades de la compañía, a través de un plan establecido para reanudar el funcionamiento cotidiano.

Cabe resaltar, que en muchas ocasiones no se tiene control de estos riesgos por lo que la empresa puede ser afectada de forma substancial.

Ninguna entidad, sin importar su tamaño u origen está **exenta de sufrir este tipo de amenazas** y de acuerdo a la forma en que se gestione el riesgo puede desarrollar consecuencias mayores o menores.

Es importante tener en cuenta que no se debe relacionar con el plan de prevención de pérdidas, ya que para este se necesitan registrar las actividades que se van a llevar a cabo a través de sistemas, **autenticación, seguridad y control para poder identificar la magnitud de lo que se extravió.**



Fuente: Inteli

## 02 Gestión de continuidad de negocio

Se desarrolla en seis etapas que explicaremos a continuación:

### **Etapas 1**

**Creación del programa de BCM:** aquí se debe elaborar el programa de gestión de continuidad, en el que se debe tener cuenta el tamaño y complejidad de la organización, a su vez se elegirán los responsables, quienes estarán a cargo y se les designará su función.

### **Etapas 2**

**Comprensión de la compañía:** se recolecta la información necesaria, con el fin de darle importancia a cada una de las actividades las cuales deben ser clasificadas en clave, de apoyo y a su vez designar los recursos que se necesitan. Se realiza la evaluación del impacto del negocio y de los riesgos.

### **Etapas 3**

**Definición de estrategias:** se seleccionan aquellas actividades que permiten que la organización pueda recuperar su servicio en cierto tiempo determinado en caso de sufrir algún tipo de incidente.

## **Etapas**

### **Etapas 4**

**Elaboración y ejecución de una respuesta:** se redactarán las respuesta que se darán frente alguna amenaza que se pueda presentar. Este contará con un paso a paso que se deberá poner en práctica para actuar de manera correcta y siguiendo los protocolos establecidos.

### **Etapas 5**

**Cumplir los acuerdos pactados en el BCM:** en esta etapa se le da relevancia a las estrategias y planes definidos con el fin de cumplir el propósito por el que se implementó el sistema. Se llevará a cabo a través de ejercicios en diferentes momentos que permitan evaluar la continuidad de negocio y a su vez tener la oportunidad de mejora.

### **Etapas 6**

**Cultura organizacional:** todos los empleados y miembros de la organización deben estar alineados con el sistema de gestión de continuidad de negocio, entender que esto hace parte de la compañía y que de ellos también depende su buen funcionamiento, se debe incluir dentro de los valores para que ellos sientan y entiendan esta relación.

## **03 Tipos de proyectos de continuidad**

### **Plan de continuidad de negocio (PCN)**

Se tienen en cuenta sus diferentes frentes como: infraestructura, recurso humano, sistemas industriales, estrategias de comunicación y tecnología, es importante que cada uno de ellos cuente con un plan de acción en caso de que se llegue a presentar una amenaza.

### **Plan de continuidad TIC**

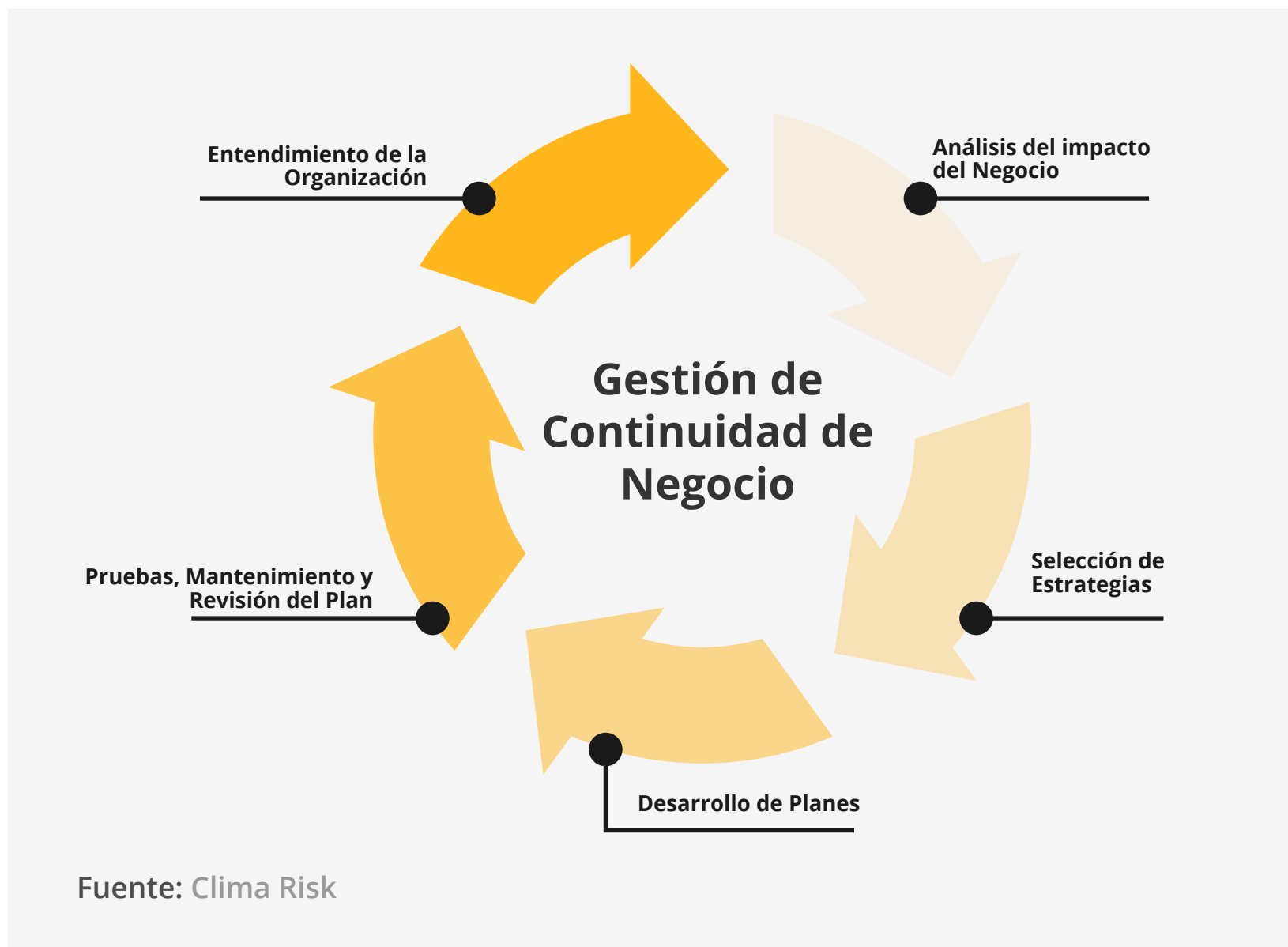
Este se enfoca únicamente a riesgos tecnológicos que puedan traer grandes pérdidas o afectar de manera directa a la empresa.

### **Plan de recuperación ante desastres (PRD)**

Este se relaciona ante posibles catástrofes que se puedan dar.



## 04 Norma ISO 22301



Es una normativa creada por la Organización Internacional de Normalización (ISO), la cual **brinda buenas prácticas y formas para llevar a cabo la gestión de la continuidad de negocio**, con el fin de minimizar los impactos que pueden traer la materialización de un riesgo afectando de manera directa a la institución.

Este estándar internacional está basado en la norma británica **BS 25999, la cual fue sustituida en mayo del 2012 por la ISO 22301**. En la actualidad tiene 109 requisitos los cuales marcan las pautas de cómo se debe llevar a cabo la implementación del Sistema de Seguridad de la Información (SGCN).

Además, brinda los elementos claves para que todos los miembros pertenecientes a la institución estén preparados y sepan cómo actuar en caso de verse enfrentados a este tipo de situaciones cumpliendo con las políticas internas y regulaciones.

La ISO 22301 ofrece un **marco básico el cual permite que se pueda continuar trabajando durante una eventualidad de riesgo** o inesperada, velando por la seguridad de sus empleados, infraestructura y evitando que la reputación se vea afectada hasta el punto de crear una crisis interna y externa.

También hay que tener en cuenta que la ISO 22301 otorga certificación permitiendo que la entidad pueda **demostrarle a sus clientes, empleados y proveedores que están blindados frente a este tema**.

### **Lo que permite:**

- Establecer, implementar, continuar y mejorar el SGCN.
- Tener una relación acorde con la política de continuidad de negocio de la firma.
- Generar conformidad con lo que se está llevando a cabo.
- Esta norma es certificable.
- Hacer la auditoría de conformidad de la ISO 22301.

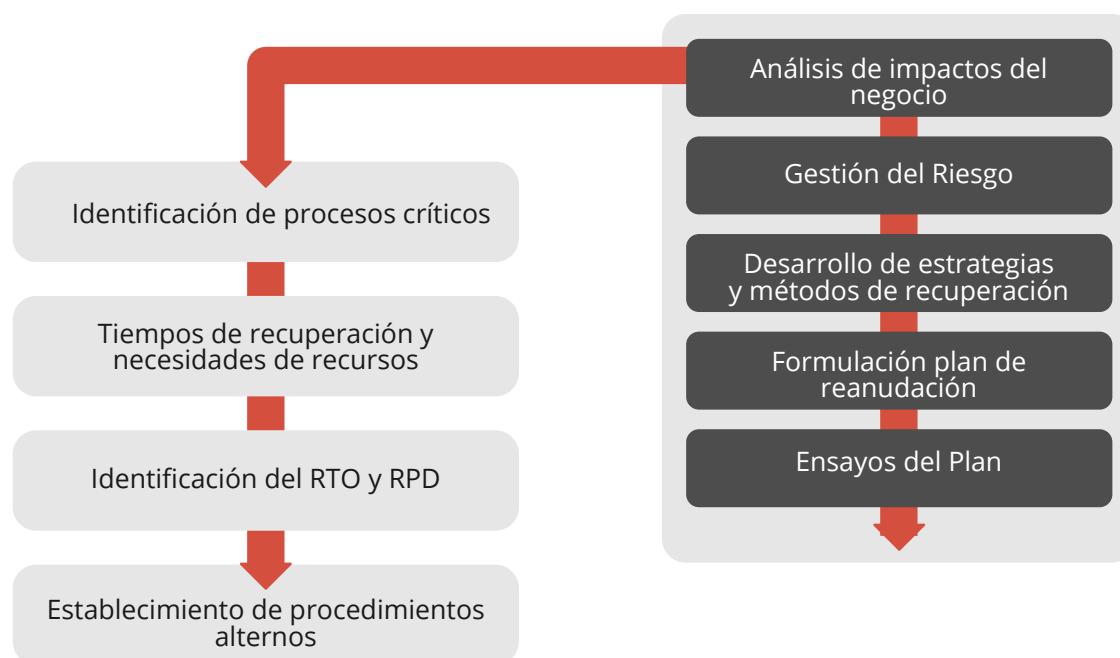
## Los beneficios que ofrece son:

- Permite la coordinación entre los empleados.
- Se puede identificar los riesgos a los que puede estar expuesta la compañía y de qué manera pueden afectar la continuidad de la empresa.
- Contar con las respuestas adecuadas al momento de enfrentar una crisis.
- Tener la capacidad para recuperarse rápidamente.
- Contribuye a mejorar la reputación.
- Valor agregado frente a la competencia.
- Generar confianza antes los clientes y nuevos prospectos.

## Información que se debe documentar

- El alcance.
- La lista de requisitos legales, normativos y de otra índole.
- Política de la continuidad de negocio.
- Objetivos de la continuidad del negocio.
- Competencias del personal.
- Comunicación con las partes interesadas.
- Análisis del impacto en el negocio.
- Evaluar el riesgo.
- Estructura de la respuesta ante incidentes.
- Planes de continuidad del negocio.
- Procedimientos de recuperación.
- Resultados de acciones preventivas.
- Auditoría interna.
- Revisión de la dirección.
- Acciones correctivas.
- Mejora continua.

## Estructura



Fuente: Blog de Consultores

**Se encuentra conformada por diez secciones las cuales están divididas en:**

- Introducción
  - Alcance.
  - Referencias.
  - Normativas.
  - Términos de definiciones.
  - Requisitos de la norma:
- **Contexto:** identificar el alcance del SGCN y verificar si está cumpliendo con los objetivos planteados.
  - **Liderazgo:** las directivas deben involucrar a los miembros de la compañía y estar llevando a cabo actividades que generen compromiso por parte de todos.
  - **Planificación:** se definen los objetivos y de qué manera se llevará a cabo la implementación del SGCN.



- **Apoyo:** tener todas las herramientas necesarias para permitir su ejecución y al personal competente para realizar el plan de acción.
- **Funcionamiento:** una vez se defina y se capacite se debe llevar a cabo su funcionalidad.
- **Evaluación:** realizar auditorías periódicas que permitan verificar si el SGCN está siendo eficiente y si se requieren de mejoras.
- **Mejora:** se pueden identificar si en ciertas etapas se pueden realizar cambios que traigan resultados positivos.

## Certificación

Obtener la certificación permite que cualquier empresa mejore la forma en cómo gestiona este tipo de riesgo y lo pueda hacer por medio de un sistema internacionalmente aceptado el cual permite actuar de manera eficiente ante una situación o evento de amenaza.

### Los pasos que se debe seguir son:

- Preauditoría.
- Auditoría.
- Certificación.

## Beneficios:

- Generar la cultura de continuidad de negocio dentro de la compañía.
- **Brindar confianza a todas las partes relacionadas** de la empresa como clientes, proveedores, prestadores de servicio y empleados acerca de la adopción de medidas internacionales que garantizan el buen funcionamiento del negocio.
- **Establecer indicadores medibles** que permitirán alcanzar los objetivos propuestos.
- Identificar de mejor manera los riesgos y oportunidades a los que se enfrenta la institución.
- Reducción de costos.
- Protección de todos los activos.
- Blindarse de pérdidas monumentales.
- Evitar propagar una crisis y mala reputación.

## 05 Plan de continuidad de negocio, según la ISO 22301

En ocasiones algunas empresas a lo largo del desarrollo de sus actividades, se han visto enfrentadas en sufrir situaciones que pueden poner en peligro la permanencia de la compañía como tal. Para evitar este tipo de amenazas, en la actualidad, **las organizaciones están implementando el Sistema de Gestión de Continuidad de Negocio** basado en la normativa ISO 22301.

### ¿Qué es?

Es un plan que se diseña con el fin de **mantener la operación normal de la compañía** en caso de que se presente alguna eventualidad que pueda afectar de manera directa o indirecta las actividades cotidianas.

Gracias a esto las empresas pueden contar con **planes de contingencia** que contribuyen a mitigar los riesgos y el impacto dentro de la compañía.

## ¿Para qué sirve?

Este tipo de sistemas le dan la **posibilidad a las entidades de que puedan restablecer sus operaciones** luego de sufrir un incidente, el cual haya ocasionado problemas en el desarrollo de las actividades cotidianas. Además, contribuye en la protección de la reputación de la institución, prevención en pérdidas económicas, servicio al cliente y cumplimiento de plazos.

Por otro lado, también **permiten que se anticipen a los riesgos a los que están expuestos**, pues ayuda a que se puedan preparar planes en caso de sufrir una emergencia catastrófica, y cómo actuar frente a la crisis.

## ¿Cómo se ejecuta?



Fuente: Ficohsa



## Fases de un plan de continuidad de negocio

### 1. Determinación del alcance

Se debe clasificar cada una de las áreas dándole una clasificación de prioridad a cada una de ellas, con el fin de entender cuáles son las más vulnerables y de esta manera poder ir trabajando en la continuidad de la organización, en este punto es clave la participación de la dirección.

### 2. Análisis de la empresa

Se debe recoger toda la información de la organización con el fin de identificar cuáles son los procesos de negocios críticos (activos), cómo se les dará soporte y cuáles son las necesidades que se presentan.

### 3. Determinación de la estrategia

Una vez estén definidos los activos se debe establecer que si en caso de que se llegue a presentar una amenaza están en la capacidad de recuperar estos activos en corto plazo, si por el contrario requiere de un tiempo mayor se deben establecer estrategias.

### 4. Respuesta a la contingencia

Se elegirán las estrategias necesarias que se podrán en marcha en caso de presentarse un desastre y se creará un plan de crisis en donde se documentará toda la información.

## 5. Pruebas, mantenimiento y revisión

En este punto es demasiado importante contar con recursos tecnológicos que permitirán crear planes de prueba, mantenimiento y revisión, para identificar cuáles son las buenas prácticas y en qué se debe mejorar.

## 6. Concienciación

Se debe crear una cultura dentro de la organización para que todos los empleados conozcan el plan de acción y se apropien de la situación, al igual que entiendan cuál será su rol dentro de este plan.

### Ventajas

- Mantener el nivel de servicio en límites predefinidos.
- Establecer un periodo de recuperación.
- Determinar la capacidad que puede tener la empresa en caso de materializarse un riesgo de alto impacto.
- Mitigar permanentemente el riesgo de interrupción de servicios.
- Administrar una eventual crisis, protegiendo principalmente la integridad de las personas y activos de la empresa.
- En caso de crisis garantizar un efectivo flujo de las comunicaciones internas y externas.
- Garantizar el principio de la “empresa en marcha” logrando la recuperación de la operación crítica en el menor tiempo posible.
- Minimizar las pérdidas - contener el impacto y minimizar la probabilidad de cometer errores.