**PLAN DE CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN DE DESASTRES**

[Plan de continuidad del Negocio 2](#_Toc5280453)

[¿Qué es y por qué necesitamos un plan de continuidad del negocio? 2](#_Toc5280454)

[Tipos de eventos que debemos considerar en nuestros Planes de Continuidad de Negocio 2](#_Toc5280455)

[Eventos No intencionados 2](#_Toc5280456)

[Eventos intencionados 2](#_Toc5280457)

[Eventos catastróficos 2](#_Toc5280458)

[Eventos Biológicos 2](#_Toc5280459)

[Como elaborar un Plan de contingencias y Recuperación de Desastres 3](#_Toc5280460)

[Etapas fundamentales de un Plan de Contingencias 3](#_Toc5280461)

[Definición general del plan. 3](#_Toc5280462)

[Determinación de vulnerabilidades 3](#_Toc5280463)

[Selección de los recursos alternativos. 4](#_Toc5280464)

[Preparación detallada del plan 5](#_Toc5280465)

[Pruebas y mantenimiento 5](#_Toc5280466)

[Conclusiones Generales 5](#_Toc5280467)

# Plan de continuidad del Negocio

## ¿Qué es y por qué necesitamos un plan de continuidad del negocio?

Continuidad de negocio es el término que se acuña para referirse a las **estrategias y planificación mediante las cuales las organizaciones se preparan para dar respuesta a eventos catastróficos** tales como incendios, inundaciones, ataques cibernéticos, accidentes o errores humanos.1

# Tipos de eventos que debemos considerar en nuestros Planes de Continuidad de Negocio

## Eventos No intencionados

* Errores u omisiones.
* Fallas propias del equipamiento

## Eventos intencionados

* Actos desleales
* Intrusiones
* Omisiones maliciosas
* Daños
* Huelga

## Eventos catastróficos

* Incendios
* Inundaciones
* Fallos eléctricos
* Terremotos

## Eventos Biológicos

* Pandemias
* Intoxicaciones

# Como elaborar un Plan de contingencias y Recuperación de Desastres

## Etapas fundamentales de un Plan de Contingencias

### Definición general del plan.

En esta etapa los altos responsables del organismo deben establecer: quiénes, y cómo, deben elaborar el plan, implementarlo, probarlo y mantenerlo; qué acontecimientos debe contemplar y dónde se debe desarrollar el plan. Los aspectos principales de esta etapa son

### Determinación de vulnerabilidades

**Marco del plan**

* ¿Debe limitarse a los equipos centrales?
* ¿Debe incluir los equipos departamentales, PC's y LAN's?
* ¿Qué procesos son, estratégicamente, más importantes?
* ¿Quiénes deben componer el equipo de desarrollo del plan?
* ¿Quién será el responsable de este equipo?
* ¿Cómo se relacionarán con el resto de la institución?
* ¿Qué nivel de autonomía tendrá el equipo?
* ¿A quién reportará?

**Apoyo institucional**

Un alto responsable (idealmente el máximo) de la institución remitirá una circular a todos los departamentos involucrados, comunicándoles el proyecto y su importancia estratégica para el organismo. Asimismo, debe instar su total colaboración e informarles de su responsabilidad en la elaboración del mismo.

**Presupuesto**

Debe prever los gastos asociados con:

* La adquisición del paquete informático, o contratación de la empresa de servicios, para la elaboración del proyecto.
* Reuniones, viajes, formación del personal.
* Costos del personal que constituye el equipo de elaboración del plan.
* Almacenamiento externo y transporte de los soportes de respaldo de la información.
* Adquisición o contratación de equipos.

El propósito es obtener información de las consecuencias, de todo tipo, que tendría la ocurrencia de un siniestro.

**Identificación de aplicaciones críticas**

Se determinarán las aplicaciones críticas priorizándolas en orden de importancia. Se obtendrá así un listado en el que las aplicaciones más vitales, que ocuparán los primeros lugares de la lista, serán las que se deban recuperar primero, y siempre en el orden de aparición.

**Identificación de recursos**

Se especificarán los recursos de los que dependen las aplicaciones críticas. Estos recursos serán: equipo lógico de base, equipos físicos, de comunicaciones, etc.

**Período máximo de recuperación**

¿Qué significan los términos **RTO y RPO**?

El término **RPO** (Recovery Point Objetive o Punto de recuperación objetivo) se refiere al tiempo que transcurre entre el momento del desastre y el último punto de restauración de nuestros datos, es decir, la cantidad de datos que nuestra empresa va a perder en caso de que se produzca un fallo del sistema.

El término **RTO** (Recovery Time Objetive) tiene que ver con el tiempo de recuperación. Es decir, el tiempo que estamos dispuestos a asumir entre la caída del sistema o la pérdida de datos, hasta que dicho sistema ha sido levantado de nuevo o bien, se han recuperado los datos eliminados.

**Conclusiones de RPO y RTO**

Es necesario definir correctamente ambos términos a la hora de redactar nuestro plan de continuidad del negocio, de manera que la empresa tenga siempre presente ambos factores y con este conocimiento, establecer la política de seguridad y la inversión correspondiente. Cuanto menores queremos que sean ambos factores, mayor será la inversión que tenga que hacer nuestra empresa, pero tengamos en cuenta que cualquier empresa, sin datos... está perdida...4

### Selección de los recursos alternativos.

Es deseable contar con recursos alternativos para garantizar la continuidad del negocio o la rápida recuperación de un desastre. Aunque lo deseable en general diste de ser la realidad, se puede enumerar recursos que podrían ser de utilidad a la hora de prevenir o solucionar un evento no deseado:

* Operar en contingencia en otro centro de cómputos
* Duplicidad de la información
* Alta disponibilidad para resguardo y recuperación
* Sistemas de provisión alternativos de servicios(agua, luz, gas, internet)

### Preparación detallada del plan

Incluye la documentación de las acciones a tomar, los actores a involucrar, los recursos a emplear, procedimientos a seguir, etc. en un formato adecuado para su uso en situaciones críticas. Esta documentación debe estar disponible en varios lugares accesibles inmediatamente. Dicho documento de ser comprensible para el lector y carecer de ambigüedades.

### Pruebas y mantenimiento

Es muy importante y sirve para garantizar que dicho plan no sea una mera tarea costosa y académica. Las pruebas del plan tienen como objetivo garantizar el correcto funcionamiento y verificar su eficacia a la hora de responder a los eventos que pretende evitar o resolver.

El mantenimiento tiene como objetivo mantenerlo actualizado, incorporando todos los cambios que suceden en la organización que tengan relevancia en el plan y su ámbito de acción.

# Conclusiones Generales

Elaborar un plan de Continuidad del negocio, contingencias y recuperación de desastres es una tarea compleja, costosa y sumamente importante para toda organización. De su correcto diseño, implementación y probada eficacia dependen que una Organización puede sortear un evento no deseado pero potencialmente pasible de ocurrir.

La inversión asociada a su elaboración es directamente proporcional a los costos asociados a contar o no con dichos recursos o activos.

Referencias bibliográficas:

1. [www.iso.org](http://www.iso.org)