Planes de continuidad de negocio

Daniel Cruz Allende

PID_00177813

Universitat Oberta de Catalunya
www.uoc.edu

Índice

Introducción..... 5

Objetivos..... 7

1. Planes de continuidad de negocio..... 9

2. Enfoques en los planes de continuidad de negocio..... 12

3. Plan de continuidad de negocio..... 14
3.1. Elementos de los planes de continuidad de negocio 15
3.1.1. Definición de las situaciones críticas 15
3.1.2. Asignación de responsabilidades 15
3.1.3. Definición de las acciones de respuesta 16
3.1.4. Mantenimiento 16

4. Fases de los planes de continuidad de negocio..... 18
4.1. Fase I 18
4.1.1. Gestión de riesgos 19
4.1.2. Business Impact Analysis (BIA) 19
4.1.3. Desarrollo de la estrategia del plan de continuidad de negocio 21
4.2. Fase II 24
4.3. Fase III 24

5. Estructura de los planes de continuidad de negocio..... 25
5.1. Objetivo 26
5.2. Alcance 27
5.3. Descripción de la situación que se debe controlar 27
5.4. Listado de procedimientos concretos y sus responsables 28
5.5. Disparo de alarma 28
5.6. Plan de respuesta 29
5.7. Plan de respaldo 30
5.8. Plan de recuperación 30
5.9. Plan de análisis y mejora 31
5.10. Planes de prueba 32
5.11. Resumen de las relaciones entre las fases 32

6. Conclusiones..... 33

Introducción

El objetivo de todas las organizaciones, desde el punto de vista de la seguridad de la información, es tratar de reducir los riesgos y evitar los posibles incidentes de seguridad. Para ello disponemos de una normativa de referencia: la ISO 27000. Ahora bien, hay que tener en cuenta que siempre puede llegar a darse alguna situación imposible de proteger o de evitar.

Para hacer frente a estas situaciones, las organizaciones necesitan crear planes de continuidad de negocio, que tienen como fin evitar que las actividades de negocio queden interrumpidas.

Dependiendo de la organización, la interrupción de la actividad de negocio puede suponer un auténtico caos, traduciéndose en pérdidas económicas elevadísimas. Por ello, los planes de continuidad de negocio son fundamentales cuando hablamos de seguridad de la organización.

Además, debemos ser conscientes de que nunca podrá obtenerse la seguridad total. Por ello, conviene disponer de planes de continuidad de negocio. Y es que, como suele decirse:

> "El único sistema que es realmente seguro es uno apagado y desconectado de la red, encerrado en una caja fuerte forrada de titanio, enterrado en un búnker, rodeado de gas nervioso y custodiado por guardas armados y muy bien pagados. Incluso entonces, no daría mi vida por ello..."
>
> Gene Spafford
> Director de Computer Operations, Audit, and Security Technology (COAST), Universidad de Purdue

Por más que las organizaciones pretendan evitar los problemas de seguridad, debe tenerse claro que las medidas que adopten o bien pueden fallar o bien son insuficientes ante todas las amenazas que acechan.

El objetivo de la seguridad de la información es evitar que las actividades propias de la organización se vean interrumpidas por ninguna circunstancia.

Por ese motivo, los planes de continuidad de negocio son imprescindibles, independientemente del tamaño de la organización: además de las inversiones que ésta haya realizado en medidas de seguridad, también necesita tener establecido un plan de continuidad.

Estos planes de continuidad de negocio no sólo tienen por objetivo tratar de evitar las interrupciones en la actividad de negocio. También intentan minimizar el tiempo de inactividad en el caso de que finalmente se produzcan dichas interrupciones.

Podríamos resumir lo que hasta aquí hemos dicho destacando que los planes de continuidad de negocio equivalen a "**qué hacer en caso de que todo lo demás falle**".

Objetivos

Al acabar de trabajar los materiales de este módulo, los participantes deberían alcanzar los siguientes objetivos:

1. Saber qué es un plan de continuidad de negocio y cuáles son sus objetivos respecto a la seguridad de la información de las organizaciones.

2. Identificar las fases de los planes de continuidad de negocio y la manera de implantarlas.

3. Ser capaz de asignar las acciones determinadas en el plan de continuidad de negocio a las personas que configuran el equipo de seguridad de la información de la organización.

4. Conocer la estructura y el contenido del documento del plan de continuidad.

1. Planes de continuidad de negocio

Los planes de continuidad de negocio hacen frente a situaciones que no suelen ocurrir. Ahora bien, cualquier organización ha de estar preparada ante ellas, ya que pueden darse en cualquier momento. De hecho, cada vez son más frecuentes, como se demuestra en los siguientes ejemplos:

(20-08-04) Un fallo eléctrico paraliza el sistema informático de Barajas e interrumpe la facturación

Decenas de personas han tenido que esperar tiempo de más tras los mostradores de facturación del aeropuerto de Barajas a primera hora de este viernes después de que un corte en el suministro eléctrico, producido a las 8.10 horas a causa de una subida de tensión, haya interrumpido durante veinte minutos el sistema informático. El fallo eléctrico afectó, principalmente, al servicio de transporte de equipajes, lo que hizo que el aeropuerto tuviera que detener la facturación de maletas. Los retrasos no han llegado a afectar la hora de salida de los vuelos.

El incendio en una subestación eléctrica de Unión Fenosa deja a oscuras Madrid

La ciudad poco a poco vuelve a la normalidad.

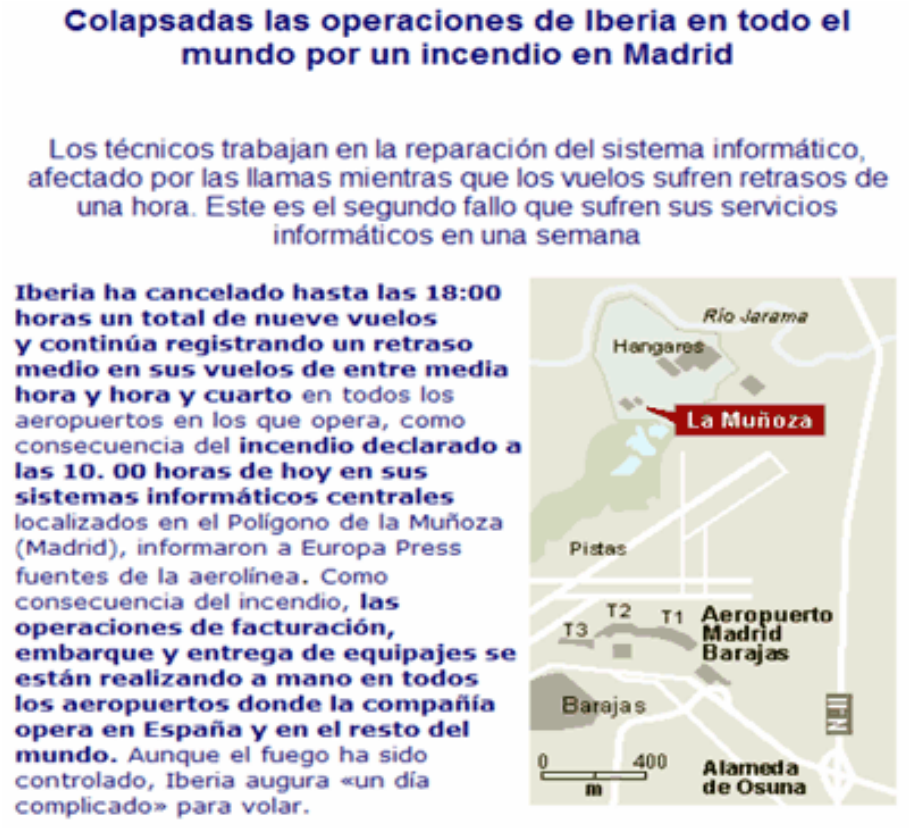
Un incendio en uno de los transformadores de la subestación eléctrica de la compañía Unión Fenosa en Méndez Álvaro ha dejado sin luz esta tarde a más de 80.000 clientes de varias zonas de Madrid y ha provocado que la subestación de Iberdrola de la calle Ayala dejara de funcionar durante media hora, privando de luz a otros 15.000 vecinos del distrito de Salamanca.

Un incendio en una subestación eléctrica deja sin luz a miles de madrileños

ELMUNDO.ES | AGENCIAS

MADRID - Un incendio desatado en una subestación eléctrica de Unión Fenosa en las inmediaciones de **Méndez Álvaro (barrio del sur de Madrid)** ha dejado sin luz a varios distritos de la capital. Según la compañía eléctrica, el apagón ha afectado a 250.000 clientes.

Usuarios de Retiro, Chamberí, Centro, Puente de Vallecas, Ciudad Lineal-Ventas, Moratalaz, Salamanca, Arganzuela, Pacífico y Vicálvaro se han quedado sin luz a media tarde. Hasta el momento, cerca de 22.000 clientes continúan a oscuras.



Colapsadas las operaciones de Iberia en todo el mundo por un incendio en Madrid

Los técnicos trabajan en la reparación del sistema informático, afectado por las llamas mientras que los vuelos sufren retrasos de una hora. Este es el segundo fallo que sufren sus servicios informáticos en una semana

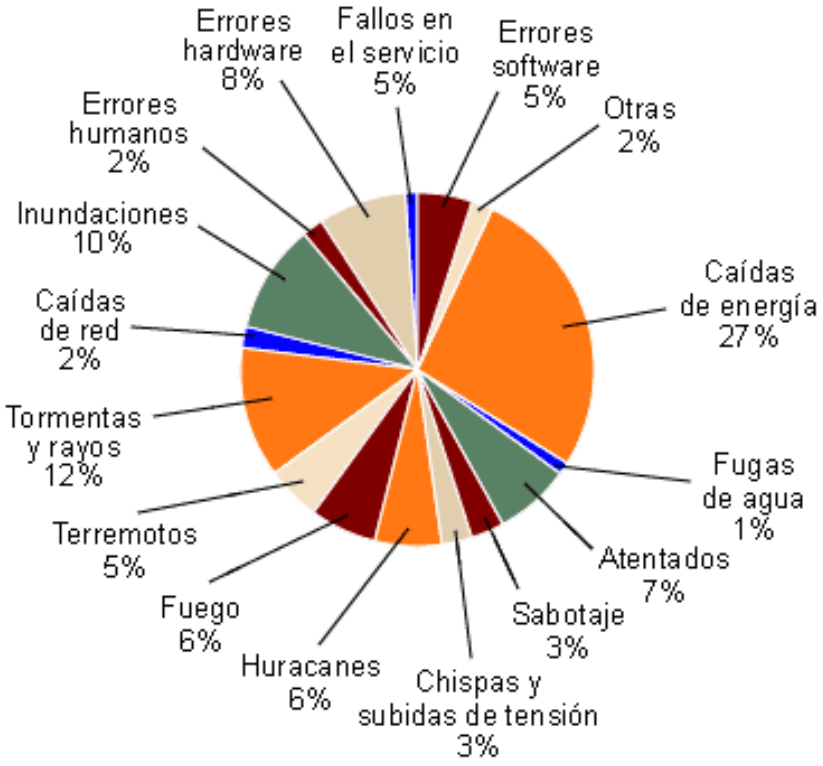
Iberia ha cancelado hasta las 18:00 horas un total de nueve vuelos y continúa registrando un retraso medio en sus vuelos de entre media hora y hora y cuarto en todos los aeropuertos en los que opera, como consecuencia del **incendio declarado a las 10. 00 horas de hoy en sus sistemas informáticos centrales** localizados en el Polígono de la Muñoza (Madrid), informaron a Europa Press fuentes de la aerolínea. Como consecuencia del incendio, **las operaciones de facturación, embarque y entrega de equipajes se están realizando a mano en todos los aeropuertos donde la compañía opera en España y en el resto del mundo.** Aunque el fuego ha sido controlado, Iberia augura «un día complicado» para volar.

Como se puede ver, estas situaciones se dan. Y no sólo se dan, sino que además tienen consecuencias importantes para la organización: incluso pueden provocar su cierre.

Un plan de continuidad de negocio pretende evitar, por todos los medios, la interrupción de las actividades de la organización.

Los planes de continuidad de negocio se definen para **cuando** falle el sistema, no **por si falla**.

Circunstancias que justifican la necesidad de disponer de un plan de continuidad de negocio



El análisis de la imagen nos muestra que las situaciones son muy diversas y, en muchos casos, no dependen de las propias organizaciones y no pueden ser evitadas a través de las medidas de seguridad, lo que no significa que no puedan provocar pérdidas importantes.

2. Enfoques en los planes de continuidad de negocio

Para evitar la posible confusión terminológica, vamos a definir una serie de conceptos que se suelen usar como sinónimos aunque no lo sean.

- **Disaster Recovery Planning (DRP).** El DRP es una estrategia planificada en fases, cuyo objetivo es recuperar todos los servicios relacionados con las tecnologías de la información y la comunicación y los recursos que los conforman, en el menor tiempo posible, a partir de un evento que ocasiona una interrupción mayor en su funcionamiento.

- **Bussiness Resumption Planing (BRP).** El objetivo del BRP es tratar de reanudar todos y cada uno de los procesos de negocio que posee la organización y que se hayan podido ver afectados por un fallo o incidente en las diferentes aplicaciones IT que los conforman.

- **Continuity od Operations Planning (COOP).** El objetivo del COOP es tratar de conseguir la recuperación de las funciones estratégicas de una organización que son desempeñadas en sus instalaciones corporativas.

- **Contingencia Planning (CP).** El objetivo del CP es tratar de conseguir la recuperación de los servicios y recursos de TI después de un desastre que provoca una interrupción mayor en su funcionamiento.

- **Emergency Response Planning**. Estos planes tratan de conseguir la salvaguarda de los empleados, el público, el medio ambiente, así como del resto de activos de la organización ante una situación de desastre.

- **Plan de continuidad de negocio (PCN).** El PCN es un conjunto formado por planes de actuación, planes financieros, planes de comunicación, planes de contingencias, etc., destinados a "mitigar el impacto" provocado por la concreción de determinados riesgos sobre la información y los procesos de negocio de una compañía.

El PCN es un elemento estratégico global. En este sentido, se sustancia en *N* planes de contingencia de áreas de negocio y en *N* planes de contingencia de las infraestructuras en las que se apoya el negocio, entre ellas los sistemas de información y comunicaciones.

Estos PCN tienen como objetivo dar respuesta de forma rápida y ágil a las situaciones que no han podido ser evitadas por las medidas de seguridad implantadas por la organización.

Esta respuesta de la organización es la prevista ante aquellas situaciones de riesgos que afectan de una forma crítica al servicio que hay que proteger. En este sentido, es fundamental, para cada organización, determinar el tiempo crítico de recuperación y conseguir tanto que este tiempo sea el mínimo como que el incidente tenga el menor impacto posible.

Lo primero que hay que hacer es implantar todos los controles que se han ido detallando a lo largo de la asignatura; es decir, los que se presentan en la normativa ISO 27002 y más concretamente, la Norma BS25999, específica para la continuidad de negocio. Después, como una nueva medida de seguridad con la que debe contar una organización, se diseña e implanta el plan de continuidad de negocio para que, si llega a suceder un desastre, se ejecute dicho plan y se puedan rcuperar los porcesos de negocio en el menor tiempo posible.

Características de un plan de continuidad de negocio

- Se encuentra en un proceso de mejora continua de la gestión de riesgos de la organización.
- Debe estar totalmente orientado a recuperar los procesos de negocio críticos para la organización.
- Debe estar diseñado para integrarse con el resto de elementos de seguridad de la organización.
- Debe servir para automatizar un conjunto de tareas de manera que se evite tener que planificarlas en momentos de crisis.

3. Plan de continuidad de negocio

Los planes de continuidad de negocio persiguen los siguientes objetivos:

- **Mantener el nivel de servicio** en los límites definidos por la compañía. Se pretende que las actividades de la organización siempre puedan ser ofrecidas dentro de unos mínimos, de forma que pueda considerarse que la actividad no está interrumpida.

  Nota

  El plan de continuidad de negocio no sólo debe recuperar los servicios, sino que debe recuperarlos, como mínimo, con el nivel de servicio marcado por la propia organización. Si el plan de continuidad de negocio no puede alcanzar este nivel, debemos considerar que no es el adecuado para dicha organiazción.

- **Establecer un periodo de recuperación mínimo** para garantizar la continuidad del negocio. Cada organización debe marcar el tiempo que considera que puede sobrevivir sin ofrecer sus actividades; es decir, debe marcar los tiempos de inactividad de sus activos.

- **Recuperar la situación inicial de los servicios y procesos.** Es decir, tratar de restablecer la organización al estado en el que se encontraba antes de que llegara a suceder la contingencia.

- **Analizar el resultado de la aplicación del plan de contingencias y los motivos del fallo** para optimizar las acciones. Durante la ejecución de estos planes, se genera una serie de evidencias para que puedan ser analizadas y detectar e identificar el motivo que provocó la necesidad de ejecutar dichos planes.

Estos planes de continuidad de negocio están basados en otro de los elementos fundamentales desde el punto de vista de la seguridad: el **análisis de riesgos**.

Análisis de riesgos

El análisis de riesgos permite identificar situaciones que podrían provocar algún tipo de incidente de seguridad en una organización. Asimismo, durante la gestión de estos riesgos, se define cómo cada organización puede o pretende protegerse de los riesgos analizados previamente.

En el caso de que se detecten situaciones de riesgo que no puedan ser controladas mediante la implantación de alguna medida de seguridad, por ejemplo, porque el coste de este control es elevado teniendo en consideración la probabilidad de que el incidente suceda, dichas situaciones pasan a controlarse por medio de los planes de continuidad de negocio.

Los planes de continuidad de negocio están íntimamente relacionados con el análisis de riesgos, puesto que sin ellos no sabría la organización ante qué situaciones deberían ejecutarse dichos planes.

3.1. Elementos de los planes de continuidad de negocio

Podemos identificar cuatro elementos fundamentales en los planes de continuidad de negocio en las organizaciones.

3.1.1. Definición de las situaciones críticas

Consiste en el proceso de identificación de los riesgos analizados, riesgos que podrían afectar a la organización y que no pueden ser evitados mediante la implantación de diferentes medidas de seguridad. Dichas situaciones serán las que aparezcan reflejadas en los planes de continuidad de negocio y las que deberán ser evitadas por la organización.

Como resultado se obtiene lo siguiente:

- **Activos críticos**. Son los activos que se verían afectados por estos riesgos. Este proceso se basa en el análisis de riesgos. Recordemos la relación de activos – amenazas – vulnerabilidades = riesgos.

- **Procesos de trabajo**. Se trata de relacionar o identificar qué procesos de negocio de la organización se podrían ver afectados por las amenazas que puedan dañar a los activos de la organización.

3.1.2. Asignación de responsabilidades

Una vez que tenemos identificados los riesgos que provocan la necesidad de disponer de planes de contingencias, debe pasarse a la asignación de responsabilidades. Como resultado se obtiene lo siguiente:

- **Un comité de emergencia**. Este comité será el encargado de actuar en caso de que llegue a producirse la situación de emergencia. Tendrá la responsabilidad de que el servicio pueda recuperarse en los tiempos establecidos por la organización.

- **Unos responsables de los planes**. Serán las personas, dentro del comité de emergencia, responsables de cada uno de los planes de contingencia que forman el plan de continuidad de negocio de una organización. Estos responsables tiene la obligación de mantener actualizados los planes, así como de verificar que éstos permiten la recuperación ante determinadas situaciones.

3.1.3. Definición de las acciones de respuesta

Consiste en determinar ante qué situaciones deberían ejecutarse cada uno de los planes de contingencia que conforman los planes de continuidad de negocio.

Como resultado se obtiene lo siguiente:

- **Indicadores de disparo**. Serán los puntos que marcarán el momento exacto en el que debe empezar a ejecutarse el plan.

- **Secuencia de acciones**. Se indicarán todas y cada una de las acciones que tendrán que llevarse a cabo desde el momento en el que se empieza a ejecutar el plan hasta que se llega a la recuperación de la contingencia y se regresa al estado inicial.

- **Registros**. Son las evidencias que quedan de la ejecución de todas y cada una de las acciones detalladas anteriormente.

3.1.4. Mantenimiento

Se trata de mantener tanto los planes de continuidad de negocio como los planes de contingencia que los forman. Como resultado se obtiene lo siguiente:

- **Datos de prueba y disparo**. Después de la ejecución de un plan, se analizan todos los registros de las acciones que se han llevado a cabo para extraer conclusiones.

- **Propuestas de mejora**. Una vez analizados los registros, se podrán proponer mejoras para optimizar los planes establecidos.

Los planes de continuidad de negocio deben responder a las diferentes situaciones de riesgo definidas y recoger todas las acciones que deben llevarse a cabo desde el momento en que se detecta la contingencia hasta que la organización vuelve a sus condiciones de funcionamiento.

Para que el plan de continuidad de negocio sea efectivo, es importante:

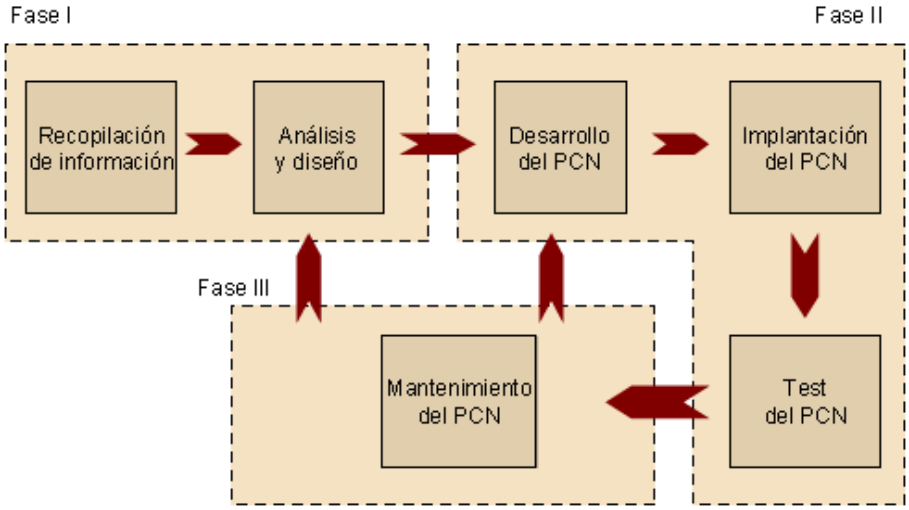
- Detectar los recursos necesarios
- Definir la disponibilidad, mantenimiento y operatividad de los recursos
- Establecer claramente el momento de disparo
- Asignar un responsable a los planes de contingencias específicos
- Asignar responsabilidades para cada acción definida

- Establecer un proceso de revisión una vez recuperada la situación

4. Fases de los planes de continuidad de negocio

Los planes de continuidad de negocio son procesos cíclicos que requieren una constante actualización, puesto que han de reflejar la situación real de la organización en cada momento.

En la siguiente imagen representamos las fases de los planes de continuidad de negocio:



4.1. Fase I

La primera fase en la creación de los planes de continuidad de negocio consiste en recopilar la información necesaria que permita elaborar los planes para cada uno de los escenarios de riesgos ante los que hay que protegerse.

Nota

Esta fase es la más importante de cara al resultado final y también se puede considerar como la más complicada, ya que será a partir de los resultados del análisis cuando se desarrollarán los planes de continuidad de negocio finales.

Una vez que se posee toda la información sobre los riesgos ante los que hay que protegerse, se procede al diseño del plan de continuidad de negocio; es decir, se plantea cómo quiere protegerse la organización ante estas situaciones.

En esta fase, además, se analiza cuánto está dispuesta a invertir la organización (en tiempo y dinero) para recuperarse de los desastres.

Esta primera fase consta de los siguientes procesos que analizaremos seguidamente:

- Gestión de riesgos
- Business impact analysis
- Desarrollo de estrategias del plan de continuidad de negocio

4.1.1. Gestión de riesgos

Los planes de continuidad de negocio, como ya hemos comentado, están íntimamente relacionados con el análisis de riesgos y la gestión de riesgos: se trata de identificar los riesgos a los que está expuesta la organización y buscar la manera de minimizarlos.

Recordad

Los planes de continuidad de negocio no deben ser considerados con unas medidas de seguridad de las que echar mano en caso de necesidad, sino que se trata del último recurso que tiene la organización ante una situación de riesgo que se ha concretado.

En primer lugar, se deben gestionar de la mejor manera posible los riesgos detectados y aquellas situaciones por debajo del umbral de riesgos de la organización que no puedan ser controladas, se procederá a tratarlas a través de los planes de continuidad de negocio.

Por lo tanto, los planes de continuidad de negocio deben ser totalmente personalizados para cada organización, puesto que cada una se encuentra expuesta a unos riesgos diferentes.

4.1.2. Business Impact Analysis (BIA)

Éste es el proceso más importante y el eje sobre el cual girará todo el plan de continuidad de negocio. El BIA consiste en identificar los procesos relacio-na-dos con la misión de la organización y analizar con mucho detalle los impactos en la gestión comercial del negocio que puede tener una interrupción de dichos procesos como resultado de un desastre.

Procedimentalmente, el BIA consiste en la realización de una serie de entrevistas con representantes de diferentes perfiles dentro de una organización, para obtener la información que permita identificar los procesos críticos de la organización y las consecuencias económicas que podría provocar su interrupción.

Nota

El BIA se realiza a nivel de proceso y en ningún caso se trata de analizar las consecuencias que tiene el daño en un determinado activo, sino en la globalidad del proceso.

Cuando se realizan las entrevistas, debe tenerse en cuenta que todo el mundo considera que sus funciones son las más importantes. Por lo tanto, hay que ser capaz de alejarse de la organización para poder tener una visión más global que ayude a corregir los sesgos de la información obtenida.

Corrección de sesgos

Hay diferentes técnicas que ayudan a ajustar los resultados de las entrevistas a la realidad; una de ellas consiste en hacer entrevistas cruzadas: preguntar sobre una misma tarea a diferentes perfiles.

Los resultados de las entrevistas se analizan para obtener la visión global que requiere esta fase y se presentan a la dirección de la organización. No podemos olvidar que el objetivo final de esta fase es identificar las consecuencias económicas de la interrupción de los procesos clave del negocio.

El BIA concluye cuando se ha conseguido indicar de una forma clara, y con valores económicos, una jerarquía de procesos a salvaguardar en caso de que se produjese un desastre.

En este sentido, hay cuatro grandes tipos de procesos que se pueden identificar a la hora de la realización del BIA:

- Procesos críticos. Procesos cuya interrupción comporta unas consecuencias económicas que no puede asumir la organización, para los que no se ha podido identificar ningún proceso alternativo que permita ejecutar estas funciones con el nivel mínimo de servicio.

- Procesos vitales. Procesos con una mayor toleracia a los fallos que los críticos. Para estos procesos se ha identificado un proceso alternativo que permite mantener la actividad durante un periodo de tiempo corto. El coste de la interrupción de estos procesos es asumible por la organización siempre que no exceda de un número reducido de días.

- Procesos sensibles. Las funciones que desarrollan estos procesos pueden asumirlas procesos alternativos durante un periodo relativamente largo. Pero para su ejecución se requerirá la contratación de personal extra. A pesar de ello, puede considerarse que el coste de la implantación del proceso alternativo (incluida la contratación de personal extra) comporta un coste medio para la organización.

- Procesos no críticos. Las funciones que desarrollan estos procesos pueden asumirlas procesos alternativos durante un periodo relativamente largo con un coste nulo, o relativamente bajo, para la organización.

La realización de las entrevistas

Al plantearse la realización de las entrevistas, no debemos olvidar que las llevamos a cabo para identificar los aspectos siguientes:

- Nivel de servicio que se debe mantener en la organización bajo cual-quier circunstancia. Este aspecto importante en aquellos procesos de negocio que se desarrollan de cara al público (el cliente final). Puesto que en caso de incumplirse, pueden derivarse unas consecuencias económicas relativas al incumplimiento de los contratos que se tienen firmados.
  Recordemos que los planes de continuidad de negocio deben asegurar, por lo menos, el nivel mínimo de servicio establecido por la organización en cada proceso.

- Tiempo máximo de inactividad de cada proceso que puede permitirse la organización. Este tiempo mínimo se establece valorando la pérdida económica que la organización puede asumir como consecuencia de la inte-

rrupción de dicho proceso. La reducción del tiempo de inactividad provoca un aumento exponencial en el coste económico del plan de continuidad de negocio: cuanto mayor sea el tiempo de inactividad que un proceso puede permitirse, menos costoso será el plan de continuidad de negocio, y a la inversa.

Todo plan de continuidad de negocio tiene que estar enfocado a no superar los tiempos de inactividad máximos identificados, el RTO (*Recovery Time Objective*).

- Procesos alternativos. Disponer de procesos alternativos para la realización de un proceso, siempre y cuando el nivel de servicio no caiga por debajo del mínimo identificado, permite reducir bastante el coste de los planes de continuidad de negocio.

Procesos alternativos

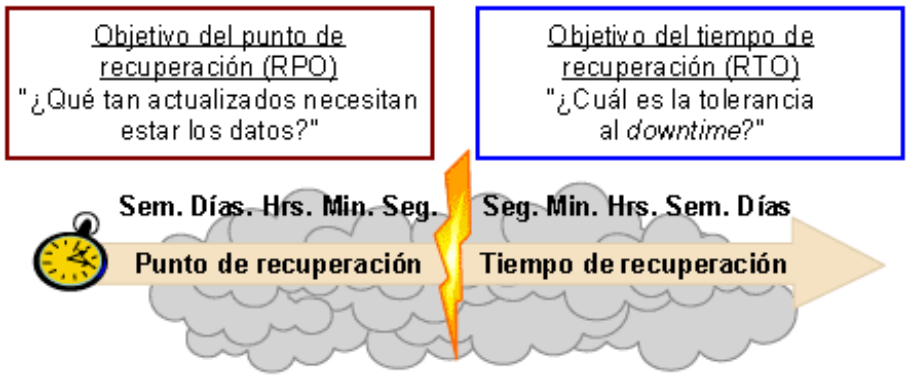
Un proceso alternativo podría ser la realización de determinadas acciones (en formato papel, por ejemplo), en el caso de que el sistema informático se viera afectado.

- Primeros datos que permiten volver a ofrecer el servicio. Identificar si para la recuperación del proceso que se haya visto afectado se necesita disponer de la información que se tenía justo antes de que sucediera el incidente, o si, por el contrario, se puede utilizar la información anterior (hasta qué momento: una hora, un día, dos...). Se trata de determinar lo que se conoce como RPO (*Recovery Point Objective*).

4.1.3. Desarrollo de la estrategia del plan de continuidad de negocio

Esta subfase consiste en el estudio de las diferentes estrategias que pueden permitir recuperar los diferentes procesos identificados en el BIA en el menor tiempo posible y con la menor inversión.

A la hora de plantear las diferentes estrategias, se deberá tener presentes, sobre todo, dos de los aspectos básicos identificados mediante el BIA: tiempo máximo de inactividad asumible (RTO) e información necesaria para recuperar los procesos (RPO):



Las diferentes estrategias son las siguientes:

- ***Cold site***. Esta estrategia consiste en disponer de una segunda ubicación, identificada y contratada previamente, para que, en caso de necesidad, la organización pueda desplazar a ella la ejecución de algunos procesos (o todos).
  Esta segunda ubicación contendrá únicamente las instalaciones básicas (cableado, sistemas de aire acondicionado, etc.), en ningún caso se prevé la necesidad de disponer de los equipos informáticos comprados. Como mucho, se podría disponer de contratos de servicio con los proveedores de los equipos para que los suministren en un determinado tiempo.
  Si se opta por una solución de *cold site*, se deberá tener en cuenta que comporta la adquisición de los nuevos equipos y su configuración, el traslado de la información (y del personal, si es el caso) como pasos previos a levantar el servicio y trabajar con los nuevos equipos en la nueva ubicación.

- ***Warm site***. Esta estrategia consiste en disponer de una segunda ubicación, identificada y contratada previamente, y de los equipos, por lo menos de parte de ellos, considerados como los más importantes para la realización de este proceso.
  Además, los equipos de que se disponga en esta segunda ubicación deberán estar parcialmente configurados (configuraciones de red, y equipos de red y periféricos, por ejemplo) para que en el momento de la contingencia no se tenga que partir de cero.
  Los *warm sites* están destinados, principalmente, a la recuperación de procesos que pueden estar un tiempo, generalmente breve, inactivos.
  Respecto de los *cold sites*, los *warm sites* comportan menos tiempo en la adquisición y configuración de equipos (lo más básico ya se tiene) y, por lo tanto, permiten levantar el servicio en un periodo de tiempo menor.

- ***Hot site***. Esta estrategia es, desde el punto de vista de la seguridad, la mejor de todas porque minimiza el tiempo de inactividad de un proceso, pero a su vez, es la que requiere una mayor inversión, porque comporta disponer de todos los equipos comprados actualizados y configurados para poder utilizarlos de forma automática o en pocas horas. También necesitará disponer de personal con conocimientos y documentación ajustada y que refleje la situación real de la organización.
  Por su elevado coste, esta estrategia está destinada a procesos muy críticos que no pueden estar inactivos mucho triempo, por lo que, generalmente, no se puede realizar el volcado de la información en el momento de la contingencia: un *hot site* requiere estar continuamente sincronizado. En este sentido, se puede optar por uno de los dos sistemas siguientes;
  – Volcado sincronizado: cualquier modificación que se realice en la información que se utiliza en producción se lleva a cabo de forma instantánea en el segundo centro, con lo que ello comporta en cuanto al ancho de banda y los equipos necesarios.

– Volcado asíncrono: los centros se configuran para que de forma periódica, y como mucho a lo largo de 24 horas, se realice un volcado total de la información en producción al centro alternativo. De esta forma, en caso de desastre, se dispondrá de la información de como máximo hace un día, y en muchas organizaciones es suficiente para poder levantar el proceso.

Disponemos de dos soluciones más, a la hora de plantearse la creación de un segundo centro alternativo:

- Sitios móviles. Remolques dedicados a la ubicación de equipos y sistemas. Suelen contener: servidores, estaciones de trabajo, equipos de comunicaciones, enlaces vía satélite, etc. Los sitios móviles, a pesar de que no son muy comunes, podrían ser útiles ante desastres que afectasen a una amplia zona geográfica.

- Acuerdos recíprocos. Dos o más empresas acuerdan proveerse mutuamente de instalaciones en caso de emergencia. Se reservan espacios y, en caso de desastre, sólo se necesita transportar los equipos y conectarlos a la red de la empresa "receptora".

Estas soluciones tienen la ventaja de que su coste es inferior a la contratación de un *site* (sea *hot*, *warm* o *cold*) a una empresa especializada en este tipo de servicios, pero presenta algunos inconvenientes: este tipo de acuerdos no suele obligar a las partes a su cumplimiento (no son empresas dedicadas a este tipo de servicios) y también podría darse algún problema de incompatibilidades entre configuraciones.

Conclusiones

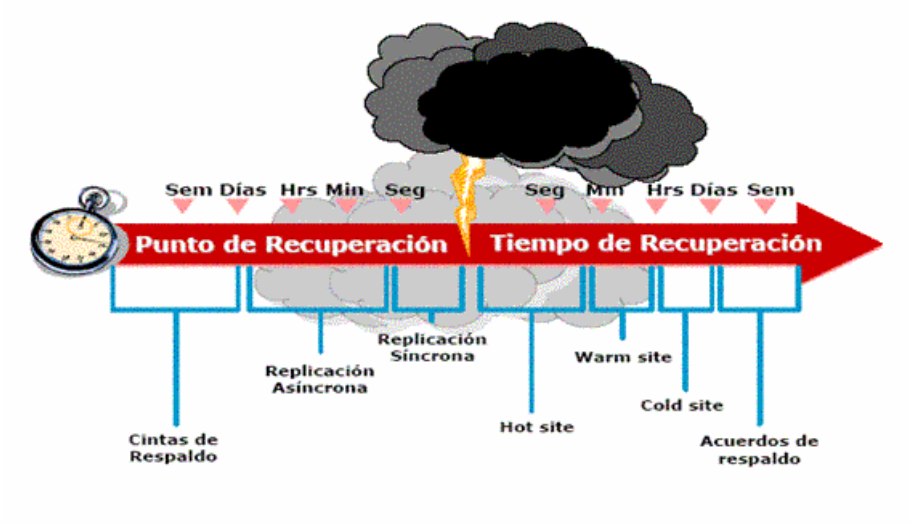
A la hora de seleccionar una de las estrategias anteriores, hay que tener presente que todas ellas presentan unos costes elevados, y que es más recomendable encontrar procesos manuales alternativos a tener que escoger una solución más restrictiva.

Si se opta por contratar una segunda ubicación, debería encontrarse a una distancia suficiente como para que una situación de riesgo en la organización no la afecte. En general, se recomienda un mínimo de cinco kilómetros, pero, como todas las medidas de seguridad, esta distancia depende de los riesgos a los que se encuentre expuesta la organización.

En cualquiera de las soluciones, a la hora de efectuar la selección de la estrategia a seguir, se ha de considerar que no sólo se trata de un coste de adquisición de nuevos equipos, sistemas e instalaciones, sino que también hay un importante coste relativo al mantenimiento que requieren dichos equipos, sistemas e instalaciones.

A partir del planteamiento de las diferentes opciones o estrategias, se debe escoger aquélla que permita a la organización cumplir con sus RTO y RPO con el nivel de servicio marcado siempre con la mínima inversión posible.

A continuación mostramos gráficamente las combinaciones más habituales de cara a los planes de continuidad, en base a las estrategias posibles, según los tiempos de RTO y de RPO:



4.2. Fase II

Una vez diseñado el plan, se procede a su desarrollo, es decir, se definen las diferentes acciones que deberán llevarse a cabo para poder proceder a la recuperación. Asimismo, en esta fase se indican, con todo tipo de detalles, las acciones que deben realizarse para recuperar la normalidad.

Una vez que esté detallado este plan, se procede a su implantación, es decir, a la compra de equipos, a designar ubicaciones, personal y a conseguir el resto de los recursos que se requieran para poder ejecutar los planes diseñados y desarrollados dentro de los tiempos máximos de inactividad que la organización pueda asumir.

Y, como todo control de una organización (los planes de *backup*, por ejemplo), requieren ser probados antes de que surja la necesidad de ponerlos en práctica. Se harán las pruebas pertinentes en esta fase.

4.3. Fase III

Consiste en la mejora de los planes después de la realización de las pruebas. Para ello, se emplearán las evidencias y registros que estas pruebas han generado.

El objetivo de estas mejoras es el de reducir el tiempo de recuperación de los escenarios de riesgos identificados.

5. Estructura de los planes de continuidad de negocio

Como hemos venido diciendo durante este módulo, los planes de continuidad de negocio no dejan de ser una serie de acciones que han de llevarse a cabo en caso de que suceda un determinado incidente de seguridad que no puede ser evitado o contrarrestado por las propias medidas de seguridad que tiene implantadas la organización.

Pero debe quedar claro que, al igual que el análisis de riesgos o la política de seguridad, estos controles no son más que documentos que con posterioridad deben aplicarse en una organización. Si no se realiza esta implantación, dichos controles quedarán como un documento que no se podrá utilizar ni aplicar cuando surja la necesidad.

Cuando se habla del documento del plan de continuidad de negocio, debe considerarse el siguiente aspecto fundamental:

Cada plan de continuidad de negocio es diferente del de otra organización, puesto que ninguna de ellas tiene las mismas necesidades.

En este sentido, a la hora de la redacción y creación debe tenerse muy claro el objetivo que se persigue con estos planes de continuidad, que no es otro que el de conseguir que la interrupción del negocio sea mínima si se dan algunas situaciones.

Esta salvaguarda del negocio es lo que hace que sea necesario que el plan sea totalmente personalizado, puesto que cada organización posee sus características y además tiene sus propios recursos para conseguir ofrecer sus servicios.

Una vez desarrollado el plan de continuidad, presentaría una estructura similar a ésta:

- Objetivo
- Alcance
- Descripción de la situación que hay que controlar:
  - Riesgos que deben controlarse
  - Activos que intervienen
  - Nivel de servicio exigido
  - Tiempos para cada respuesta: tiempo total de reacción
  - Recursos necesarios en cada uno de los planes. Disponibilidad y operatividad
- Listado de procedimientos concretos y sus responsables
- Disparo de alarma
- Plan de respuesta
- Plan de respaldo
- Plan de recuperación
- Plan de análisis y mejora
- Planes de prueba

Esta estructura, si está completa, será aplicable en una organización en caso de necesidad. A continuación se detallan qué aspectos es necesario que queden reflejados en cada uno de estos puntos.

5.1. Objetivo

Este primer punto consiste en la explicación de lo que se pretende conseguir con la creación e implantación del plan de continuidad de negocio, de manera que, cuando un trabajador de la organización haya accedido a este documento, sepa y tenga claro qué es lo que justifica la creación del plan.

Ejemplo de definición del objetivo

El objetivo de un plan de continuidad de negocio podría expresarse de la siguiente manera:

"Como es sabido, nuestra organización posee una información muy sensible y las actividades que realizamos con ella son fundamentales para su correcto funcionamiento. La Dirección, por tanto, ha desarrollado estos planes de continuidad de negocio con la intención de evitar que estas actividades básicas se interrumpan por la irrupción de algún suceso que no pueda controlarse con las diferentes medidas de seguridad que están implantadas."

La idea es que todos los trabajadores, aun sin ser expertos en seguridad, comprendan la función de estos planes de continuidad.

5.2. Alcance

Es fundamental que la ejecución del plan se centre en el alcance definido.

El alcance de un plan de continuidad de negocio podría llegar a incluir la totalidad de una organización o, por el contrario, podría limitarse a una parte o a unos determinados procesos dentro de la misma, los que se consideren más críticos.

En la elaboración del alcance, deberán concretarse claramente, en los planes de continuidad de negocio, los servicios que se pretenden garantizar, así como las localizaciones. También deberá definirse el personal que se verá involucrado en la ejecución de estos planes.

Definición del alcance para una empresa

Imaginamos que una organización posee diversos centros distribuidos a lo largo de toda la geografía española. Los planes de continuidad de negocio pueden hacer referencia únicamente a una determinada sede, por lo que el alcance sería el siguiente:

- Las actividades de negocio que se desarrollen en esta sede
- El personal que trabaja en ella
- Los activos que se encuentran en la sede

5.3. Descripción de la situación que se debe controlar

Es en este punto donde se refleja la relación existente el análisis de riesgos y el plan de continuidad de negocio: las situaciones que tendrán que ser controladas serán las que comporten un riesgo mayor para la organización que no puede ser reducido mediante la implantación de alguna medida de seguridad.

Además, sobre la base de estos riesgos que pretenden evitarse, se pueden determinar otros elementos fundamentales para la posterior elaboración del plan de contingencias.

Combinando el análisis de riesgos y el BIA obtendremos el detalle de los procesos prioritarios para la organización y ante qué situaciones será necesario que se ejecuten los planes.

En esta fase también se elabora la lista de activos que deben tenerse en cuenta en la ejecución del plan de continuidad. Al definir el alcance de dicho plan, se podrá determinar cuales de los activos quedan dentro y también poder saberse cómo se ve afectado cada uno de ellos por las diferentes amenazas que provocan riesgos elevados.

Desde el punto de vista de la funcionalidad de la organización, en este punto se determinará cuáles son los niveles mínimos que se quieren mantener cuando ésta se encuentre bajo la realización/ejecución del plan de continuidad.

Los tiempos de respuesta, los que determinan el tiempo que la organización puede estar sin ejecutar sus procesos, son fundamentales. Una vez que se tienen claros los tiempos de respuesta deseados, podrá hacerse una estimación de los recursos que van a necesitarse para la ejecución de los planes, y concretamente de los recursos necesarios para cada una de las fases en las que se divide el plan de continuidad: plan de respuesta, plan de respaldo y plan de recuperación.

5.4. Listado de procedimientos concretos y sus responsables

Este punto lo conforma el listado de procedimientos que es necesario conocer, y a los que con posterioridad se hará referencia, para poder recuperarse de las contingencias marcadas.

De la misma forma, será necesario que estén designados los responsables de cada uno de los procedimientos que han sido identificados como necesarios. Serán ellos los encargados de actualizar estos procedimientos, no por necesidades del plan sino por la propia operativa de la organización.

Procedimiento de copias de seguridad

Es muy habitual que una organización, para ejecutar su plan, necesite disponer del procedimiento de "copias de seguridad", puesto que durante alguna de las fases del plan de continuidad de negocio se requerirá recuperar la información de alguno de los soportes de *backup* que posee la organización.

5.5. Disparo de alarma

Este punto es fundamental para el éxito del plan de continuidad.

Se denomina **disparo de alarma** el momento a partir del cual debe comenzarse la ejecución del plan de continuidad de negocio.

Es importante que esté claramente identificado quién es el responsable de lanzar el aviso de que es necesario entrar en contingencia y que hay que ejecutar las pertinentes acciones. No es aconsejable que no esté definida esta persona ni los momentos a partir de los cuales se necesita comenzar la ejecución del plan. De esta manera se evitan situaciones interpretables.

Debe saberse que el momento de disparo dependerá de cada organización, puesto que, a la hora de la verdad, cada una tendrá un tiempo de respuesta determinado. Cuanto más breve sea éste, antes tendrá que saltar el momento de disparo.

El tiempo máximo del momento de disparo es aquel que, sumado al tiempo establecido para la ejecución del plan de continuidad de negocio, es igual al tiempo máximo de respuesta que ha definido la organización.

Ejemplo

Supongamos que tenemos estos datos:

- Tiempo máximo de respuesta: seis horas.
- Tiempo de ejecución del plan: cuatro horas.

El tiempo de disparo de alarma ha de ser como máximo de dos horas desde la parada de las actividades de negocio.

5.6. Plan de respuesta

En este punto se definen las acciones que deben llevarse a cabo para la ejecución del plan. Cada una de las acciones que se considera que han de realizarse, deben tener asociadas un responsable, que será el encargado de su ejecución.

Este conjunto de acciones se divide en tres fases diferentes:

- Plan de respuesta
- Plan de respaldo
- Plan de recuperación

El plan de respuesta consiste en el conjunto de acciones que se realizarán inmediatamente después del disparo de la alarma de contingencia.

Conviene determinar las siguientes acciones:

- **Acciones para proteger a las personas**. Son el conjunto de acciones destinadas a salvaguardar a las personas, por encima del resto de los activos. Estas acciones, en muchos casos, implican diferentes planes de emergencia.

- **Acciones para cortar la situación de riesgo: control de las amenazas**. Este conjunto de acciones va encaminado a reducir o eliminar la amenaza que ha provocado la ejecución del plan. Por ejemplo, la extinción de un incendio.

- **Acciones para proteger a los activos**. Estas acciones van encaminadas a salvar los activos que no se hayan visto afectados por esa amenaza.

- **Acciones de notificación pública**. Estas acciones consisten en las comunicaciones que debe hacer la organización a organizaciones externas para notificar la situación que se ha provocado. Estas acciones a veces son sinceras y otras tratan de ocultar la situación en la que se encuentra la organización.
  Se debe notificar el estado de la situación a los medios de comunicación (en caso de que sea necesario), a los proveedores, a los clientes, a los socios, etc. A todos aquellos que estén involucrados en el proceso de negocio que se haya visto afectado.

- **Registro de las acciones que se van realizando**. Es necesario que cada una de las acciones que se lleven a cabo queden registradas para su posterior análisis.

El plan de respuesta consiste en las primeras acciones que deben realizarse cuando la organización detecta una contingencia y que van encaminadas a minimizar su impacto.

5.7. Plan de respaldo

Es el conjunto de acciones que deben desarrollarse para poder ofrecer el servicio que se ha visto afectado. Siempre se pretende mantener el servicio dentro de los niveles requeridos por la organización.

Conviene determinar los siguientes elementos:

- **Recursos necesarios para mantener la operación**. Se detectarán qué recursos o activos serán necesarios para poder ejecutar estas acciones.

Recurso de recuperación de información

Un ejemplo de recurso puede ser la máquina de *backup* que posee la organización y que se encuentra en otro edificio.

- **Mantenimiento de los recursos**. Se establecerán las operaciones que deben llevarse a cabo con los recursos detectados anteriormente para que estén operativos igual que lo estaba el que se ha visto afectado por la contingencia.

- **Activación de las diferentes acciones**. Se fijará el momento en el que se tienen que activar cada una de las acciones que se han diseñado. Debe estar identificada la persona que se encarga de la activación.

- **Identificación del personal implicado**. Se identificará el personal implicado en la ejecución de estas acciones. Tienen que ser avisadas de que se requiere su participación en estos planes.

- **Registro de las acciones llevadas a cabo: inicio, desarrollo y resultados**. Es necesario que cada una de las acciones que se lleven a cabo queden registradas para poder ser analizadas posteriormente.

5.8. Plan de recuperación

El plan de recuperación consiste en el conjunto de acciones que deben llevarse a cabo para retornar a la situación inicial. Es decir, el plan de continuidad de negocio no se acaba cuando la organización ha conseguido ofrecer el servicio dentro de los niveles establecidos, sino cuando es capaz de volver al punto en el que se encontraba justo antes de que se produjera la contingencia.

Hay que tratar de seguir estos pasos:

- **Restitución de activos, suministros, entorno**. Consiste en volver a recuperar los activos que se vieron dañados por la contingencia. Hay que tener en cuenta que, en muchas ocasiones, los recursos que ofrece el servicio en estado de contingencia son de características inferiores a las habituales. Son recursos que sólo se utilizan de forma puntual y durante un tiempo de excepción.

- **Arranque de los sistemas, servicios, etc**. Una vez que se han comprado o recuperado los activos principales deberán arrancarse y se comprobará si funcionan correctamente. Éste es el paso en el que se realizan las migraciones de datos y las configuraciones de los activos para poder ofrecer los servicios.

- **Pruebas para comprobar los sistemas restaurados**. Es necesario que se realicen pruebas, una vez que se han configurado los activos, para estar seguros de que éstos no producirán errores en el momento en el que vuelvan a asumir la ejecución de los procesos de negocio.

- **Puesta en operación**. En el momento en el que todas las pruebas han constatado que los activos funcionan correctamente se procederá a realizar la actividad con estos nuevos recursos.

- **Retirada de los planes de respaldo**. Cuando los nuevos recursos están funcionando, se retirarán los activos de contingencia y se guardarán en la forma en la que se encontraban antes del incidente para poder utilizarlos en otras situaciones de emergencia.

- **Registro de las acciones realizadas y resultados**. Es necesario que cada una de las acciones que se lleven a cabo consten en registros y que éstos puedan recogerse para su posterior análisis.

Concluido el proceso, la organización se encuentra, por fin, en el mismo estado en el que se encontraba antes de que sucediera la contingencia. Eso conlleva también que, en el caso de que volviera a suceder la contingencia, podrá volver a ejecutar estos planes con la seguridad de que se dispone de los activos necesarios para que el servicio no se vea interrumpido.

5.9. Plan de análisis y mejora

Una vez finalizadas las acciones, deben recogerse todos y cada uno de los registros que se han ido generando en las diversas fases del plan de continuidad de negocio. Después, se analizarán para detectar los posibles fallos que se han ido produciendo durante estas ejecuciones.

Este plan de análisis tiene como objetivo poder elaborar procedimientos de mejora de estos planes, de modo que se reduzca el tiempo de realización de las diferentes acciones. Los registros que se analizarán son los siguientes:

- Datos sobre la situación de emergencia: causas, duración, daño producido.
- Datos sobre el desarrollo y adecuación de los planes de respuesta, respaldo y restauración. Son registros tomados durante el desarrollo de los planes.

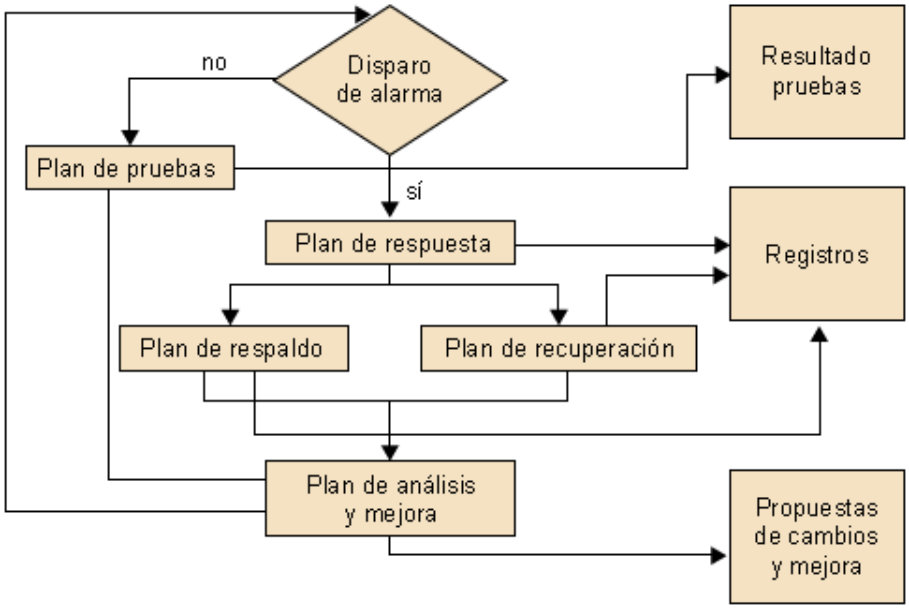
A partir de estos datos, se procede a elaborar un informe para que el comité de emergencia, que es el equipo que posee la responsabilidad de los planes de continuidad de negocio, pueda proponer mejoras en ellos.

5.10. Planes de prueba

No basta con tener perfectamente descritas las acciones que deben llevarse a cabo en caso de que llegara a producirse una determinada contingencia, sino que también es necesario probarlas para estar seguros de que con estos planes se pueden conseguir los objetivos marcados por la dirección.

Estas pruebas tienen que estar planificadas, porque en muchas ocasiones pueden provocar interferencias con las actividades de negocio de la organización. A pesar de ello, deben realizarse del modo más real posible para asegurarse de que, en caso de necesidad, se podrá hacer uso de estos planes de continuidad con la tranquilidad de que se evitará la interrupción de la actividad de la organización por un tiempo superior al previsto por la dirección.

5.11. Resumen de las relaciones entre las fases



6. Conclusiones

Los planes de continuidad de negocio son fundamentales para asegurar la información, que es lo que pretende la organización con la implantación de las medidas de seguridad.

En estos planes deben quedar detalladas todas y cada una de las acciones que han de llevarse a cabo para recuperarse de determinadas situaciones, así como el orden en el que se tienen que ir realizando.

Estas acciones tendrán claramente identificadas a las personas que deben llevarlas a cabo para evitar que, en el momento de necesidad, deba decidirse quién es la persona encargada de realizarlas.

Es fundamental que los planes de continuidad de negocio estén actualizados y que reflejen siempre la situación real de la organización, puesto que, en caso contrario, no es seguro que ésta se pueda recuperar dentro de los tiempos establecidos.

La progresión en el tiempo de estos planes de continuidad sería la siguiente: