



PLAN DE CONTINGENCIA Y CONTINUIDAD DE NEGOCIO

Colección

PROTEGE TU EMPRESA

ÍNDICE

ÍNDICE

1- INTRODUCCIÓN.....	03
2- TIPOS DE PROYECTOS DE CONTINUIDAD.....	05
3- FASES DE UN PLAN DE CONTINUIDAD DE NEGOCIO.....	07
3.1. FASE 0: DETERMINACIÓN DEL ALCANCE.....	09
3.2. FASE 1: ANÁLISIS DE LA ORGANIZACIÓN.....	11
3.2.1. Mantener reuniones.....	12
3.2.2. Análisis de Impacto sobre el Negocio.....	13
3.2.3. Análisis de Riesgos.....	17
3.3. FASE 2: DETERMINACIÓN DE LA ESTRATEGIA DE CONTINUIDAD.....	19
3.4. FASE 3: RESPUESTA A LA CONTINGENCIA.....	21
3.4.1. Plan de Crisis (o de Incidentes).....	22
3.4.2. Planes Operativos de Recuperación de Entornos.....	23
3.4.3. Procedimientos técnicos de trabajo (o de Incidentes).....	24
3.5. FASE 4: PRUEBA, MANTENIMIENTO Y REVISIÓN.....	25
3.5.1. Plan de mantenimiento.....	27
3.5.2. Planes de pruebas.....	28
3.6. FASE 5: CONCIENCIACIÓN.....	29
4- RESUMEN.....	30
5- REFERENCIAS.....	31

ÍNDICE

ÍNDICE DE FIGURAS

Ilustración 1: Prioridades del Plan de Continuación de Negocio.....	03
Ilustración 2: Objetivos del Plan de Continuación de Negocio.....	07
Ilustración 3: Análisis de impacto sobre el negocio.....	13
Ilustración 4: Estrategias para el tratamiento de los riesgos	18
Ilustración 5: Información necesaria para establecer la Estrategia de Continuidad...	19
Ilustración 6: Elementos para la gestión inicial de una crisis	22

1.

INTRODUCCIÓN

Las empresas deben estar preparadas para **prevenir, protegerse, y reaccionar ante incidentes de seguridad** que puedan afectarles y que podrían impactar en sus negocios. Por este motivo es necesario proteger los principales procesos de negocio a través de un conjunto de tareas que permitan a la organización recuperarse tras un incidente grave en un plazo de tiempo que no comprometa su continuidad. De esta forma se garantiza poder dar una respuesta planificada ante cualquier fallo de seguridad. Esto repercutirá positivamente en el cuidado de nuestra imagen y reputación como empresa, además de mitigar el impacto financiero y de pérdida de información crítica ante estos incidentes.

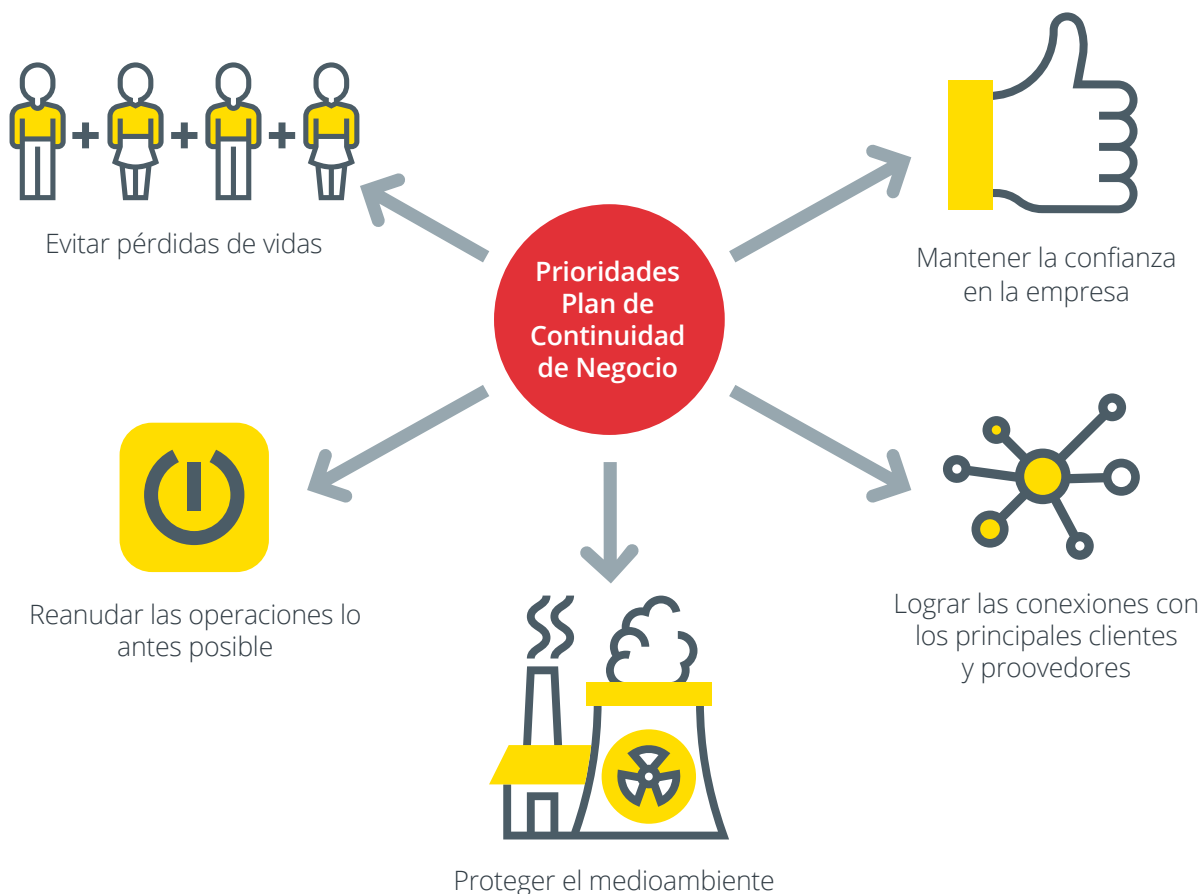


Ilustración 1
Prioridades del Plan de Continuación de Negocio

Debemos tener en cuenta que el término **continuidad del negocio** no hace referencia exclusivamente a aspectos relacionados con las tecnologías de la información.

Por ejemplo, en una empresa de mensajería se deben tener en cuenta las consecuencias de una inundación en el almacén, en una panadería se debe considerar el fallo de sus hornos, o en una empresa de atención telefónica el mal funcionamiento de la centralita.

¿Qué ocurre si hay un fallo en el sistema eléctrico?, ¿y si nuestra web no está disponible? ¿Qué ocurriría en tu empresa si hubiera una pandemia de gripe u otro virus? ¿Has considerado medidas de bajo coste como el teletrabajo en esta situación de contingencia?

Aunque podría pensarse que la continuidad del negocio es un ámbito exclusivo de las grandes organizaciones, esto no es cierto. Si bien existe una diferencia significativa, cada organización establece las medidas necesarias y proporcionales a sus necesidades para garantizar su continuidad en caso de desastre. Si hablamos del ámbito tecnológico, por ejemplo, mientras que una gran organización puede requerir el despliegue de un centro de respaldo alternativo, tan-

to de comunicaciones, sistemas como servidores en una ubicación remota, en otros casos podría ser más óptimo realizar copias de seguridad en la nube, primando el rendimiento frente al coste.



2.

TIPOS DE PROYECTOS DE CONTINUIDAD

Aunque, en términos generales, se suelen enmarcar dentro del concepto de Plan de Continuidad de Negocio [1], sí que tenemos que distinguir tres tipos según el alcance o ámbito que tengan.

► **Plan de Continuidad de Negocio (PCN)** establece la continuidad de una organización desde múltiples perspectivas: infraestructura **TIC**, recursos humanos, mobiliario, sistemas de comunicación, logística, sistemas industriales, infraestructuras físicas, etc. Cada uno de estos ámbitos tendrá a su vez un plan de continuidad más específico, ya que no es lo mismo la inundación de un almacén de logística que el corte del suministro eléctrico en una sala de servidores.

► **Plan de Continuidad TIC** (o Plan de Contingencia **TIC**, **PCTIC**), es uno de los planes que forman el plan de continuidad de negocio de nuestra organización, pero restringido al ámbito TIC. Mientras que un PCN sirve de disparador para los diferentes planes de contingencia, un **PCTIC** se limita al ámbito tecnológico.

Por ejemplo, si se produce un incendio en uno de nuestros almacenes, será necesario poner en marcha todos aquellos planes de continuidad de negocio relacionados con los procesos que han

sido afectados. En este caso, nos centraremos en la parte tecnológica.

Aunque el alcance de un PCN es por lo general superior al de un PCTIC, ya que hay otros procesos y activos no tecnológicos implicados, las fases de su elaboración son básicamente las mismas.

► **Plan de Recuperación ante Desastres (PRD)**. En este caso, su fase de análisis es menos profunda y se enfoca al ámbito más técnico, de modo que es un plan reactivo ante una posible catástrofe. Por ejemplo, si tenemos un plan de desastres para nuestra página web de comercio electrónico, el **PRD** contendrá todos los pasos para la recuperación de la aplicación.

Cabe destacar dos aspectos:

1. Estos tres planes o ámbitos son inclusivos:

- » Plan de recuperación ante desastres.
- » Plan de contiuidad TIC.
- » Plan de continuidad de negocio.

2. Dado que nuestra organización puede tener distintos servicios con distintas necesidades, lo dicho no implica que debamos abordar un proyecto que abarque todos los departamentos o servicios de la organización. Es decir, podemos desarrollar un PCTIC en un departamento o servicio de la organización que se amplíe a determinados servicios, que aunque no sean tecnológicos sí estén relacionados, o que nos interese abordarlo en este proyecto.



3.

FASES DE UN PLAN DE CONTINUIDAD DE NEGOCIO

Los planes de continuidad de negocio pueden ayudarnos a:



Mantener el nivel de servicio en los límites definidos



Establecer un período de recuperación mínimo



Recuperar la situación inicial antes de cualquier incidente de seguridad



Analizar los resultados y los motivos de los incidentes



Evitar que las actividades de la empresa se interrumpan

Ilustración 2 *Objetivos del Plan de Continuación de Negocio*

Por todo ello, debemos considerar, desde un punto de vista formal, aquellos factores que pueden garantizar la continuidad de una empresa en circunstancias adversas. Este proceso implica las siguientes **fases**:

▶ **Fase 0. Determinación del alcance.** Si nuestra empresa presenta cierta complejidad organizativa, abordar un proce-

so de mejora de la continuidad puede suponer emplear un número de recursos y un tiempo excesivo. Por tanto, es recomendable comenzar por aquellos departamentos o áreas con mayor importancia y progresivamente ir ampliando la continuidad a toda la organización. Para ello siempre con el compromiso e implicación de la dirección.

- ▶ **Fase 1. Análisis de la organización.** Durante esta fase recopilamos toda la información necesaria para establecer los **procesos de negocio críticos**, los activos que les dan soporte y cuáles son las necesidades temporales y de recursos.
- ▶ **Fase 2. Determinación de la estrategia de continuidad.** Conocidos los activos que soportan los procesos críticos, debemos determinar si en caso de desastre, seremos capaces de recuperar dichos activos en el tiempo necesario. En aquellos casos en los que no sea así, debemos establecer las diversas estrategias de recuperación.
- ▶ **Fase 3. Respuesta a la contingencia.** A partir de las estrategias de recuperación escogidas, se realiza la selección e implantación de las iniciativas necesarias, y se documenta el **Plan de Crisis** y los respectivos documentos para la recuperación de los entornos.

- ▶ **Fase 4. Prueba, mantenimiento y revisión.** A partir de la infraestructura tecnológica de nuestra empresa, desarrollaremos los planes de prueba y mantenimiento.
- ▶ **Fase 5. Concienciación.** Además del análisis y la implantación, es necesario que tanto el personal técnico como los responsables de nuestra empresa conozcan qué es y qué supone el Plan de Continuidad de Negocio así como qué se espera de ellos.



3.1. FASE 0: DETERMINACIÓN DEL ALCANCE

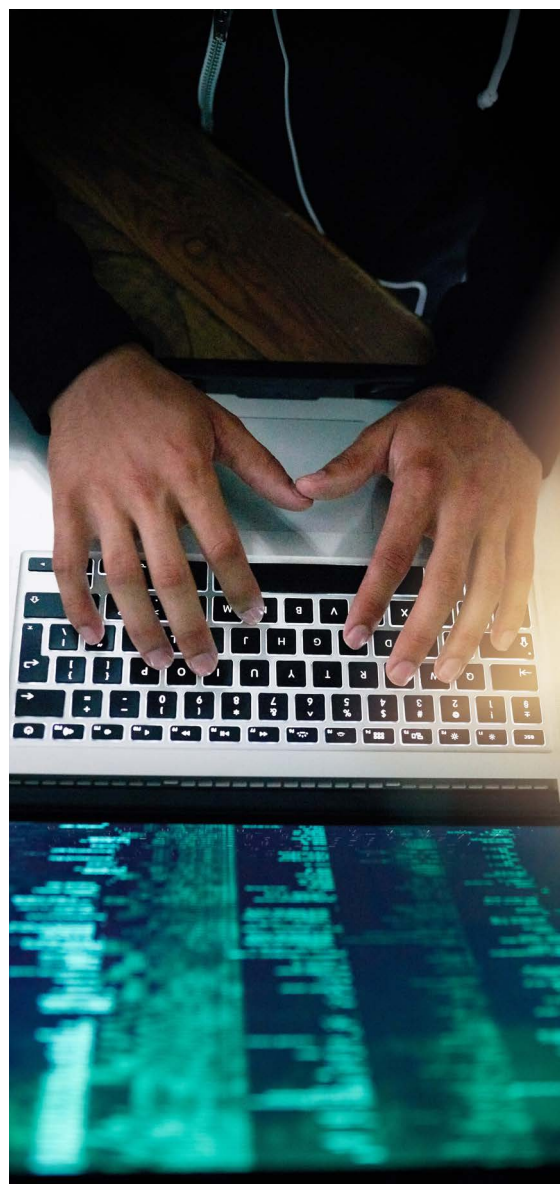
Esta fase es la de menor duración y consume un menor número de recursos. Pero su ejecución es imprescindible para poder determinar la magnitud y coste del proyecto que vamos a abordar, además de su viabilidad futura.

En esta fase determinaremos qué elementos de nuestra empresa van a ser el foco de la mejora de su continuidad. Por tanto estará implicado el personal, los activos de información, los sistemas informáticos, y otros servicios y procesos de la organización. Según los tipos de proyecto que hemos visto, lo habitual es que un PRD esté enfocado a los activos, mientras que el PC-TIC tenga un enfoque mayor en los procesos de la empresa.

El alcance habitual son aquellos **sistemas o procesos de mayor criticidad** y por tanto, los que en caso de pérdida impactarían más sobre nuestra organización. Aunque nos centramos en el ámbito de la tecnología, esto es exactamente igual para cualquier empresa: si para una panadería su elemento más crítico es el horno, ese debe ser el alcance. No tendría sentido en ese caso que el proyecto se centrara en elementos que son accesorios o cuyo impacto sobre el negocio es menor.

Otro elemento a tener en cuenta en el alcance es que durante el desarrollo del proyecto no sólo se implicarán a los activos

tecnológicos (servidores, dispositivos de red, equipos personales, bases de datos, aplicaciones, etc.), y personal de informática sino que también requerirá la colaboración de otros departamentos.



Según esto, podemos plantear el enfoque desde el punto de vista del activo, o del proceso:

- ▶ El **enfoque por activo** asume la mejora de la continuidad de un conjunto de activos, y a partir de estos obtiene la información de los procesos que los utilizan. Este enfoque es más propio de un PRD o cuando nuestro proyecto lo va a abordar el departamento técnico.
- ▶ El **enfoque por proceso** pretende mejorar la continuidad de un determinado proceso, con independencia de los activos de informática que le den soporte. Este enfoque es más propio del negocio.

Un **ejemplo** de alcance podría ser la **aplicación de contabilidad** que es crítica para la organización por razones de carácter fiscal.

Esto implicará que en el proyecto intervendrá todo el personal técnico relacionado con la aplicación, y todo el personal de los departamentos que trabajen con dicha aplicación.

- Según un **enfoque por activo** cualquier análisis se centrará en el activo, la aplicación de contabilidad, y a partir de ahí estableceremos las dependencias que nuestra organización tiene de dicho elemento.

- Según un **enfoque por proceso**, el alcance sería el proceso de contabilidad, y en ese caso el objetivo del proyecto sería la mejora de la continuidad del proceso, que puede implicar además de la mejora de la aplicación, la implantación de medidas adicionales.

El alcance que escojamos determinará el volumen de trabajo del proyecto. En una empresa pequeña puede ser interesante abordar todo los aspectos TIC, mientras que en una empresa de tamaño medio, una opción puede ser comenzar con un proceso o activo crítico y a partir de ahí ampliando poco a poco el alcance a otras áreas y activos.

Dado que nuestra idea es hacer un Plan de Continuidad de Negocio TIC **[2]**, vamos a **centrar nuestro proyecto en un enfoque por proceso**. Es decir, vamos a coger nuestro proceso más crítico y vamos a mejorar su continuidad.

Cabe destacar que aunque el enfoque a adoptar está centrado en un planteamiento TIC, éste puede aplicarse sin demasiadas modificaciones a los planes de continuidad de otros entornos: logística, producción, etc., siempre teniendo en cuenta las particularidades de cada caso.

3.2. FASE 1: ANÁLISIS DE LA ORGANIZACIÓN

Esta fase conlleva la obtención, elaboración y comprensión de las circunstancias, tecnologías, procesos y recursos de nuestra organización. Esto nos permitirá abordar las fases posteriores con garantías y sobre una base sólida. Es importante que involucremos a múltiples actores para que el resultado sea lo más cercano posible a la realidad.



3.2.1. MANTENER REUNIONES

La primera tarea a realizar es **reunirnos con los usuarios finales** del proceso que hemos seleccionado como nuestro alcance. De estas reuniones debemos obtener las dependencias de proveedores, el personal implicado, las aplicaciones que se utilicen, y datos sobre las necesidades temporales de cada aplicación.

Por ejemplo, si nuestro proceso más crítico es la contabilidad, deberemos reunirnos con todo el personal implicado en ese proceso, conocer las aplicaciones que utilizan, los equipos informáticos, qué proveedores utilizan, si dependen de otros departamentos, cuánto tiempo puede estar el proceso sin disponer de una determinada aplicación, a qué horas se utiliza o cuántos días de información podría ser asumible perder, en caso de un incidente grave.

El siguiente paso es **recopilar toda la información sobre las aplicaciones** que hemos obtenido en el paso anterior, para obtener los detalles de su funcionamiento, instalación, proveedor, etc. Esto podemos hacerlo con entrevistas al personal de informática o simplemente revisando toda la información de la que dispongamos. Siguiendo el ejemplo, así conoceremos si se realizan copias de seguridad de la aplica-

ción de contabilidad, cada cuánto tiempo, si la aplicación está en periodo de soporte y cuál es el tiempo de respuesta del proveedor, etc.

Tras estos dos pasos, tendremos una visión general de los procesos de los que queremos mejorar la continuidad.



3.2.2. ANÁLISIS DE IMPACTO SOBRE EL NEGOCIO

El siguiente paso es elaborar el Análisis de Impacto sobre el Negocio o **BIA [3]** (*Business Impact Analysis*), a partir de la información que hemos recogido. Este documento se debe de realizar siempre desde el punto de vista de negocio.

Es uno de los ejes principales del PCTIC, al contener las necesidades de los procesos que hemos definido como alcance. Así podremos clasificarlos según su criticidad y su dependencia de los activos tecnológicos.

Este documento contiene los **requisitos temporales y de recursos** de los procesos dentro del alcance y, junto con el Análisis de Riesgos define las iniciativas a implantar para recuperar los procesos en situación de contingencia.

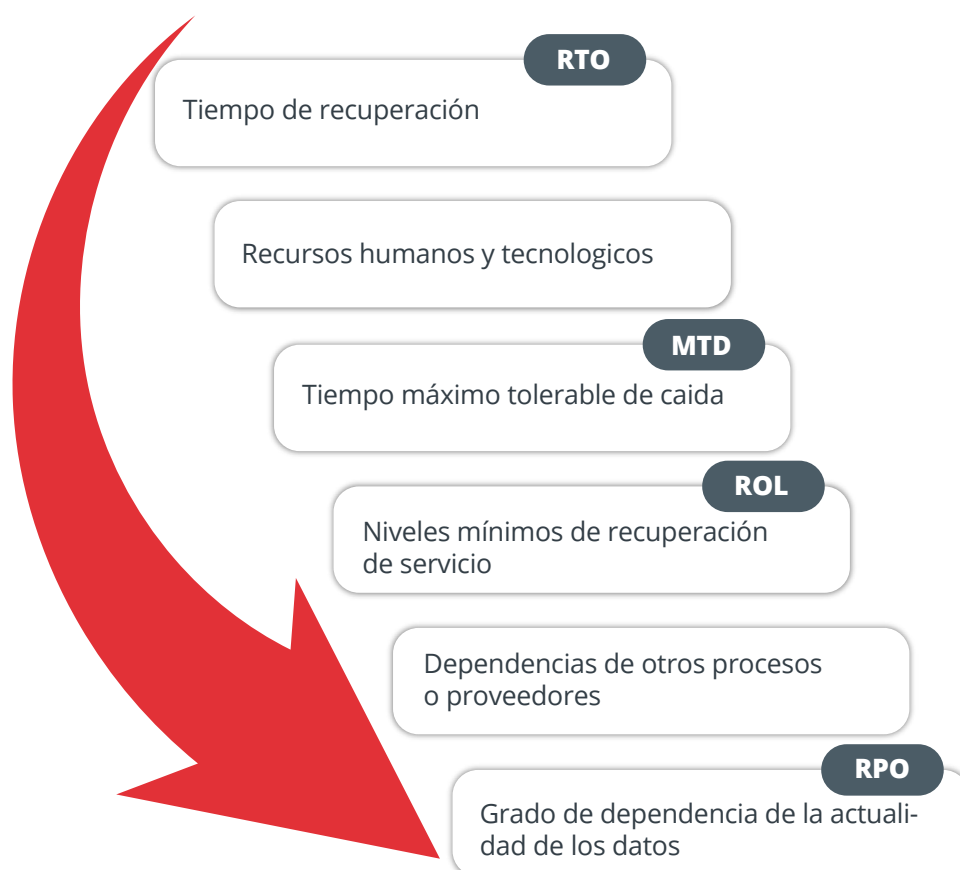


Ilustración 3
Análisis de impacto sobre el negocio

Para cada proceso que hayamos analizado, debemos haber obtenido los siguientes datos:

- ▶ **Tiempo de recuperación o RTO** (*Recovery Time Objective*). Este es el tiempo que un proceso permanecerá detenido antes de que su funcionamiento sea restaurado. Este valor tiene un gran componente de subjetividad.
- ▶ **Recursos humanos y tecnológicos empleados en el proceso.** En este punto debemos determinar las aplicaciones, sistemas, equipamiento y elementos auxiliares (impresora, fax, etc.) que cada proceso necesita para su funcionamiento en una situación de contingencia, así como los tiempos de recuperación que cada una de ellas tenga.
 - » En el caso de los recursos tecnológicos, debemos de considerar las dependencias con otra infraestructura tecnológica.
 - » En el caso de los recursos humanos, debemos identificar personal crítico sin reemplazo, ya sea por limitaciones de personal o por poseer *know-how* muy específico.
- ▶ **Tiempo máximo tolerable de caída o MTD** (*Maximum Tolerable Downtime*). Este es el tiempo que un proceso puede permanecer caído antes de que se

produzcan consecuencias desastrosas para nuestra empresa. Debemos tener en cuenta que esta valoración será en la mayoría de los casos subjetiva, ya que incluso si podemos medir cuantitativamente el impacto de una contingencia (en clientes no atendidos, ventas de la página web no realizadas, etc.), determinar en qué momento dicho impacto pone en riesgo la continuidad de nuestra empresa es una tarea muy compleja.

El **MTD** está relacionado con el negocio, mientras que el **RTO** será determinado, por lo general, por personal técnico. En todos los casos, el **RTO** debe ser inferior al **MTD**.

Por ejemplo, si el MTD de nuestro proceso de contabilidad son 72 horas y su RTO 24 horas, entonces:

- * Tardaremos 24 horas, con los recursos actuales, en poner en marcha de nuevo el proceso.
- * Si no recuperamos el proceso en 72 horas, el proceso puede dañar de manera irreversible a nuestra empresa.

- ▶ **Niveles mínimos de recuperación de servicio o ROL** (*Revised Operating Level*). Éste es el nivel mínimo de recuperación que debe tener una actividad

para que la consideremos como recuperada, aunque el nivel de servicio no sea el óptimo.

Esta variable puede ser establecida tanto en valores absolutos como porcentuales, y debe tener en cuenta el público objetivo o destinatario de la actividad del servicio, cumplimiento de compromisos satisfechos con terceras partes, porcentaje de la actividad habitual que es posible llevar a cabo, etc.

Aunque no siempre será posible determinar este valor, si nuestro proceso se basa por ejemplo en la atención de llamadas de clientes, podemos establecer un ROL en el 70%, tras lo cual consideraremos que el proceso está recuperado (lo que no implica que dejemos de aplicar las medidas de recuperación hasta el 100%).

- ▶ **Dependencias de otros procesos internos o proveedores externos.** En función de la criticidad de las actividades en las que el proveedor esté implicado, podemos solicitar a éste que indique si dispone de un Plan de Recuperación ante Desastres y qué intervalos temporales maneja. El propósito es verificar que una situación de desastre en un proveedor crítico no traslada dicha contingencia a nuestra empresa.

- ▶ **Grado de dependencia de la actualidad de los datos o RPO** (*Recovery Point Objective*). Este valor determina el impacto que tiene sobre la actividad la pérdida de datos. Este valor es crítico a la hora de determinar las políticas de copias de la organización, y no guarda relación con el **RTO** visto anteriormente.

Por ejemplo, nuestro proceso de contabilidad puede ser muy crítico, pero puede utilizar datos históricos del mes pasado, por lo que aunque su **RTO** sea muy alto, su **RPO** puede ser muy bajo.

Con la información obtenida, identificaremos principalmente los siguientes datos:

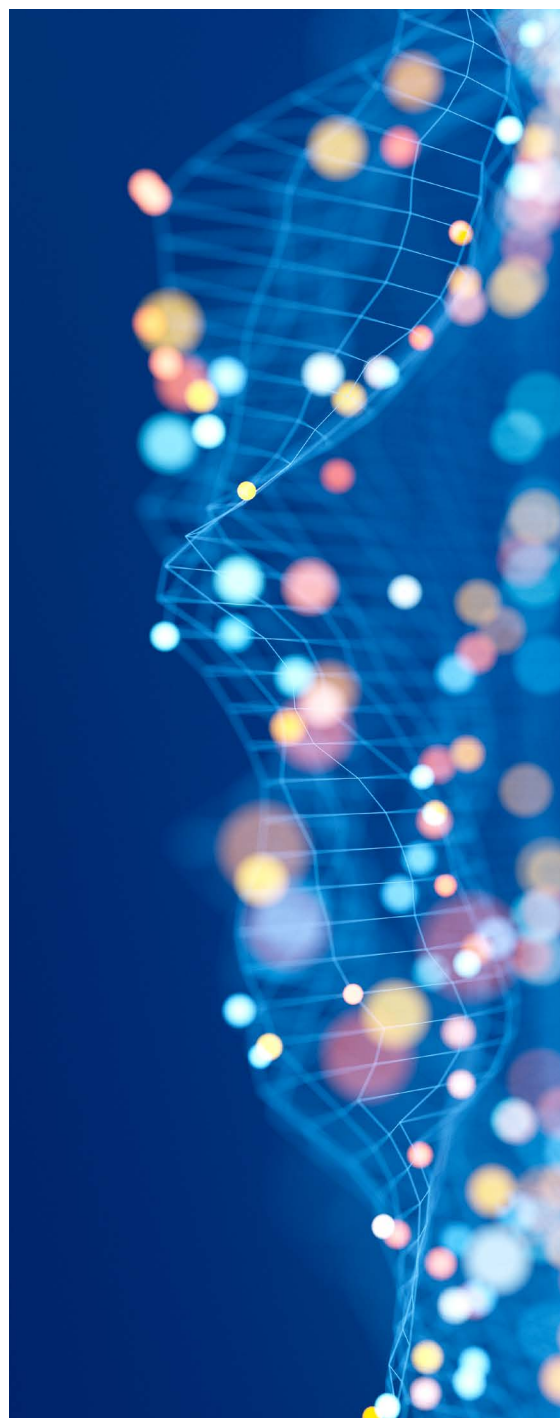
- ▶ Qué procesos debemos recuperar antes (de entre aquellos que componen el alcance), en función de su MTD. Los ordenaremos por MTD de más críticas a menos críticas. Es habitual establecer una escala dividida en tres rangos de valores; por ejemplo un MTD inferior a 24 horas, otro entre 24 y 72 horas, y uno superior a 72 horas.
- ▶ Qué aplicaciones debemos recuperar antes, en función de los procesos en los que intervengan.
- ▶ Las necesidades de copias de seguridad de cada proceso.

Debemos tener en cuenta que cuanto mayor sean las exigencias temporales y de garantía de conservación de los datos, los recursos que tendremos que invertir serán mayores. Dado que esta información nos la proporcionará cada departamento que esté implicado en el alcance, es recomendable realizar un ejercicio de evaluación adicional para detectar exigencias demasiado elevadas y no aceptar los requisitos sin una valoración previa.

Por ejemplo, aunque el responsable de contabilidad determine que su equipo no puede estar más de 2 horas sin acceso al correo electrónico, es posible que en el pasado dicha interrupción se haya producido sin consecuencias relevantes.

No obstante, es probable que los recursos para que dicho acceso no se interrumpa sean elevados.

Por tanto, debemos trasladar a los usuarios las implicaciones de los requerimientos que nos indican e instarles a considerar incidencias en el pasado, ausencias por enfermedad, etc.



3.2.3. ANÁLISIS DE RIESGO

A partir de la información obtenida en las reuniones iniciales, abordaremos la realización de un análisis de riesgos. Estudiaremos qué amenazas pueden materializarse afectando a los procesos del alcance, con qué probabilidad, qué impacto tendrían en éstos y qué activos de aquellos que intervienen en los procesos de negocio críticos (por ejemplo, aquellos con un MTD inferior a 24 horas) se verían afectados.

Para ello, realizaremos los siguientes pasos:

1. **Determinar las amenazas** a las que está expuesta la organización: robo de información sensible, inundación, pérdida de suministro eléctrico, caída del servidor de correo, etc. A diferencia de otros casos, en este tipo de proyectos nos centraremos en aquellas amenazas **que implican una indisponibilidad** de los procesos del alcance.
2. Una vez tenemos el listado de las amenazas, determinaremos **la probabilidad y el impacto** de cada una de esas amenazas. Esto puede hacerse utilizando una escala variable cualitativa, por ejemplo, de uno a cinco: de “Muy baja” a “Muy alta”. En este caso, nos interesan especialmente aquellos riesgos que impliquen un mayor impacto (y una probabilidad no despreciable), ya que son los que pueden poner en riesgo la continuidad de la organización. Nues-

tro propósito será identificar aquellos riesgos que pueden poner en peligro la continuidad o la información de los procesos críticos de la organización.

3. Por último, **realizaremos el producto de la probabilidad por el impacto de cada amenaza**, que nos servirá para identificar aquellos riesgos que debemos tratar con mayor prioridad. De esta manera obtenemos un listado de los riesgos de la organización, donde cada registro será una amenaza, un valor de impacto y uno de probabilidad.

Aunque estos tres pasos nos proporcionarán el conjunto de amenazas a las que estamos más expuestos, existen metodologías que permiten obtener resultados menos subjetivos y más fiables, pues tienen en cuenta variables como el valor de los activos, sus vulnerabilidades, etc.

Aunque lo mejor es poder establecer rangos de impacto asociados a valores temporales, de manera que nos sea posible relacionar el MTD/RTO con los tiempos de impacto de una amenaza, este aspecto es complejo de evaluar y determinar por la incertidumbre de la valoración de las amenazas.

Una vez establecidos los principales riesgos, es decir aquellos con mayor impacto, debemos tratarlos de manera adecuada [4] mediante una de las siguientes estrategias:

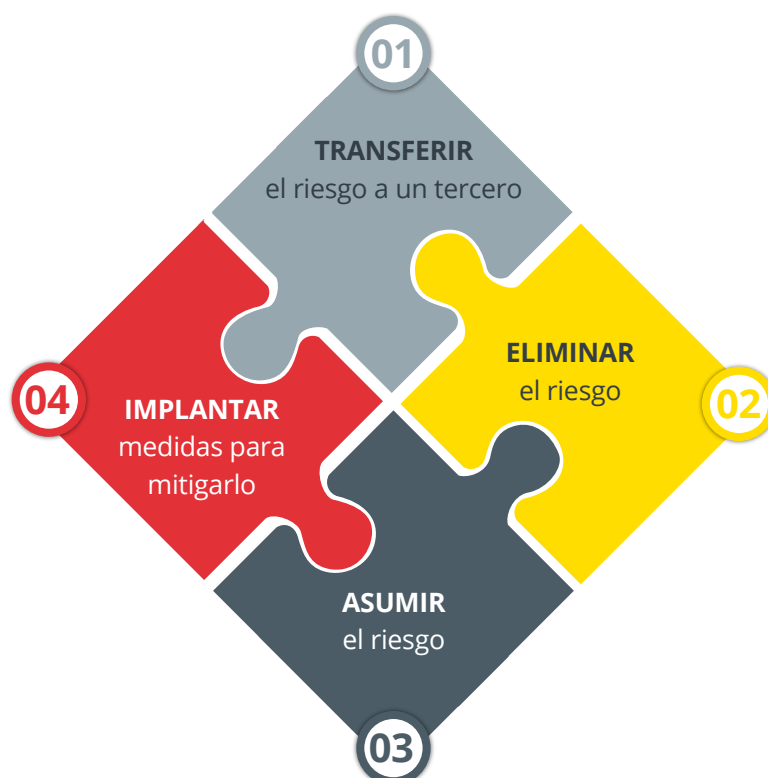


Ilustración 4
Estrategias para el tratamiento de los riesgos

Como respuesta a los riesgos, generaremos un **plan de tratamiento de riesgos** para cada uno de aquellos que superen el umbral determinado. En algunas ocasiones parte de estas medidas podrán ser consideradas posteriormente para la mejora de la continuidad.

Para cada medida, determinaremos:

- ▶ descripción de la medida o iniciativa, entendida ésta como un conjunto de controles de la misma naturaleza;
- ▶ riesgo o riesgos que mitiga;
- ▶ fecha de la implantación límite;
- ▶ responsable de la implantación;
- ▶ recursos necesarios para su implantación.

3.3. FASE 2: DETERMINACIÓN DE LA ESTRATEGIA DE CONTINUIDAD

Tras los pasos anteriores, deberemos disponer de la siguiente información:





-  Los procesos críticos del negocio, sus tiempos necesarios de recuperación y sus requisitos de pérdida de datos
-  Los recursos implicados en cada uno de los procesos: aplicaciones, etc...
-  Los tiempos de recuperación de cada uno de los recursos que puede garantizar nuestro personal técnico
-  Los riesgos a los que se encuentra sometida la infraestructura TI

Ilustración 5 *Información necesaria para establecer la Estrategia de Continuidad*

A partir de esta información, podremos determinar cuál es la diferencia entre las necesidades de los procesos de negocio incluidos en el alcance, y las capacidades de los recursos que utilizan. De este modo, identificaremos si los recursos actuales y sus estrategias de recuperación permitirían cubrir el **MTD** establecido para cada proceso.

Por ejemplo, nuestro proceso de contratación tiene un MTD de 24 horas. Éste utiliza: el correo electrónico, la aplicación específica de contabilidad y el acceso a un directorio departamental.

El email y el directorio departamental tienen un RTO de 8 horas, pero la aplicación específica de contabilidad tiene un RTO de 48 horas. Esto significa que si cae dicha aplicación, el proceso se interrumpirá durante un tiempo de 48 horas, implicando un deterioro grave de la actividad de nuestra empresa.

Por tanto, nuestro propósito debe ser implantar medidas que reduzcan este tiempo de recuperación por debajo del MTD de 24 horas. Como indicábamos antes, si ese MTD es de 8 horas, las medidas a implantar serán más costosas que en el caso de que sea de 48 horas.

Extendiendo este ejercicio a todos los procesos dentro del alcance y los diferentes ámbitos, debemos determinar qué estrategias seguir para cada uno de los diferentes elementos potencialmente afectados por una contingencia. Es decir, cómo recuperar un sistema para evitar que una contingencia lo degrade de manera irreversible para nuestra empresa.

Algunos elementos potencialmente afectables por una contingencia son los siguientes:

- ▶ **Personal.** Según el personal crítico identificado en el BIA, debemos evaluar las diferentes opciones para mitigar su ausencia.
- ▶ **Locales.** Deben evaluarse situaciones en las que no se disponga de ubicación para trabajar.
- ▶ **Tecnología.** Para las diferentes tecnologías implicadas en los activos que dan soporte al proceso se deben valorar posibles alternativas de funcionamiento o medidas complementarias.
- ▶ **Información.** Debemos considerar todos aquellos aspectos relacionados con la disponibilidad y salvaguarda de la información relacionada con los procesos críticos.
- ▶ **Proveedores.** Debemos garantizar que los proveedores críticos tienen

unos tiempos de respuesta acordes a las necesidades de nuestra empresa, y que no estamos expuestos a que nos trasladen sus posibles contingencias.

Como resultado de dicho proceso determinaremos las estrategias de recuperación más adecuadas a cada caso, teniendo en cuenta que algunos procesos pueden requerir varias estrategias de recuperación en función de su naturaleza y características.

Estas estrategias debemos implementarlas en una fase posterior, y para cada una de ellas debemos valorar el coste y viabilidad de su implantación, mantenimiento, recursos necesarios, etc., de manera que obtenamos un conjunto de iniciativas a implantar para mejorar la continuidad del proceso.

3.4. FASE 3: RESPUESTA A LA CONTINGENCIA

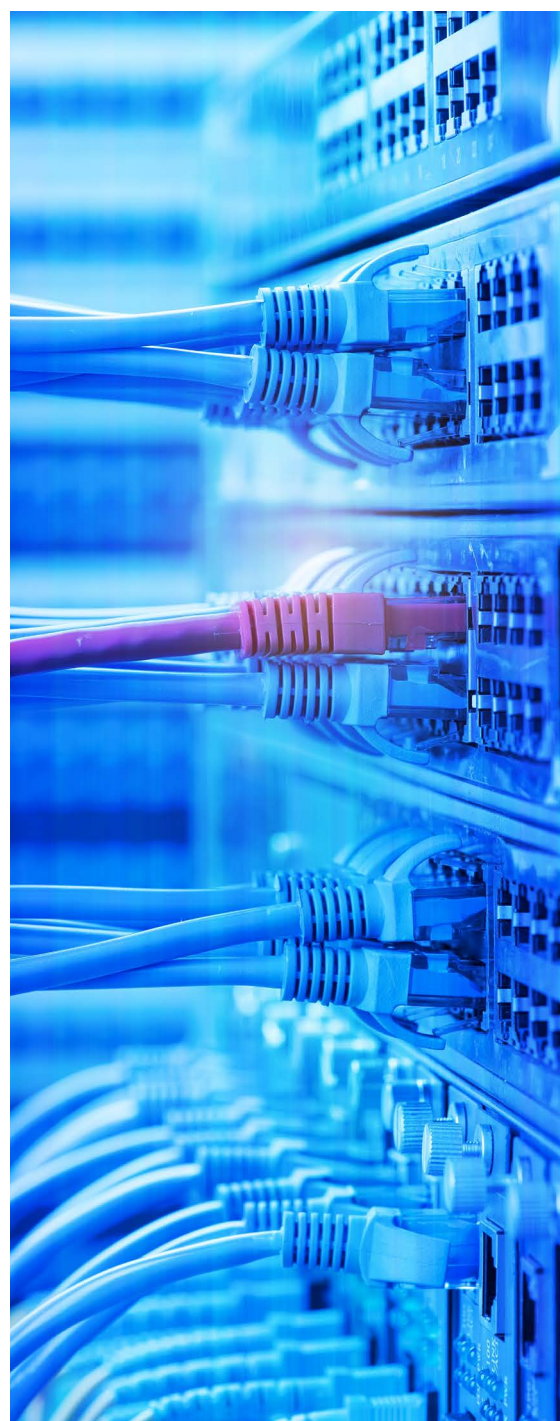
Una vez hemos definido, en el punto anterior, las estrategias de recuperación para cada uno de los elementos implicados en los procesos críticos afectados por una contingencia, esta fase es la encargada de implementar dicha estrategia.

Este proceso comienza con la **implantación de las iniciativas** identificadas en la anterior fase, y seguirá una fase de clasificación y priorización de medidas, en función del proceso afectado por su implantación y la criticidad de éste.

Durante la implantación, podemos abordar la fase de documentación de respuesta a la contingencia, y a partir de este punto nos centraremos en los elementos más relacionados con la tecnología, aunque son también aplicables a elementos que no sean tecnológicos.

Esta documentación se ejecuta en forma de árbol jerárquico, donde el elemento superior gestiona el momento crítico inmediatamente posterior a la crisis, los elementos intermedios ponen las bases para la recuperación de la infraestructura, y los nodos inferiores establecen los procedimientos técnicos detallados para dicha recuperación.

Este proceso lo organizamos en torno a los siguientes elementos que se detallan a continuación.



3.4.1. PLAN DE CRISIS (O DE INCIDENTES)

Este documento es el elemento central en la gestión de la situación de crisis, cuyo objetivo es evitar que tomemos decisiones improvisadas que puedan empeorar la crisis o que, simplemente, no se tomen.

Este plan contiene todos los elementos necesarios para la gestión de los momentos iniciales de una crisis:

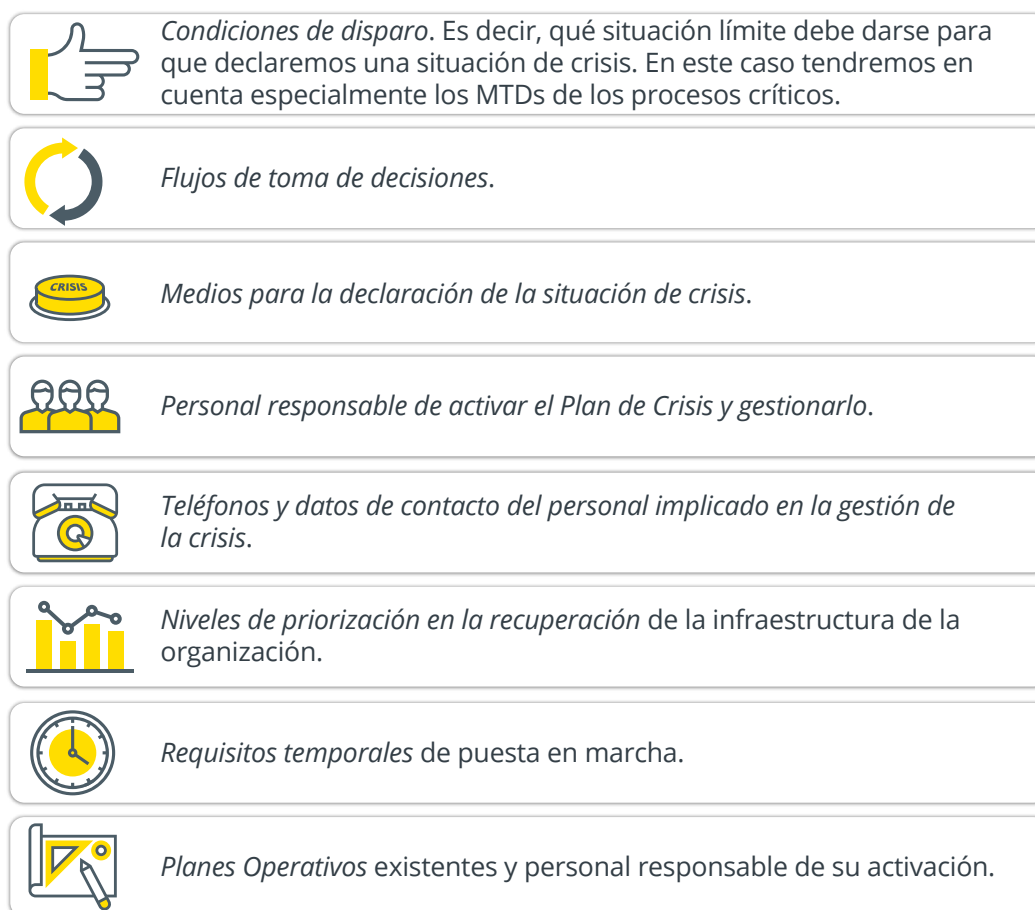


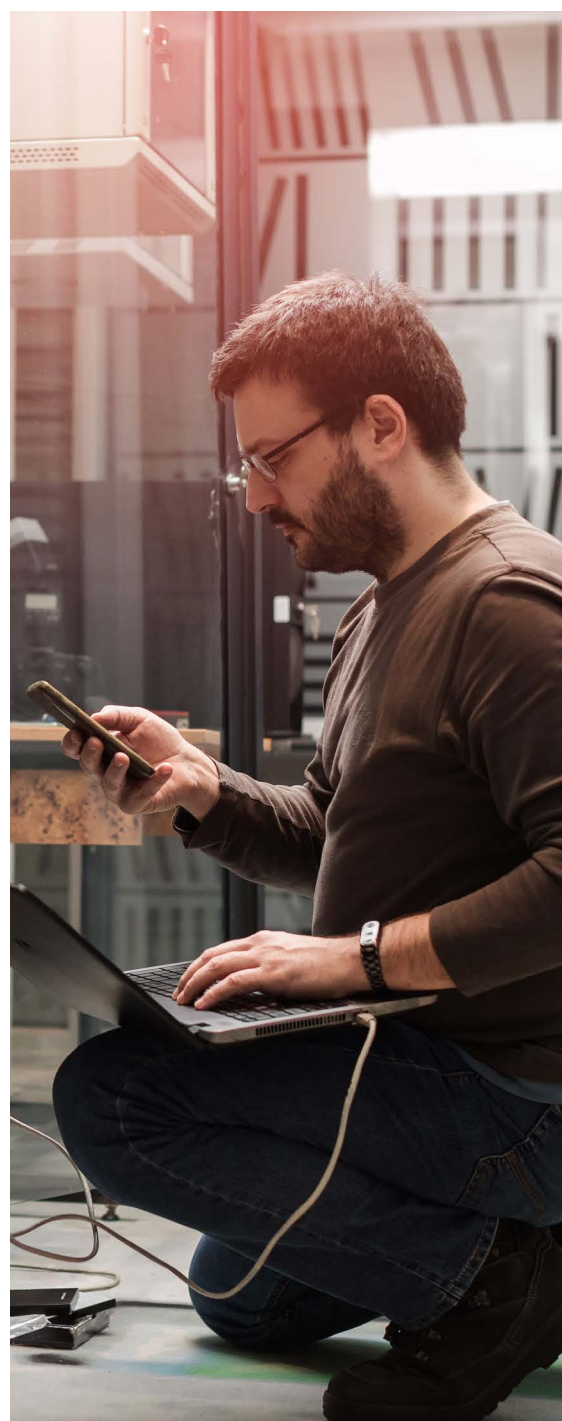
Ilustración 6
Elementos para la gestión inicial de una crisis

Tras la ejecución del Plan de Crisis, ya habremos gestionado el momento crítico de la crisis y puesto en marcha todos los procesos necesarios para la recuperación de la infraestructura afectada través de los Planes Operativos de Recuperación de Entornos **[5]**.

3.4.2. PLANES OPERATIVOS DE RECUPERACIÓN DE ENTORNOS

Una vez contenido el momento inicial de la crisis, debemos realizar una evaluación del alcance de la crisis y determinar qué Planes Operativos de Recuperación se activan. Estos documentos pueden abarcar uno o más entornos independientes y contienen información específica sobre el entorno al cual aplican. Por ejemplo, un entorno puede ser un ERP, el correo electrónico.

Tras el disparo de los diferentes Planes Operativos, cada una de las infraestructuras afectadas comenzará su proceso de recuperación, tomando como base para ello el elemento último de la ejecución de la estrategia de continuidad: los procedimientos técnicos de trabajo.



3.4.3. PROCEDIMIENTOS TÉCNICOS DE TRABAJO (O DE INCIDENTES)

Esta es toda documentación que describe cómo hemos de llevar las tareas necesarias para la gestión y recuperación de una aplicación, sistema, infraestructura o entorno. Aunque intrínsecamente no son parte de la continuidad del negocio sino de la operación diaria, es en una situación de crisis cuando se vuelven más importantes.

Por tanto, estos documentos contienen gran cantidad de información específica a cada uno de los entornos: direcciones IP, versionado de programas, listado detallado de comandos, tablas de enrutamiento, recuperación de copias de base de datos, puesta en marcha de aplicaciones, etc.



3.5. FASE 4: PRUEBA, MANTENIMIENTO Y REVISIÓN

Un Plan de Continuidad TIC tiene como objeto gestionar de la manera óptima en tiempo y forma una situación de crisis no prevista, reduciendo así los tiempos de recuperación y vuelta a la normalidad. Por tanto, es imperativo que lo mantengamos actualizado en todo momento y que su vigencia sea comprobada regularmente.

Por ejemplo, un plan de continuidad TIC no actualizado puede implicar que el personal reflejado en la documentación ya no trabaje en nuestra empresa, que las versiones de las aplicaciones sean diferentes a las documentadas, que los teléfonos de contacto sean erróneos, etc. Esto puede ser muy grave en una situación de contingencia.

Para ello, es necesario llevar a cabo diferentes **pruebas** sobre los entornos que hayamos definido en el alcance, con diferentes grados de complejidad y elaboración. Entre todas las pruebas, debemos realizar pruebas de todos los entornos al menos una vez al año para cubrir el conjunto de amenazas que hemos definido como potencialmente catastróficas.

En la ejecución de las pruebas, es necesario llevar a cabo una planificación previa que tenga en cuenta los siguientes aspectos:

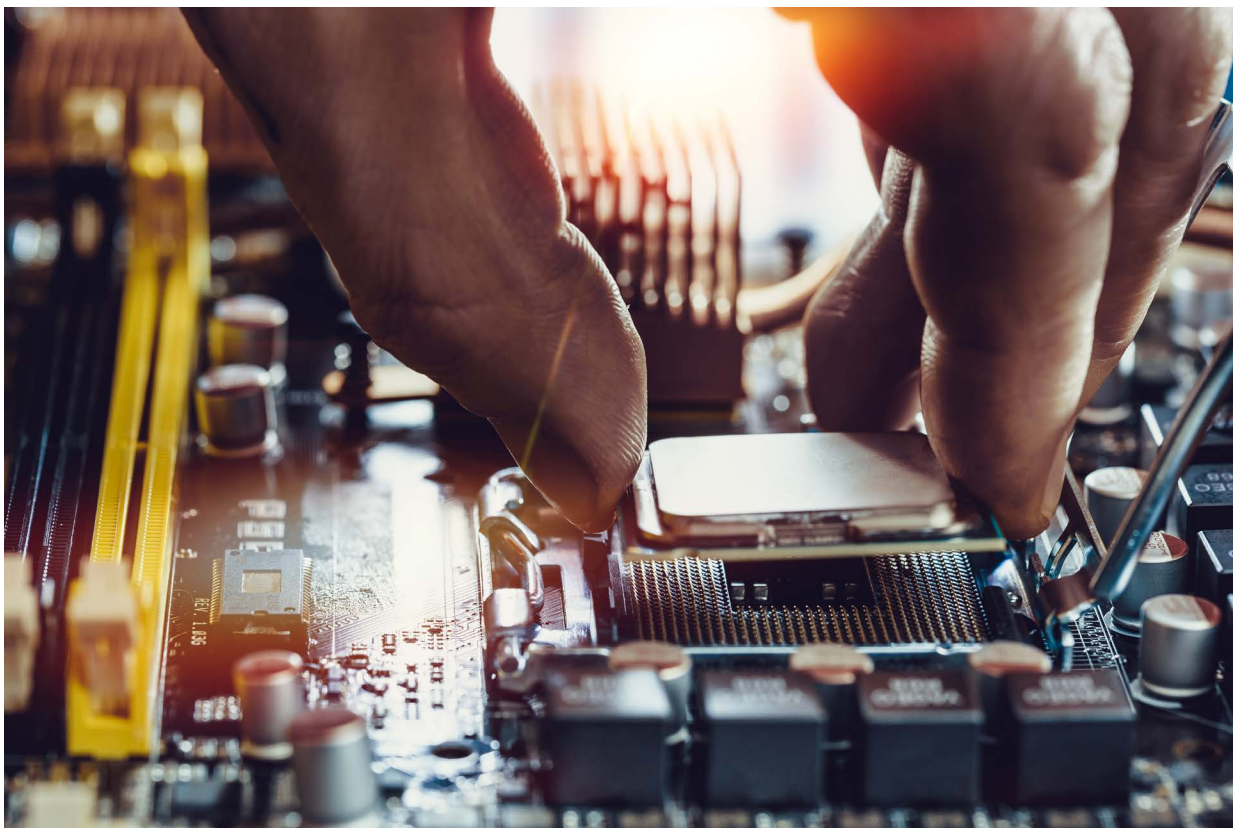
- ▶ personal técnico implicado en la prueba;
- ▶ usuario del aplicativo implicado en la prueba;
- ▶ personal externo implicado en la prueba: clientes, proveedores, etc;
- ▶ descripción de la prueba a realizar;
- ▶ descripción del resultado esperado tras la ejecución de la prueba;
- ▶ hora y fecha de realización; debemos tener en cuenta que siempre que la prueba pueda implicar una pérdida de servicio, ya sea ejecutada con éxito o no, debe planificarse ésta en un horario de mínimo impacto.

Tras la prueba, deberá elaborarse un informe que recoja los resultados y describa las posibles incidencias surgidas durante ésta: resultados no esperados, tiempos estimados superados, mala comunicación con el personal, indisponibilidad de proveedores, etc.

Cualquier incidencia que se haya producido debe analizarse para la aplicación de las medidas correctoras que sean necesarias.

Algunas posibles pruebas que pueden realizarse, siempre teniendo en cuenta que éstas dependen de la idiosincrasia de cada organización y que deben analizarse y planificarse cuidadosamente, son las siguientes:

- ▶ Realizar la comprobación de que ante una caída del suministro eléctrico, el sistema de alimentación ininterrumpida y el grupo electrógeno entra en funcionamiento.
- ▶ Verificar los tiempos de recuperación de los posibles repositorios documentales de la organización en una máquina de pruebas. Los permisos de los ficheros deben ser los que cada fichero tenía antes de la recuperación.
- ▶ Recuperación de las aplicaciones críticas del negocio (y los datos asociados) en máquinas instaladas durante la prueba.
- ▶ Acceso remoto a la infraestructura desde una ubicación remota.
- ▶ Si disponemos de entornos replicados o en configuración de clúster, debemos garantizar que ambos elementos pueden funcionar de manera independiente, y que ante la caída de uno de ellos, el otro dispositivo funciona correctamente.



3.5.1. PLAN DE MANTENIMIENTO

El propósito es mantener actualizada toda la documentación cada vez que se produzca un cambio significativo en la organización, a nivel de infraestructuras TIC, de personal, o de cualquier otro aspecto implicado en los procesos críticos.

Esto permitirá que la documentación que tengamos que utilizar en una situación de crisis refleje fielmente la información de los distintos actores involucrados en los procesos: infraestructura técnica, personal, proveedores externos y terceras partes que deben tenerse en cuenta en una situación de contingencia.

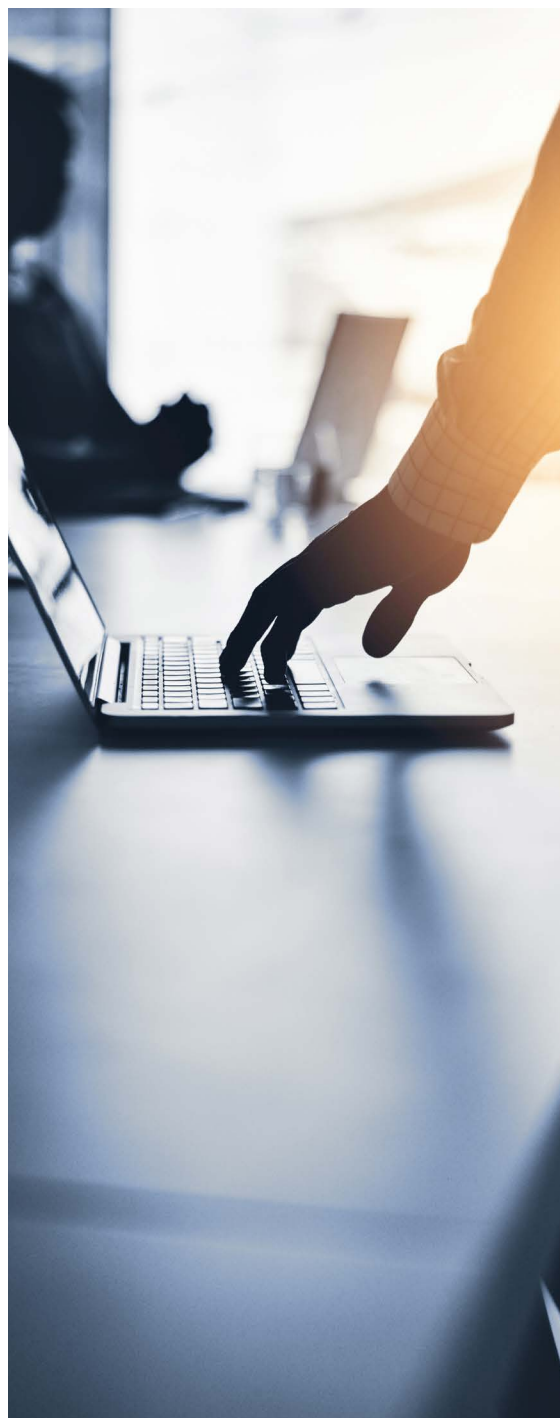


3.5.2. PLAN DE PRUEBAS

El objetivo es mostrar los distintos tipos de pruebas de contingencia que debemos llevar a cabo. A pesar de que el **plan de mantenimiento** contiene aquellos eventos que deben disparar una revisión o modificación del sistema (por ejemplo, el cambio de un proveedor, atravesar con éxito una fase de crisis), en la ejecución de los planes de prueba es vital para garantizar la salud del PCTIC.

Esto permite:

- ▶ garantizar que la información del plan se mantiene actualizada;
- ▶ garantizar que en situación de contingencia, la organización podrá recuperarse en los tiempos establecidos, aspecto que puede determinar la continuidad de la organización;
- ▶ incrementar la cohesión del personal implicado en una potencial contingencia;
- ▶ mejorar el conocimiento de los usuarios en relación con las pruebas de continuidad;
- ▶ incrementar la confianza de los usuarios en la organización.



3.6. FASE 5: CONCIENCIACIÓN

Como última fase de la implantación de nuestro Plan de Continuidad de Negocio TIC, pero no por ello menos importante, debemos llevar a cabo aquellas tareas que incrementen la concienciación del personal **[6]** en relación con la continuidad. Debe realizarse tanto del personal implicado en los procesos de negocio, como del personal de TI.

En concreto, debemos plantear un proceso de concienciación que contemple la descripción de los elementos que utilizamos en la continuidad (análisis de impacto sobre el negocio, plan de crisis, estrategias de recuperación, etc.). Además deben de considerarse aspectos como las responsabilidades, pruebas que debemos realizar, etc.

El público objetivo en este caso deberá ser tanto el personal técnico como el personal de negocio que tenga algún tipo de relación con los procesos críticos dentro del alcance.



4.

RESUMEN

Tal y como hemos visto, podemos resumir las tareas para realizar un Plan de Continuidad TIC en los siguientes pasos:

- ▶ Determinar el **alcance** de los servicios y procesos objeto de la mejora de su continuidad.
- ▶ Realizar **reuniones** con los departamentos implicados y determinar sus necesidades y requerimientos.
- ▶ Realizar reuniones con personal técnico y determinar con qué capacidades y **recursos** cuentan.
- ▶ Identificar los **servicios y procesos críticos** junto con los **activos** tecnológicos que los sustentan y sus dependencias.
- ▶ Obtener los **riesgos** a los que están expuestos los servicios y procesos.
- ▶ Identificar qué **medidas** o iniciativas llevar a cabo para que las capacidades tecnológicas sean superiores a las demandas de negocio.
- ▶ Elaborar el **plan de crisis** para identificar las primeras acciones a realizar cuando ocurre un accidente.
- ▶ Elaborar los **planes de recuperación** para cada entorno implicado en el alcance.
- ▶ Elaborar las **instrucciones técnicas** de trabajo para poder llevar a cabo el plan de recuperación.
- ▶ Elaborar el **plan de mantenimiento** e implantarlo.
- ▶ Elaborar el **plan de pruebas** e implantarlo, realizando comprobaciones periódicas para verificar que son correctas.
- ▶ Realizar la **formación** al personal implicado en el Plan de Continuidad de Negocio.

5.

REFERENCIAS

[Ref - 1]. Banco de España «Recomendaciones relativas a la continuidad de negocio» - https://www.bde.es/f/webbde/COM/Supervision/politica/ficheros/es/Recomendaciones_relativas_a_la_continuidad_del_negocio.pdf

[Ref - 2]. INCIBE, Políticas de seguridad para la pyme «Continuidad de negocio» - <https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/continuidad-negocio.pdf>

[Ref - 3]. INCIBE, Plantilla ejemplo para el inventario básico de activos para BIA - <https://www.incibe.es/sites/default/files/contenidos/dosieres/plan-contingencia-continuidad-negocio/plantilla-ejemplo-bia.xls>

[Ref - 4]. INCIBE, Gestión de riesgos. Una guía de aproximación para el empresario - <https://www.incibe.es/protege-tu-empresa/guias/gestion-riesgos-guia-empresario>

[Ref - 5]. INCIBE, Plantilla ejemplo para un plan de recuperación de entornos - <https://www.incibe.es/sites/default/files/contenidos/dosieres/plan-contingencia-continuidad-negocio/contingencia-y-continuidad-de-negocio-plan-de-recuperacion.pdf>

[Ref - 6]. INCIBE, KIT de concienciación para empresas - <https://www.incibe.es/protege-tu-empresa/kit-concienciacion>



GOBIERNO
DE ESPAÑA

MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL



INSTITUTO NACIONAL DE CIBERSEGURIDAD



protege
tu empresa