INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

Deloitte.

Guía práctica para PYMES:
cómo implantar un Plan de Continuidad de Negocio

OBSERVATORIO DE LA **SEGURIDAD** DE LA **INFORMACIÓN**

Edición: Octubre 2010

El Instituto Nacional de Tecnologías de la Comunicación (INTECO), sociedad estatal adscrita al Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología.

La misión de INTECO es aportar valor e innovación a los ciudadanos, a las pymes, a las Administraciones Públicas y al sector de las tecnologías de la información, a través del desarrollo de proyectos que contribuyan a reforzar la confianza en los servicios de la Sociedad de la Información en nuestro país, promoviendo además una línea de participación internacional. Para ello, INTECO desarrollará actuaciones, al menos, en líneas estratégicas de Seguridad Tecnológica, Accesibilidad, Calidad TIC y Formación.

El Observatorio de la Seguridad de la Información (http://observatorio.inteco.es) se inserta dentro de la línea estratégica de actuación de INTECO en materia de Seguridad Tecnológica, siendo un referente nacional e internacional al servicio de los ciudadanos, empresas, y administraciones españolas para describir, analizar, asesorar y difundir la cultura de la seguridad y la confianza de la Sociedad de la Información.

Datos de contacto:
Instituto Nacional de Tecnologías de la Comunicación (INTECO)
Observatorio de la Seguridad de la Información
Avda. José Aguado, 41. Edificio INTECO. 24005 León
Teléfono: +(34) 987 877 189 / Email: observatorio@inteco.es
www.inteco.es

Deloitte presta servicios de auditoría, asesoramiento fiscal y legal, consultoría y asesoramiento en transacciones corporativas a entidades que operan en un elevado número de sectores de actividad. La firma aporta su experiencia y alto nivel profesional ayudando a sus clientes a alcanzar sus objetivos empresariales en cualquier lugar del mundo. Para ello cuenta con el apoyo de una red global de firmas miembro presentes en más de 140 países y con más de 168.000 profesionales que han asumido el compromiso de ser modelo de excelencia.

Deloitte cuenta con un grupo encargado de realizar servicios correspondientes a la gestión del riesgo informático que se denomina Enterprise Risk Services (ERS). Este grupo está formado por cerca de 200 profesionales, 7 socios en España y varios miles de especialistas a nivel mundial, dedicados exclusivamente a servicios de auditoría informática, seguridad informática, identificación y gestión de los riesgos de las operaciones asociados a los sistemas de información, así como a servicios enfocados a mantener el nivel de control interno requerido en la utilización de la tecnología. Como parte de la estrategia de diferenciación en los servicios prestados, debemos destacar la cualificación de su equipo de profesionales, quienes atesoran más de 300 certificaciones en materia de seguridad de la información, continuidad de las operaciones y auditoría informática.

Datos de contacto:
Deloitte
Plaza Pablo Ruíz Picasso, 1. Torre Picasso. 28020 Madrid
Teléfono: +(34) 915 14 50 00
Fax: + (34) 915 14 51 80
Si desea información adicional, por favor, visite www.deloitte.es

Depósito Legal: LE-1496-2010
Imprime: gráficas CELARAYN, s.a.

INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

Deloitte.

Guía práctica para PYMES:
cómo implantar un Plan de Continuidad de Negocio

Índice

1. ¿A quién va dirigida?

Los principios de esta guía, si bien están dirigidos especialmente a la pequeña y mediana empresa española, así como a los profesionales autónomos, son aplicables a cualquier empresa española, sin importar el sector, la actividad, la ubicación geográfica, la posible dispersión en múltiples sedes ni el tamaño de la entidad. Posteriormente el tiempo, el esfuerzo y el presupuesto son los parámetros que diferirán ampliamente en función del tamaño de la empresa.

De forma más concreta, la intención de esta guía es que sea explotada por aquel al que le ha sido encomendada la responsabilidad de ejecutar las medidas orientadas a garantizar la continuidad de sus actividades de negocio (ya sea el área de tecnología y sistemas, el área de auditoría o gestión de riesgos, o incluso personal al que se le encarga la gestión sin tener conocimientos previos).

Las razones por las que esta guía va dirigida principalmente a la PYME española son varias:

- Según el Directorio Central de Empresas (DIRCE) de 2009, más del 99% del tejido empresarial español está constituido por pequeñas empresas (las microempresas constituyen el 94,8% y las pequeñas el 4,4%), lo que constituye el motor principal de la economía y de la producción en España.

- El grado de implantación de planes de continuidad de negocio en las pequeñas y medianas empresas españolas es notablemente inferior si se compara con las grandes empresas. Todas las empresas españolas, independientemente de su sector de actividad, son conscientes de la importancia de aplicar este tipo de planes, pero principalmente las grandes disponen de recursos técnicos, económicos y humanos necesarios para convertir esta necesidad en una realidad tangible.

- A partir de los estudios realizados por INTECO sobre seguridad de la información en el ámbito de la empresa, se evidencian lagunas en el conocimiento y una falta de recursos en la PYME española en materia de continuidad de negocio.

2. ¿Por qué es importante la continuidad?

La competitividad creciente entre las organizaciones empresariales, las demandas cada vez más exigentes de clientes y *stakeholders*, o los requerimientos regulatorios cada vez más restrictivos, son factores que hoy en día fuerzan a las empresas a demostrar la resistencia de las actividades de negocio a permanecer activas ante cualquier contingencia grave.

Una caída de la luz, una inundación, un incendio o un robo han de considerarse amenazas reales que deben ser tratadas de forma preventiva para evitar, en caso de que éstas sucedan, que las pérdidas sean tan graves que afecten a la viabilidad del negocio. Son múltiples las organizaciones que, independientemente de su tamaño, fracasan o incluso desaparecen por la falta de procesos, mecanismos y técnicas que mitiguen los riesgos a los que están expuestas y garanticen una alta disponibilidad en las operaciones de su negocio.

De este modo, es necesario que las organizaciones establezcan una serie de medidas técnicas, organizativas y procedimentales que garanticen la continuidad de las actividades o procesos de negocio en caso de tener que afrontar una contingencia grave.

> Uno de los principales inconvenientes o barreras a las que se enfrenta una organización cuando decide abordar cualquier tipo de iniciativa relacionada con la continuidad de negocio es la falta de conocimiento y de instrucciones claras y concisas que detallen por dónde empezar y qué aspectos deben tenerse en cuenta para garantizar el éxito.

Esta guía trata de salvar estos niveles de desorientación a través de un marco de actuación para aquellas organizaciones que deseen entender y abordar los principios y las prácticas de continuidad de negocio de una forma integral (desde el momento inicial en el que se reconoce la necesidad de desarrollar un programa o estrategia de continuidad, hasta su mantenimiento y actualización constante).

3. ¿Cuál es la utilidad de esta guía?

Esta guía tiene el objetivo de identificar y explicar de forma desglosada las actividades necesarias para diseñar, implantar y mantener un Plan de Continuidad de Negocio, proporcionando, siempre que sea posible, gráficos, ejemplos ajustados a las necesidades reales de la pequeña y mediana empresa española y experiencias de casos de éxito con los que compararse. Así, se pretende que la organización asimile y entienda cada una de las fases y tareas que componen dicho Plan.

Si bien existen multitud de manuales, estándares y recomendaciones que tratan de guiar a las organizaciones a adoptar estrategias de continuidad de negocio, la mayoría de ellas son teóricas, expresadas con un lenguaje formal, y no tienen en cuenta la situación, la problemática, las necesidades reales o los niveles de conocimiento por parte de este tipo de organizaciones.

INTECO ha tratado de cubrir estas deficiencias a lo largo del diseño y elaboración de esta guía, teniendo en cuenta la situación actual de la PYME española desde el punto de vista de la tecnología y la seguridad de la información, las principales barreras a las que se enfrentan cuando deciden abordar planes de continuidad de negocio, así como los principales errores en los que suelen incurrir en la citada materia.

El resultado es un documento en el que se expone de forma clara y sencilla los aspectos a considerar y las actividades a desarrollar por cualquier organización que desee estar preparada ante posibles incidencias de seguridad que puedan paralizar la entrega de sus productos y/o servicios.

Esta guía nace para que la pequeña y mediana empresa española (PYME) se familiarice con la continuidad de negocio y comprenda por qué es necesario tener planes preventivos orientados a garantizar la continuidad de sus operaciones ante una situación de contingencia, qué aspectos tiene que tener en cuenta para el desarrollo de su estrategia de continuidad y qué beneficios proporciona disponer del mismo.

Del mismo modo, la guía pretende resaltar y concienciar a las organizaciones acerca de la importancia crítica que tiene asegurar la continuidad de sus operaciones, así como la necesidad de hacer frente de forma proactiva a incidentes graves de seguridad.

Esta guía no es en absoluto un conjunto de requerimientos específicos, sino que, basándose en la experiencia, expone buenas prácticas y recomendaciones acerca de las fases y actividades que conviene adoptar.

4. ¿Por qué es necesario adoptar un plan de continuidad de negocio?

Los recientes acontecimientos prueban que las organizaciones no pueden estar preparadas para todos y cada uno de los eventos adversos que pueden sucederles y que pueden impactar en sus actividades de negocio.

El fallo de la red eléctrica de Barcelona en julio de 2007 que impactó en servicios críticos como sanidad y transporte, el incendio del edificio Windsor en Madrid en el año 2005, el atentado terrorista de las Torres Gemelas en el 2001, e incluso caídas de los servicios de telefonía y ADSL en los correspondientes operadores son ejemplos de sucesos de gravedad crítica que afectan a las organizaciones, a los gobiernos y a los ciudadanos.

Cada año son millones las organizaciones que padecen inundaciones, incendios, ataques terroristas, actos vandálicos y otras amenazas. Las compañías que logran superar estos traumas son las previsoras, las que están preparadas para enfrentarse a lo peor, las que estiman los posibles daños que pueden sufrir y ponen en marcha las medidas necesarias para protegerse.

Toda organización depende de sus recursos, del personal y de las tareas que día a día son ejecutadas con el fin de mantener los beneficios y la estabilidad. La mayoría posee bienes tangibles, empleados, sistemas y tecnologías de información, etc. Si alguno de estos componentes es dañado o deja de estar accesible por la razón que sea, la organización puede paralizarse. Cuanto mayor sea el tiempo de inactividad, mayor es la probabilidad de que tenga que comenzar de nuevo desde cero. Incluso muchas organizaciones no son capaces de recuperarse después de ser víctima de algún desastre.

Adicionalmente, en ocasiones existe la percepción errónea de interpretar como una falta de confianza o una señal de debilidad el hecho de que una organización anticipe que algún componente de su actividad de negocio puede fallar. Nada más lejos de la realidad.

La adopción de una estrategia de continuidad constituye un ejercicio de responsabilidad y predisposición a anticiparse a cualquier tipo de evento adverso que haga peligrar el negocio.

Aparte de prevenir o minimizar las pérdidas para el negocio que un desastre puede causar, el objetivo principal de cualquier programa orientado a gestionar la continuidad de negocio de una organización es garantizar que ésta dispone de una respuesta planificada ante cualquier trastorno importante que puede poner en peligro su supervivencia. Esta afirmación de por sí constituye un argumento irrefutable que explica la necesidad de instaurar en todas las compañías tales estrategias, independientemente de su tamaño y/o sector de actividad.

Además puede aportar otros beneficios:

- **Ventaja competitiva frente a otras organizaciones:** el hecho de mostrar que se toman medidas para garantizar la continuidad de negocio mejora la imagen pública de la organización y revaloriza la confianza frente a accionistas, inversores, clientes y proveedores.

Por otra parte, el retorno de la inversión (ROI) en aspectos de continuidad es más perceptible en términos de reputación e imagen pública.

- **Gestión preventiva de los riesgos:** a través de la gestión de la continuidad, una organización es capaz de abordar la gestión proactiva de amenazas y riesgos que pueden impactar en sus operaciones.

- **Previene o minimiza las pérdidas** de la organización en caso de desastre: es capaz de identificar de forma proactiva los posibles impactos e inconvenientes que una interrupción de sus actividades de negocio puede provocar.

- **Asegura la "resiliencia" de las actividades de negocio ante interrupciones**, aumentando la disponibilidad de los servicios dispuestos para el cliente.

- **Menor riesgo de sufrir sanciones económicas al adaptarse a requerimientos regulatorios**: para algunos sectores de actividad (como por ejemplo la normativa MiFID para las compañías de actividades y servicios de inversión para particulares ubicadas en los estados miembros de la Unión Europea, o el programa para la Protección de las Infraestructuras Críticas impulsado por la Comisión Europea), la adopción de planes de continuidad de negocio es un requerimiento regulatorio que debe ser satisfecho. El cumplimiento de tal requerimiento evita el riesgo de sufrir sanciones económicas.

- **Asignación más eficiente de las inversiones en materia de seguridad:** tal y como se detalla en la presente guía, todo plan de continuidad de negocio está diseñado conforme a un proceso previo de análisis de riesgos, el cual permite priorizar los mismos y fijar los esfuerzos y los presupuestos en las áreas más necesitadas.

5. ¿Por dónde empezar?

Como paso previo al proceso formal de desarrollar e implantar un plan de continuidad de negocio, toda organización debe tener en consideración 6 aspectos claves que son descritos a continuación:

1. **Tiempo y recursos:** toda estrategia para abordar la implantación de un Plan de Continuidad de Negocio requiere de tiempo y recursos (humanos, económicos e incluso tecnológicos). Dicho requerimiento convierte a las direcciones de las organizaciones en un componente clave para apoyar la gestión de continuidad y dotar de tales recursos a la organización.

2. **Implicación y compromiso de la dirección:** reforzando el punto anterior, la dirección, como ente que toma las decisiones y proporciona los fondos necesarios, debe ser concienciada y debe estar convencida de la necesidad de este tipo de planes.

   Esta misión de concienciación a menudo resulta un proceso complejo por varias razones: los canales de comunicación con la dirección no siempre son fluidos, el lenguaje empleado en términos de "riesgo", "impacto", "vulnerabilidad" y otros conceptos relacionados con la seguridad y las tecnologías de la información puede no ser el idóneo para que sea entendido y asimilado por la dirección.

   Para conseguir el citado apoyo de la dirección, es necesario dirigirse a la misma en términos más tangibles y de negocio como son los costes de implantar los planes de continuidad y los beneficios que éstos proporcionan. Otro aspecto útil en este sentido es el cálculo del coste de la interrupción de un proceso de negocio en términos financieros, el cual dependerá de varios factores como la pérdida de ingresos durante la interrupción, la disminución de la productividad del trabajador e incluso la pérdida de imagen y reputación de la organización.

Así por ejemplo, el citado cálculo para una entidad cuya actividad principal es la comercialización y venta de bienes por Internet debería contemplar: el número de interrupciones que puede tener en un año, el tiempo (por ejemplo, en horas) que no va a poder dar servicios y el coste por hora que conlleva la interrupción de su actividad:

Coste de la interrupción al año: 3 interrupciones x 1,5 horas x 2.000 €/h= 9.000 €.

De esta forma, la dirección tendrá información más tangible que le permitirá entender qué riesgos está asumiendo y evaluar si es necesario abordar un plan de continuidad de negocio.

3 **Conocer la organización es necesario y crítico**: los procesos de negocio, el apoyo de los mismos en las Tecnologías de la Información (TI), el conocimiento de personas clave para la organización, los productos y servicios, la estrategia de negocio o las metas de la organización, los procesos internos, etc. Toda organización debe conocer cuál es su ámbito de negocio y los procesos que le permiten desarrollar su actividad.

La esperanza de que una organización recupere sus actividades tras un desastre es nula si no dispone previamente de un buen conocimiento acerca de cómo funciona. Ante esta afirmación, es frecuente la postura de muchas organizaciones al pensar que "obviamente, una compañía conoce cómo funciona". Pero si se analiza este asunto detenidamente, muchas de ellas se sorprenderían de lo verdaderamente complicado que resulta entender y asimilar su funcionamiento al nivel de detalle que es requerido para poder reconstruir sus actividades en caso de que sea necesario. Cada miembro de la plantilla conoce sus funciones y sus responsabilidades al detalle, aunque si se tiene en cuenta que cada actividad de negocio está constituida por infor-

mación, funciones, redes, personas, tiempo, interdependencias, etc., difícilmente se puede identificar a alguien que sea capaz de explicar todos y cada uno de los procesos de negocio de su organización.

4 **Definir el alcance:** un paso clave que una organización debe abordar cuando decide impulsar un plan de continuidad de negocio es decidir acerca del alcance del mismo. En ocasiones el plan de continuidad exigido es demasiado extenso si se aplica a toda la organización, y termina fracasando. Por ello, es importante determinar qué áreas, procesos de negocio o productos/servicios de la organización serán incluidos en el plan. Incluso en los casos en los que la organización tenga varias sedes, será necesario establecer un alcance geográfico.

En este sentido, algunas preguntas que deben contemplarse cuando la organización trata de determinar el alcance de su estrategia de continuidad son:

- ¿Cuáles son las actividades más importantes y críticas de la compañía?
- Desde el punto de vista financiero, operativo, legal o asociado a la imagen de la compañía, ¿qué impacto tendría una interrupción los servicios o de los procesos de la empresa?
- ¿Durante cuánto tiempo puedo permitirme que la entrega de mis productos o servicios esté interrumpida?

5 **Colaboración de las áreas que componen la empresa:** un plan de continuidad de negocio impacta y necesita del apoyo y la colaboración de las diferentes áreas de la organización: los proyectos de continuidad de negocio tienen que contar con enfoques no solo tecnológicos, sino también de negocio (relación con proveedores de servicio, recursos humanos, atención al cliente, recursos financieros, recurso logísticos, etc.).

6 **Plantearse la necesidad de asesoramiento externo**: conocer si es necesario disponer o no de ayuda especializada y saber dónde encontrarla, ya que muchos de los problemas a los que se tiene que enfrentar una organización para implantar su plan de continuidad de negocio ya han sido analizados y solucionados por otras empresas previamente.

6. Estructura de la guía

A continuación se presentan las fases que deben ser abordadas en toda gestión de continuidad de negocio:

- **Fase I. Diseño del Plan y establecimiento de la Política de Continuidad de Negocio:** comprende la identificación de las actividades que deben ser realizadas de forma previa para comenzar el proceso de desarrollo e implantación del Plan de Continuidad.

- **Fase II. Conocimiento de los procesos de negocio de la organización y análisis de riesgos que impactan en las actividades de negocio:** con el fin de identificar los productos y servicios clave de la PYME, los recursos clave que soportan estas actividades y los riesgos a los que está expuesta.

- **Fase III. Medidas preventivas:** esta fase plantea la posibilidad de aplicar medidas de seguridad preventivas y proactivas con la intención, en la medida de lo posible, de evitar o gestionar los incidentes graves, sin necesidad de activar el plan de continuidad de negocio a no ser que sea estrictamente necesario.

- **Fase IV. Estrategia de recuperación:** considerando que no todas las actividades de negocio tienen las mismas prioridades de recuperación, esta fase establece los objetivos y las prioridades de recuperación en función de los riesgos que impactan en las operaciones de negocio.

- **Fase V. Desarrollo e implantación del Plan:** conjunto de prácticas, procedimientos a seguir y tecnologías para la recuperación de

las operaciones críticas después de producirse un desastre. Dichos procedimientos deben soportar las estrategias de recuperación previamente seleccionadas.

- **Fase VI. Mantenimiento del Plan:** teniendo en cuenta que todo Plan de Continuidad de Negocio debe ser difundido, revisado, actualizado y probado regularmente, esta fase describe acciones de difusión y formación del Plan, así como las pruebas y el proceso de mejora continua del mismo.

7. Fase I: Diseño del plan y establecimiento de la política de continuidad de negocio

7.1. OBJETIVOS

En esta fase, y tras haber obtenido el soporte y las inversiones necesarias, la empresa que decide abordar un plan continuidad de negocio debe averiguar qué se va a hacer y por qué.

7.2. TAREAS

7.2.1. DESIGNAR UN COORDINADOR DE CONTINUIDAD DE NEGOCIO

Una tarea clave de esta fase es designar un coordinador/líder que se encargará de gestionar y supervisar el proceso de elaboración e implantación del plan de continuidad de negocio.

E incluso, si la inversión lo permite y en función del tamaño de la organización y el alcance del plan, es recomendable asignar personal adicional y constituir un equipo de continuidad de negocio.

El coordinador o el equipo deben trabajar con la dirección para identificar el alcance y los objetivos que persigue el plan, así como las actividades de negocio que son críticas en la organización.

Adicionalmente, el perfil o perfiles de las figuras encargadas de la gestión de la continuidad de negocio en una PYME no tiene que estar forzosamente localizado en las áreas de tecnología y sistemas (tal y como muchas organizaciones asumen y derivado de la idea perenne de que los procesos de continuidad de negocio están constituidos principalmente por componentes tecnológicos).

7.2.2. ELABORAR LA POLÍTICA DE CONTINUIDAD DE NEGOCIO

En paralelo, y con el fin de formalizar un marco de actuación que determine los objetivos, y el alcance (actividades de negocio incluidas) del plan, así como las funciones y responsabilidades del mismo, debe elaborarse la política de continuidad de la organización. Normalmente es la figura citada en el apartado anterior el encargado de diseñar y elaborar esta política.

Generalmente la citada política es entendida como un documento sencillo, claro y conciso que establece a alto nivel (estratégico) los objetivos, el alcance y las responsabilidades en la gestión de la continuidad de negocio en la organización.

A continuación se muestra un ejemplo de plantilla de una Política de Continuidad de Negocio que permite conocer con más exactitud el enfoque que con frecuencia es aplicado a la elaboración de la misma:

INTRODUCCIÓN

En la que se detalle de forma resumida la materia tratada (Plan de Continuidad de Negocio), la estructura del documento y lo que se persigue a través del mismo.

OBJETIVOS

En este apartado se detallan los objetivos que serán satisfechos mediante la aplicación de la propia política, como garantizar la continuidad de las actividades y de los servicios, aplicar los procedimientos de contingencia y planes de respuesta necesarios, etc.

ALCANCE

Indica los procesos u operaciones de negocio que son cubiertos por la política, así como los recursos que soportan los citados procesos. Si aplica, también puede llegar a considerarse la zona geográfica sujeta a las instrucciones marcadas por la política.

RESPONSABILIDADES

Relación de los diferentes responsables implicados de una forma u otra en la gestión de la continuidad de negocio (gerencia, coordinador, equipo, áreas de negocio, proveedores de servicio, etc.) junto con una descripción detallada de sus funciones y obligaciones (gestión de riesgos, asignación y distribución de los recursos, desarrollo de procedimientos de respuesta, realización de pruebas periódicas, formación, etc.).

7.2.3. ESTABLECER LA PLANIFICACIÓN DEL PROYECTO

Finalmente el coordinador o equipo de continuidad debe aplicar sus habilidades de gestión de proyectos para programar y desarrollar los siguientes componentes del plan de trabajo: tareas a llevar a cabo para satisfacer los objetivos descritos en la política de continuidad, responsables de ejecutar tales tareas, tiempos de ejecución, hitos, presupuestos, plazos e indicadores de éxito.

7.3. RIESGOS ASOCIADOS AL DISEÑO DEL PLAN Y ESTABLECIMIENTO DE LA POLÍTICA DE CONTINUIDAD DE NEGOCIO

Con más frecuencia de la deseada, las organizaciones no disponen de un perfil con las capacidades y aptitudes necesarias para afrontar con garantías la adopción de un plan de continuidad de negocio. Este hecho se acentúa más cuanto menor es el tamaño de la organización.

7.4. RECOMENDACIONES

El coordinador formalmente designado es la persona competente para gestionar y supervisar el desarrollo y la implantación del plan de continuidad de negocio, por lo que es importante que disponga de las siguientes capacidades o conocimientos:

- Liderazgo.
- Conocimiento de la organización y de sus actividades de negocio.
- Habilidades sociales de comunicación, ya que está previsto que interaccione de forma fluida con las diferentes áreas de la organización que probablemente tengan otras prioridades.
- Capacidad para gestionar proyectos: planificación, definición de recursos necesarios, seguimiento, reporte, etc.

Para aquellas organizaciones que constituyen un equipo de continuidad de negocio, es aconsejable que esté formado por personal que pertenezca o conozca las diferentes actividades de negocio (tecnología y sistemas, financiero, comercial, recursos humanos, etc.), ya que los riesgos y amenazas varían en función de dicha actividad y deben ser puestos en común, identificados y priorizados.

Por otro lado, se hace necesario remarcar que el contenido de la política de continuidad de negocio debe ser claro, sencillo y conciso, con el fin de evitar interpretaciones o expectativas erróneas. Para ello es aconsejable, aparte del conocimiento de la organización y de esta guía, la investigación de fuentes externas en busca de publicaciones y buenas prácticas emitidas por organismos especializados, estándares, etc.

8. Fase II: Conocimiento de los procesos de negocio de la organización y análisis de riesgos

8.1. OBJETIVOS

Identificados los objetivos y el alcance de la gestión de continuidad de negocio a través de la citada Política de Continuidad de Negocio, la empresa debe:

- Entender la organización mediante la identificación de productos y servicios clave, así como las actividades y recursos críticos que los soportan.
- Estimar el impacto y las consecuencias de los posibles fallos en esas actividades y recursos críticos.
- Identificar y valorar los riesgos que podrían interrumpir la entrega de los productos y servicios de la empresa, así como de los recursos sobre los que están soportados.
- Adicionalmente, la externalización de determinados servicios u operaciones abre un nuevo ámbito de gestión, ya que es frecuente que la responsabilidad de continuidad de negocio para los servicios externalizados no sea transferida al proveedor o tercero.

8.2. TAREAS

8.2.1. ESTUDIAR LOS PROCESOS Y ACTIVIDADES DE NEGOCIO

Tanto las actividades de negocio que se encargan del desarrollo de productos y servicios de la organización, como los recursos/activos[3] que dan so-

3 En materia de riesgos y continuidad de negocio es común hablar indistintamente de "activos" o de "recursos" como aquello que es necesario en una organización para la consecución de sus actividades y objetivos de negocio.

porte a dichas actividades deben ser identificados y analizados describiendo las personas implicadas, la información y las aplicaciones empleadas, los proveedores utilizados, etc.

Adicionalmente, es importante considerar que toda organización es un ente complejo de equipamiento, personas, tareas, departamentos, mecanismos de comunicación y relaciones con proveedores externos, los cuales pueden prestar servicios críticos que deben ser considerados. Uno de los desafíos más grandes en continuidad de negocio es entender todas las complejidades e interrelaciones existentes. Son las llamadas interdependencias internas y externas.

> Una organización puede implantar copias de seguridad, redundancia de equipos informáticos y suministros eléctricos, formación y entrenamiento de sus empleados, etc. Pero si no conoce cómo todos estos componentes interactúan para dar forma a una actividad de negocio, cualquier iniciativa terminará resultando una pérdida de tiempo de trabajo efectivo.

A modo de ejemplo, se presenta una tabla que incluye que las actividades de negocio de una organización y que podría servir como punto de arranque del trabajo de identificar y conocer en detalle todas las operaciones de negocio de la organización:

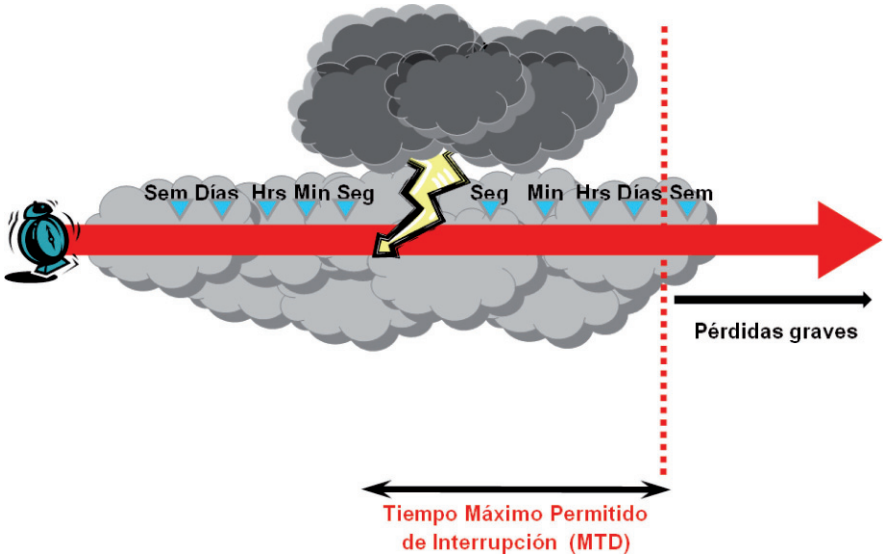
Área	Actividades de negocio
Recursos Humanos	• Administración de personal • Gestión de nóminas • Control de presencia • Desarrollo del personal
Compras	• Relación con proveedores • Gestión de pedidos
Ventas	• Comercialización de productos • Marketing • Facturación • Gestión de impagos
Producción	• Generación del producto/servicio
Administración y finanzas	• Contabilidad • Cuentas de resultados • Tesorería
Asesoría jurídica	• Gestión contractual • Gestión societaria
Auditoría interna	• Auditoría de las actividades de negocio • Reporting a la dirección
Tecnología y Sistemas	• Automatización y eficiencia de los procesos • Innovación

8.2.2. IDENTIFICAR Y VALORAR EL IMPACTO ASOCIADO A LAS INTERRUPCIONES DE LOS PROCESOS DE NEGOCIO

Es necesario que las empresas realicen el esfuerzo de identificar y valorar el impacto que podría tener en la organización si una actividad se paralizase, así como el tiempo de interrupción que puede ser soportado por la organización hasta que las pérdidas no sean asumibles (tiempo máximo permitido de interrupción o MTD por sus siglas en inglés).

En la siguiente ilustración se muestra, a modo de ejemplo, la línea temporal que marca un desastre y la estimación del tiempo máximo permitido de interrupción (MTD) para una determinada actividad de la organización.

Línea temporal en la que se localiza el Tiempo Máximo Permitido de Interrupción



Las siguientes son algunas estimaciones de tiempos máximos permitidos de interrupción que pueden ser empleados por las empresas para conocer la criticidad de sus actividades y/o de sus recursos: no prioritario (30 días); normal (7 días); importante (72 horas); urgente (24 horas) y crítico (minutos u horas).

Por ejemplo, si una compañía que comercializa sus productos por Internet sufre la caída de su línea de conexión a Internet durante 3 horas y consecuentemente calcula que las pérdidas asociadas a la interrupción ascienden a 60.000 €, la citada línea de comunicación será considerada un recurso crítico para la compañía y tendrá que adoptar una estrategia de continuidad prioritaria consistente en implantar una línea de comunicación redundante y alternativa.

En este punto es necesario destacar que el impacto total asociado a la paralización de alguna actividad de la organización depende de varios factores:

Tipos de Impacto	Descripción del Impacto
Operativos	Actividades de negocio que dejan de estar en funcionamiento o el coste de las horas de trabajo perdidas por los empleados
Económicos	Costes directos o indirectos como por ejemplo el lucro cesante o el daño emergente
Regulatorios o contractuales	Sanciones por incumplimiento legal o penalizaciones por incumplimiento del contrato con clientes
Imagen	Relación de aspectos más intangibles y por tanto más difíciles de valorar como la imagen, la fiabilidad y la reputación de la organización frente a clientes, proveedores y accionistas

Todos ellos deben ser considerados para que las conclusiones del análisis y las estimaciones sean completas y veraces.

En la siguiente ilustración se detalla cualitativamente y a modo de ejemplo la secuencia para calcular el impacto (retraso en la elaboración de las nóminas y descontento de los empleados) que puede tener la paralización del proceso de gestión de nóminas de la organización derivado de la indisponibilidad de la tecnología que lo soporta.

Ejemplo cálculo de impacto sobre una actividad de negocio de la empresa

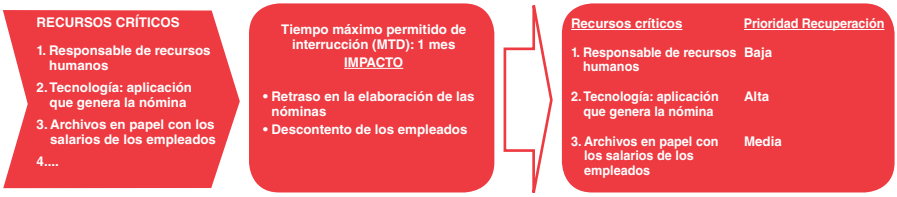
O aún más sencillo: si una organización sufriera una interrupción en su conexión a Internet, sería un problema que no pudiera realizar transacciones financieras, procesar pedidos o comunicarse con el personal.

8.2.3. IDENTIFICAR ACTIVIDADES, RECURSOS CRÍTICOS Y PRIORIDADES DE RECUPERACIÓN ASOCIADAS

La organización, a la hora de identificar y priorizar las actividades y recursos críticos, debe tener en cuenta aquellos que, en caso de pérdida, tendrían el mayor impacto sobre la actividad empresarial en el menor tiempo posible y, por tanto, necesitarían ser restaurados con mayor inmediatez.

Siguiendo con el gráfico anterior, se muestra como ejemplo la valoración cualitativa de las prioridades de recuperación (alta, media o baja) de los recursos críticos (responsable de Recursos Humanos, tecnología y archivos en papel) que soportan el proceso de gestión de nóminas a partir de la ya explicada estimación del impacto.

Ejemplo cálculo de prioridades de recuperación sobre los recursos críticos de una actividad de negocio de la empresa



Es decir, del hecho de concluir que la tecnología que habilita el proceso de gestión de nóminas tiene una prioridad de recuperación "alta", se deriva que dicho recurso es crítico y por tanto más importante que otros (responsable de Recursos Humanos o archivos en papel) desde el punto de vista de su recuperación.

Otros ejemplos de identificación de recursos críticos pueden ser:

- Las redes de comunicaciones en organizaciones que dependen de las comunicaciones internas y externas para funcionar adecuadamente.
- Los sistemas de alimentación energética en aquellas compañías que requieren de suministro eléctrico para fabricar sus bienes.
- El conocimiento del fundador y gerente de la empresa, el cual es el único que dispone de la experiencia y entendimiento detallado de sus actividades de negocio.
- El listado de clientes y contactos comerciales disponible únicamente en soporte papel.

Existen dos parámetros muy específicos que están estrechamente relacionados con la recuperación: Tiempo de Recuperación Objetivo (***RTO***) y Punto de Recuperación Objetivo (***RPO***).

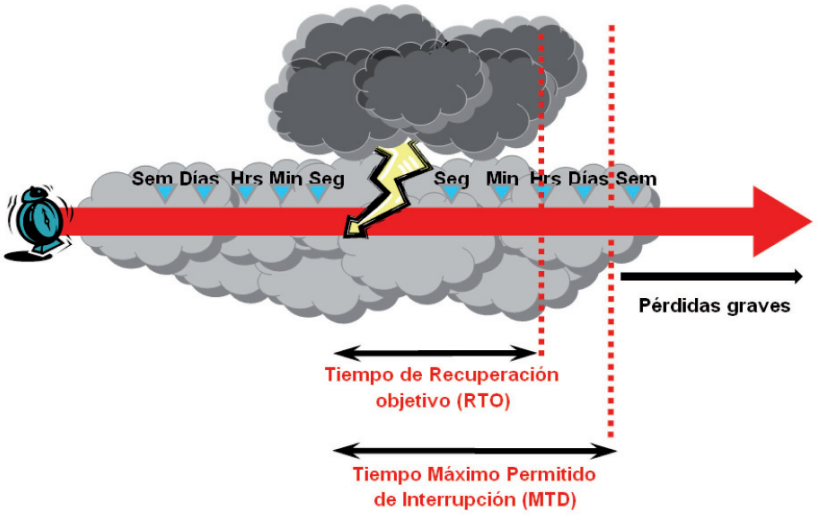
El RTO establece la urgencia que las diferentes unidades de negocio precisan para volver a su funcionamiento habitual. Por tanto, determina los plazos en los que deben volver a funcionar con normalidad. Estos pueden establecerse en períodos de tiempo en función de la criticidad de los procesos y pueden ser cuestión de horas o semanas en aquellos procesos prescindibles. Por tanto, se trata de identificar el orden en que hay que tratar de reconstruir la actividad, recuperando antes aquellos procesos cuya paralización suponen un mayor impacto para la organización. En una situación de crisis siempre hay recursos limitados y es necesario elegir qué hacer primero atendiendo a un criterio de negocio.

El RPO se refiere al punto más reciente en el tiempo en el que los sistemas pueden ser recuperados, reflejando por tanto cuánta es la cantidad de información que una organización puede permitirse perder sin que le afecte negativamente. Por tanto, el RPO determina la periodicidad con la que deben salvaguardarse los datos para todos aquellos procesos de negocio.

Cuanto más cortos son el RTO y el RPO, más complejos y caros son los planes de continuidad de negocio. Estos dos parámetros deciden también las diferentes estrategias de recuperación que serán explicadas en el apartado 10 de esta guía.

La siguiente ilustración muestra visualmente el concepto Tiempo de Recuperación Permitido (RTO) y su relación con el Tiempo Máximo Permitido de Interrupción (MTD) (considerando la ocurrencia en algún momento del tiempo de un desastre):

Ubicación en el tiempo del RTO y el MTD antes de que una empresa sufra pérdidas graves



Las tareas identificadas hasta ahora a lo largo de esta fase (estudiar los procesos, calcular el impacto e identificar las actividades) conforman el comúnmente denominado **Análisis de Impacto en el Negocio (BIA).**

El BIA constituye la base para elaborar un plan de continuidad de negocio y consiste en describir qué pérdidas potenciales tendrá la organización si alguna de sus actividades de negocio (por ejemplo la facturación o el pago de las nóminas de los empleados) o de los recursos que las soportan (por ejemplo los sistemas informáticos) se paraliza. Este análisis va a permitir que las organizaciones sepan qué recursos van a tener que proveer al plan de recuperación y en qué orden para restablecer y recuperar la operativa después de un desastre.

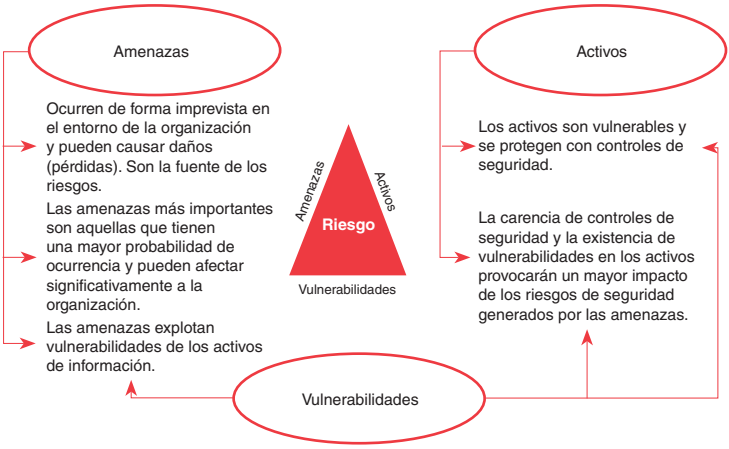
8.2.4. ANÁLISIS DE RIESGOS

¿Con qué probabilidad puede ocurrir un desastre o una interrupción severa de mis servicios o actividades críticas?

El alcance del proceso de análisis de riesgos enmarcado en la implantación de un plan de continuidad de negocio es acotado, ya que la organización debe tener presente los factores y la probabilidad que pueden desencadenar una interrupción de sus actividades críticas.

El análisis de riesgos consiste en identificar las amenazas sobre estos activos y su probabilidad de ocurrencia, las vulnerabilidades asociadas a cada activo y el impacto que las citadas amenazas pueden provocar sobre la disponibilidad de los mismos.

Interrelaciones entre las variables que componen el riesgo (activo, amenaza, vulnerabilidad)



Si bien existen diversas metodologías de análisis de riesgos (MAGERIT, OCTAVE), e incluso herramientas que ayudan a automatizar el proceso (EAR/PILAR), todas ellas siguen la siguiente secuencia de acción:

- Identificar activos: para cada una de las actividades críticas de la organización, es necesario identificar y valorar los activos involucrados. La mayor parte de esta tarea debiera haber sido completada en el BIA.

- Identificar y evaluar las amenazas sobre los activos identificados previamente y su probabilidad de que sucedan. Aunque existen diversas tipologías de amenazas, algunos ejemplos de ellas son fuego, inundación, fallo eléctrico, absentismo laboral, huelgas, etc.

- Identificar y valorar las vulnerabilidades o debilidades asociadas a los activos, las cuales pueden ser explotadas por las amenazas.
- Valorar el impacto resultante de que una amenaza se aproveche de una vulnerabilidad del activo y provoque daño sobre el mismo.
- Calcular el riesgo como la probabilidad de que se produzca un impacto determinado en la organización.

El proceso de análisis de riesgos puede ser abordado de forma cualitativa, cuantitativa o incluso mezcla de ambos. En la siguiente tabla se describen los 2 tipos de análisis de riesgos junto con las ventajas e inconvenientes asociados a los mismos.

Descripción de tipos de análisis de riesgos

Tipo de Análisis de Riesgos	Descripción	Ventajas	Inconvenientes
Cualitativo	Basado en clasificaciones descriptivas y subjetivas del riesgo	• Sencillez • Rapidez • Equilibrio Coste-Beneficio • Uso extendido	Subjetividad
Cuantitativo	Basado en términos monetarios	• Exactitud • Objetividad	Complejidad para estimar costes reales

Para que la empresa se familiarice y comprenda de forma más concreta el enfoque aplicado sobre los tipos de análisis de riesgos descritos, se expone a continuación un ejemplo de cada uno de ellos:

Ejemplo de Análisis de Riesgos Cualitativo

Partiendo de que el Riesgo (R) es la Probabilidad (P) de que una amenaza explote una vulnerabilidad asociada a un activo:

Riesgo (R)= Impacto (I) x Probabilidad (P)

Donde:

* *Impacto (I)= f (criticidad del activo, gravedad de la vulnerabilidad). Posibles valores: alto, medio o bajo.*
* *Probabilidad (P)= f (frecuencia de la amenaza, facilidad de explotación de la vulnerabilidad). Posibles valores: alto, medio o bajo.*

La empresa estima que existe una alta probabilidad (P) de que una inundación (amenaza) inutilice la oficina (activo) situada en el sótano del edificio (vulnerabilidad) y paralice sus actividades provocando un impacto (I) alto. En función de la siguiente matriz de evaluación cualitativa:

IMPACTO				
	ALTO	RIESGO MEDIO	RIESGO CRÍTICO	RIESGO CRÍTICO
	MEDIO	RIESGO BAJO	RIESGO MEDIO	RIESGO CRÍTICO
	BAJO	RIESGO BAJO	RIESGO BAJO	RIESGO MEDIO
		BAJO	MEDIO	ALTO
		PROBABILIDAD		

** Riesgo (R)= Impacto (I) Alto x Probabilidad (P) Alta= Riesgo crítico*

Ejemplo de Análisis de Riesgos Cuantitativo

Si se quiere calcular el daño o la pérdida en términos monetarios que la inundación citada en el ejemplo anterior puede provocar en la organización:

Daño o pérdida= Valor del activo (€) x Factor de Exposición (%) x Probabilidad de Ocurrencia

Donde:

* *La oficina de la organización, valorada en 100.000 €, es el activo valorado.*
* *El Factor de Exposición es el porcentaje (%) del activo que se vería dañado como consecuencia de la inundación. Si la organización considera que la inundación daña la totalidad de la oficina, el factor de exposición sería del 100% (si estima que solo se queda inutilizada la mitad de la oficina, el factor de exposición sería del 50%).*
* *La probabilidad de ocurrencia de la amenaza (inundación) es calculada en función del número de veces que la amenaza puede ocurrir en un año. Si se estima que una inundación puede ocurrir una vez cada diez años:*

Probabilidad de Ocurrencia= 1 vez / 10 años= 0,1 veces/año

De esta forma el daño o la pérdida que puede sufrir el activo se estima:

Daño o pérdida= 100.000 € x 100% x 0,1 veces/año= 10.000 €

Independientemente de la metodología o de las herramientas empleadas para el análisis de riesgos, el resultado del proceso será un mapa de riesgos que permite identificar y priorizar aquellos que pueden provocar una paralización de las actividades de negocio de la organización o de los recursos críticos sobre los cuales dichas actividades están soportadas.

¿Qué puede hacer la organización ante los riesgos que ha identificado? Existen diferentes opciones para hacer frente a los mismos:

- **Aceptar el riesgo:** la organización conoce el riesgo y decide asumirlo sin tomar ninguna acción al respecto, bien porque no tiene capacidad o bien porque el coste para mitigar el riesgo es desproporcionado para los beneficios que aporta.

- **Transferir el riesgo:** como por ejemplo a través de la subcontratación de servicios o mediante la contratación de un seguro de cobertura, de forma que si el riesgo se materializa exista una compensación externa que lo mitigue.

- **Reducir el riesgo a niveles aceptables por la organización:** mediante el diseño y la implantación de controles o medidas preventivas o que atenúen los impactos y las consecuencias del mismo (ver Fase III: Medidas preventivas).

- **Evitar el riesgo:** mediante la eliminación del mismo (por ejemplo a través de la reingeniería de procesos o incluso suspendiendo la actividad que origina el riesgo sin penalizar los objetivos de negocio de la organización).

Las distintas opciones para hacer frente a los riesgos pueden ser utilizadas conjuntamente, si bien es destacable que no todos los riesgos pueden ser reducidos o prevenidos a un nivel aceptable.

La continuidad de negocio constituye por sí misma una estrategia o una opción de respuesta para hacer frente a aquellos riesgos que pueden interrumpir las operaciones de la organización.

8.3. RIESGOS ASOCIADOS AL CONOCIMIENTO DE LOS PROCESOS DE NEGOCIO Y ANÁLISIS DE RIESGOS

Si la organización o los responsables en materia de continuidad de negocio no interpretan correctamente los riesgos a los se expone y cómo impacta la paralización de sus actividades de negocio, son varios los problemas que pueden surgir:

- Dificultad para preparar la respuesta ante incidentes de seguridad.
- Identificación y priorización errónea de los impactos en el negocio y de los riesgos.
- Derivado del punto anterior, deficiencias para seleccionar las prioridades y los procedimientos de recuperación más adecuados.

Por otro lado, es habitual que las organizaciones adopten procesos de gestión de riesgos que generan matrices de análisis complejas y engorrosas de desarrollar y mantener, perdiendo la visión a alto nivel y el "sentido común" necesario para determinar en última instancia qué riesgos deben ser tomados en consideración.

8.4. RECOMENDACIONES

El Análisis de Impacto de Negocio (BIA) y el Análisis de Riesgos son procesos fundamentales que soportan el plan de continuidad de negocio y deben ser abordados con la estrecha colaboración de aquellas figuras que conocen en detalle las actividades de la organización. De esta forma los resultados finales serán fiables.

Adicionalmente, y en alusión a los diferentes métodos de análisis de riesgos, es preferible que la organización adopte un enfoque cualitativo. Aparte de ser más utilizado, este enfoque permitirá un proceso sencillo, ágil y factible en tiempo y recursos necesarios para su ejecución.

9. Fase III: Medidas preventivas

9.1. OBJETIVOS

El propósito de esta fase consiste en aplicar medidas de seguridad que eviten en la medida de lo posible que se produzcan incidentes de seguridad que, al no ser gestionados adecuadamente, hagan necesaria la activación del plan de continuidad de negocio.

9.2. TAREAS

9.2.1. IDENTIFICACIÓN Y APLICACIÓN DE MEDIDAS DE SEGURIDAD

Tomando como base los resultados del BIA y del análisis de riesgos, la organización debe identificar y aplicar controles o medidas de seguridad que:

- **Reduzcan la probabilidad** de que las actividades críticas sufran interrupciones.
- **Disminuyan el tiempo** de una eventual interrupción.
- **Limiten el impacto** que una paralización de las actividades críticas pueda provocar en la organización.
- **Incrementen la fortaleza del negocio** mediante la eliminación de puntos de fallo únicos (accesos, procesos, clientes, etc.)

De esta forma se elabora un plan de acción que contempla las acciones que la compañía pretende adoptar para prevenir y evitar en la medida de lo posible los riesgos que impactan en la disponibilidad de las operaciones. El hecho de abordar estas acciones de implantación de medidas de seguridad preventivas puede llegar a convertirse en un ahorro de costes al disminuir la posibilidad de tener que enfrentarse a males mayores que supondrían un gasto extra.

9.3. RIESGOS ASOCIADOS AL ESTABLECIMIENTO DE MEDIDAS PREVENTIVAS

No todos los riesgos tienen la misma criticidad ni todas las medidas de seguridad el mismo coste de implantación ni redundan en los mismos beneficios para la organización.

En este sentido, cabe la posibilidad de que la organización adopte un modelo de gestión ambicioso al abordar la implantación de medidas de seguridad costosas de aplicar, engorrosas de mantener y que hacen frente a riesgos que no son críticos.

No implantar medidas preventivas después de identificar riesgos sería análogo al hecho de que un individuo acuda al médico y haga caso omiso cuando éste último le indique que debe ponerse a dieta y aumentar el ejercicio físico. Entonces, ¿para qué acude al médico?

El mismo concepto se aplica a las empresas: si un equipo o responsable ha sido encargado para identificar riesgos y recomendar medidas que mitiguen los mismos, pero la organización no implanta ninguna de las soluciones propuestas, ¿para qué fin se crea dicho equipo o responsable?

Adicionalmente, la selección de medidas de seguridad inadecuadas que no atajan debidamente los riesgos a los que está expuesta la organización puede conllevar un gasto económico inútil que no contribuye al desarrollo de la estrategia de continuidad.

9.4. RECOMENDACIONES

El proceso de identificar e implantar medidas de seguridad debe estar basado en un equilibrio entre los siguientes factores:

- Riesgo que está siendo mitigado o impacto que estaría siendo reducido.
- Coste de implantar la/s medida/s de seguridad (económico y humano).
- Beneficios que la implantación de la/s medida/s de seguridad aporta a la empresa.

Por tanto, en vez de esperar a que un desastre golpee a la organización para ver cómo esta se recupera, las medidas preventivas (en ocasiones denominadas contramedidas) deben ser aplicadas con el objetivo de incrementar la fortaleza de sus actividades frente a posibles impactos previamente identificados en el BIA.

Algunos ejemplos de medidas preventivas son:

- Empleo de materiales de construcción robustos.
- Redundancia de sistemas informáticos y líneas de comunicación.
- Adquisición de seguros con diferentes grados de cobertura.
- Copias de seguridad de información que soporta una actividad crítica de la organización.
- Sistemas de detección y extinción de incendios.
- Sistemas de prevención de intrusiones y control de accesos.
- Sistemas de alarma y vigilancia.

10. Fase IV: Estrategias de recuperación

10.1. OBJETIVOS

En base a los resultados del BIA y del análisis de riesgos, el objetivo perseguido en esta fase consiste en identificar las alternativas de recuperación de las actividades críticas de la organización en los marcos de tiempo definidos y aceptados.

10.2. TAREAS

Es importante recordar que en la fase de realización del BIA, la organización calculó las pérdidas potenciales para las diferentes amenazas que pueden interrumpir sus actividades. Se exponen a continuación algunos ejemplos de estos cálculos:

- Si la sala en la que se ubican los servidores y los sistemas que dan soporte a las actividades de negocio deja de estar operativa, el coste que supondría para la organización ascendería a 60.000 € por cada día de inactividad.

- Si la conexión de mi empresa con el mundo exterior a través de Internet no está disponible, el coste estimado para la organización sería de 3.000 € por cada hora de indisponibilidad.

- Si una empresa de restauración deja de recibir los bienes comestibles de su proveedor de distribución en huelga, pasará a tener unas pérdidas aproximadas de 2.000 € por día a partir del momento en el que se quede sin existencias de reserva.

10.2.1. SELECCIÓN DE ALTERNATIVAS DE RECUPERACIÓN

La organización debe tener en cuenta los posibles daños potenciales a la hora de revisar y seleccionar las diferentes soluciones o alternativas de recuperación de sus actividades críticas, considerando adicionalmente los siguientes factores:

- La cuantía económica asociada a la implantación de la estrategia de recuperación, la cual suele constituir uno de los mayores inconvenientes a la hora de adquirir una solución de recuperación.
- Los beneficios que proporciona la citada estrategia.
- El Tiempo Máximo Permitido de Interrupción (MTD) de la actividad crítica.
- El Tiempo de Recuperación Objetivo (RTO).
- La perdida máxima de información que una empresa se puede permitir (RPO).

Ejemplos de estrategias de recuperación

Recurso crítico	Objetivo	Estrategias de recuperación
Personas que participan en las actividades de negocio	Mantener el conocimiento y las capacidades del personal con funciones y responsabilidades en actividades críticas	• Documentar actividades críticas • Formación • Conocimiento compartido y multidisciplinar • Separación de tareas clave
Instalaciones y Puestos de trabajo	Reducir el impacto que genera la falta de disponibilidad de las instalaciones de trabajo	• Instalaciones alternativas • Acuerdos recíprocos • Teletrabajo
Tecnología	Entender el entorno tecnológico que soporta las actividades críticas y mantener la capacidad para replicarlo en caso de desastre	• Redundancia de equipos y comunicaciones • Mantenimiento de la misma tecnología en diferentes ubicaciones • Copias de software crítico
Información y Documentación	Garantizar la protección y recuperación de la información vital para la organización	• Copias de seguridad • Procedimientos de recuperación • Documentación de activación del plan de continuidad
Proveedores	Identificar y mantener un inventario de proveedores de servicios clave que soportan las actividades críticas	• Contacto con proveedores alternativos • Acuerdos con terceros • Envío y almacenamiento de recursos críticos en ubicaciones alternativas
Accionistas y Socios	Proteger los intereses de socios y accionistas afectados por un desastre	• Acuerdos que garantizan el bienestar de los colectivos involucrados en el desastre
Servicios civiles de emergencia (tráfico, bomberos)	Garantizar que la organización conoce los procedimientos de los servicios de emergencia	• Recomendaciones de rutas de evacuación y puntos de reunión • Participación en simulacros

Considerando únicamente las instalaciones y puestos de trabajo de la empresa como recurso crítico, la siguiente tabla propone diferentes estrategias de recuperación en función de la naturaleza de las mismas (asumidas internamente por la PYME, contratadas a un tercero o diseñadas a medida de la empresa) y el Tiempo de Recuperación Objetivo (RTO).

Relación entre el Tiempo de Recuperación Objetivo y las Estrategias de Recuperación

Tiempo de Recuperación Objetivo (RTO)	Estrategias de recuperación		
	Internas	Contratadas	A medida
Meses	• Reconstruir o reubicar	• Ampliar el contrato de emplazamiento de recuperación	• Reconstruir, alquilar o comprar
Semanas	• Edificios prefabricados en el mismo sitio • Adaptación de edificios para otros usos	• Expansión del emplazamiento de recuperación • Unidades prefabricadas y móviles alquiladas	• Oficinas amuebladas. Subcontratación de procesos
Días	• Emplazamiento de recuperación "in situ" • Trabajo desde casa	• Emplazamiento para la recuperación de la actividad comercial • Acuerdos recíprocos • Instalaciones móviles • Procesos subcontratados	• Oficinas gestionadas
Horas	• Varias ubicaciones con personal reasignado	• Reubicar un equipo reducido de personas a un emplazamiento de recuperación contratado	
Inmediato	• Localizaciones diversas para cada actividad	• Iniciar una conmutación de las tecnologías a un emplazamiento de recuperación contratado	

Fuente: Business Continuity Institute (http://www.thebci.org/ o http://www.bcispain.com/ para su capítulo en España)

En este sentido, es importante destacar los siguientes aspectos con respecto a la selección de las estrategias de recuperación:

- La elección de las diferentes alternativas de recuperación depende de las necesidades de la organización: tiempos de recuperación objetivo (RTO), costes, recursos humanos/técnicos, etc.
- Lo más común y recomendable es adoptar una combinación de las estrategias de recuperación para los distintos recursos críticos.
- El tiempo de recuperación objetivo (RTO) definido por la organización para sus actividades críticas siempre debe ser menor al tiempo máximo permitido de interrupción (MTD).
- El coste de las estrategias de recuperación será generalmente mayor cuanto menor sea el tiempo de recuperación objetivo (RTO).

Una vez analizadas y seleccionadas las estrategias de recuperación que serán empleadas como respaldo en caso de interrupción de las actividades críticas de negocio, es necesario plasmar todas las soluciones y pasos a abordar en un plan (entendido como un conjunto de procedimientos, funciones y actividades que permitirá el restablecimiento de las citadas actividades en unos plazos razonables).

10.3. RIESGOS ASOCIADOS A LA IMPLEMENTACIÓN DE ESTRATEGIAS DE RECUPERACIÓN

Al igual que sucede en la Fase III: Medidas preventivas, consistente en la identificación y aplicación de las mismas, la selección de las estrategias de recuperación más adecuadas depende principalmente de que los resultados del BIA sean veraces y se ajusten lo más posible a la realidad de la empresa.

Así, una estimación errónea sobre las consecuencias de una paralización de las actividades críticas de la organización puede derivar en una selección desacertada sobre las estrategias de recuperación a desarrollar.

Por otro lado, es común que las organizaciones no asimilen la diferencia entre las medidas preventivas y las estrategias de recuperación.

10.4. RECOMENDACIONES

En base a los criterios previamente detallados, y teniendo en cuenta la formalidad de los resultados del proceso BIA, se recomienda una selección de las estrategias de continuidad debidamente documentada para cada actividad crítica. Dicha selección debe ser acordada y ratificada con el director o el nivel directivo de la empresa.

Además, es necesario destacar que las estrategias de recuperación seleccionadas para cada actividad deben ser acordes a los Tiempos de Recuperación Objetivo (RTO) previamente definidos y aprobados.

En paralelo, es aconsejable diseñar una planificación para la puesta en marcha de la estrategia acordada para determinar el aprovisionamiento de los recursos.

Por último, se hace necesario establecer la diferencia entre medidas preventivas y estrategias de recuperación:

- Los mecanismos preventivos explicados en la Fase III: Medidas preventivas intentan reducir la posibilidad de que una compañía sufra una contingencia grave o un desastre y, si éste se produce, disminuir el daño que provocaría (aunque la organización no pueda evitar la caída de la energía eléctrica por una avería de su compañía de suministro, sí puede habilitar baterías o fuentes de alimentación alternativas e independientes que garanticen el suministro eléctrico durante un periodo de tiempo).

- Las estrategias de recuperación son procesos focalizados en cómo rescatar a la organización en caso de que un desastre tenga lugar. Son mecanismos relacionados con la implantación de procedimientos de respuesta ante emergencias y la posibilidad de activar los mecanismos preventivos que ya han sido implantados. En la siguiente ilustración se resaltan los principales recursos sobre los cuales se deben diseñar las estrategias de recuperación:

Recursos organizacionales sobre los cuales se diseñan las estrategias de recuperación

11. Fase V: Desarrollo e implantación del plan

11.1. OBJETIVOS

Llegados a este punto, es necesario situar todas las soluciones, estrategias y pasos en un plan en sí mismo.

Es decir, una vez que las estrategias han sido definidas, deben ser documentadas y puestas en marcha por los encargados de la continuidad de negocio de la organización.

Así los esfuerzos pasan de una fase de planificación a una fase de acción e implementación en la que se pretende:

- Gestionar la respuesta a incidentes: asegurar la existencia de mecanismos que alerten de la existencia de eventos adversos y actúen frente a los mismos.

- Asegurar la continuidad de actividades críticas: garantizar que la ejecución del plan descansa sobre las figuras y/o equipos necesarios (desde su activación hasta la vuelta a la normalidad de las actividades), y que se dispone o se puede disponer de los medios materiales para llevarlas a cabo.

11.2. TAREAS

11.2.1. DEFINIR LAS FIGURAS O LOS EQUIPOS NECESARIOS PARA LA ACTIVACIÓN Y EJECUCIÓN DEL PLAN DE CONTINUIDAD DE NEGOCIO

La composición y el número de figuras o equipos que intervienen en la ejecución del plan pueden variar en función del tamaño de la organización y de su estrategia de recuperación.

Es posible destacar funciones clave que serán llevadas a cabo por los responsables (personas o equipos, dependiendo del tamaño y de los recursos de la empresa) de la activación y ejecución del plan de continuidad de negocio:

- Respuesta a incidentes: responsables de analizar y acotar el impacto que una incidencia puede provocar en la organización de forma que no se tenga que recurrir a la activación del plan de continuidad de negocio.
- Comité de crisis: encargado de activar el plan de continuidad de negocio y dirigir las acciones durante la contingencia.
- Servicios civiles de emergencia necesariamente localizables en caso de catástrofe (como por ejemplo los bomberos) que generalmente constituyen la primera figura de respuesta.
- Logística: responsable de reunir todos los medios (lugar alternativo de trabajo, material, herramientas, etc.) necesarios para contribuir a la reactivación de la actividad.
- Recuperación: asume la puesta en servicio de la infraestructura tecnológica (sistemas, aplicaciones y líneas de comunicación).
- Relaciones públicas: responsable de las comunicaciones con clientes, accionistas, medios de comunicación, etc.

Esta designación de funciones es semejante a las que se establecen en los planes de emergencia encuadrados en la Ley de Prevención de Riesgos Laborales[3] (y sus correspondientes desarrollos reglamentarios), en las que intervienen personas encargadas de poner en práctica diferentes medidas: gestionar las alertas para la actuación de los equipos de primera intervención, dar la alarma para facilitar la evacuación de los empleados, gestionar la coordinación y la cooperación entre los integrantes de los diferentes equipos de emergencia, etc.

Una vez que se han definido las figuras o equipos, así como las funciones a desempeñar por los mismos, la empresa debe desarrollar los planes o procedimientos de actuación a seguir.

11.2.2. DESARROLLAR LOS PROCEDIMIENTOS DE ALERTA Y ACTUACIÓN

Estos procedimientos, si bien no deben sustituir en ningún caso la aplicación del sentido común, recogen el conocimiento necesario para la activación y ejecución del plan de continuidad de negocio, ya que reducen el tiempo invertido en la toma de decisiones críticas y acotan los momentos de incertidumbre y el tiempo de reacción.

Deben ser concisos, factibles y accesibles a todos aquellos miembros que tienen algún tipo de responsabilidad de actuación dentro del plan.

Los objetivos y el alcance de cada uno de ellos deben ser documentados y fáciles de leer y entender por todos los miembros implicados, considerando:

- Las actividades y recursos críticos que deben ser recuperados.
- Los tiempos de recuperación de dichas actividades y recursos.

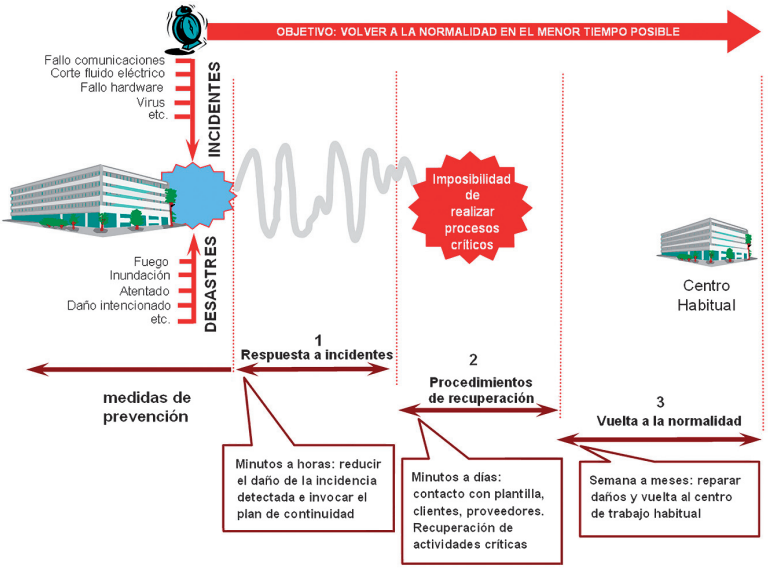
3 Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales. Disponible en: https://boe.gob.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-1995-24292

- En qué situación o situaciones debe ser utilizado cada plan.
- Información útil para la gestión de la contingencia (teléfonos, inventarios de proveedores, servicios, direcciones, *checklist*,…).

Adicionalmente, deben detallar claramente las funciones y responsabilidades de los miembros que forman parte activa del plan de continuidad de negocio, así como el método para activar o invocar el mismo (¿bajo qué circunstancias?; ¿quiénes activan el plan?; ¿cómo es activado el plan?).

La siguiente ilustración muestra las tres principales fases que deben tener lugar en el tiempo a raíz de la identificación de un incidente. El objetivo de dichas fases en conjunto es que la organización recupere la normalidad de sus actividades en el menor tiempo posible.

Etapas transcurridas desde la detección de un incidente/desastre hasta la recuperación de la normalidad en el centro de trabajo habitual



En paralelo a estas etapas, la empresa debe constituir los correspondientes procedimientos de actuación que en definitiva constituirán el plan de continuidad de negocio.

Respuesta a incidentes

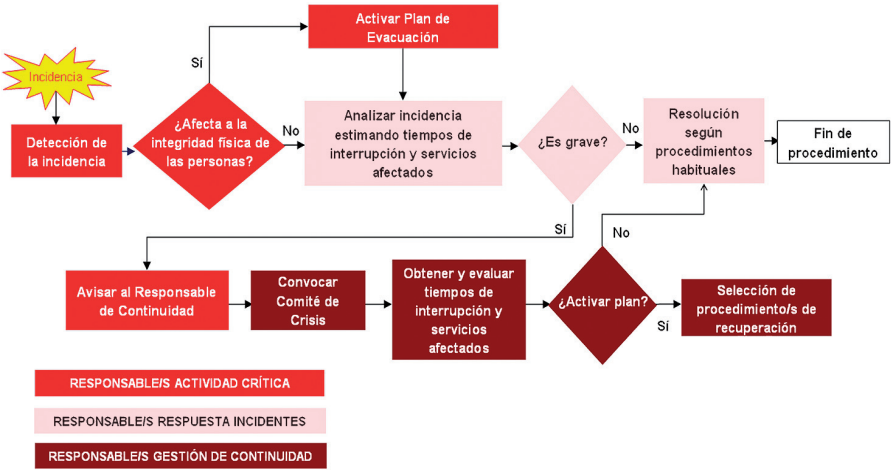
Cualquier incidente que tenga lugar en la organización y que interrumpa sus actividades críticas debe contar con un plan rápido de respuesta que permita:

- Confirmar el tipo de incidente y su criticidad.
- Tomar el control de la situación problemática generada por el incidente.
- Acotar o limitar el impacto que dicho incidente pueda provocar.

La identificación temprana de los incidentes es fundamental a la hora de responder a los mismos de forma ágil y efectiva. Un incidente que no es identificado, evaluado y gestionado adecuadamente puede derivar en un problema de mayor magnitud o incluso en una crisis.

La siguiente ilustración muestra someramente y a modo de ejemplo la secuencia de tareas a realizar en caso de que una empresa detecte la paralización de sus actividades críticas. En ocasiones es frecuente utilizar el término “Plan de Gestión de Crisis” para hacer alusión a este proceso.

Ejemplo de secuencia de tareas a realizar en caso de paralización de la actividad



Procedimientos de recuperación

Puede ser activado dentro del plan de respuesta ante incidentes y, tal y como se ha comentado en esta guía, tienen el objetivo de recuperar en el menor tiempo posible las actividades críticas de una organización que se han visto interrumpidas por un desastre.

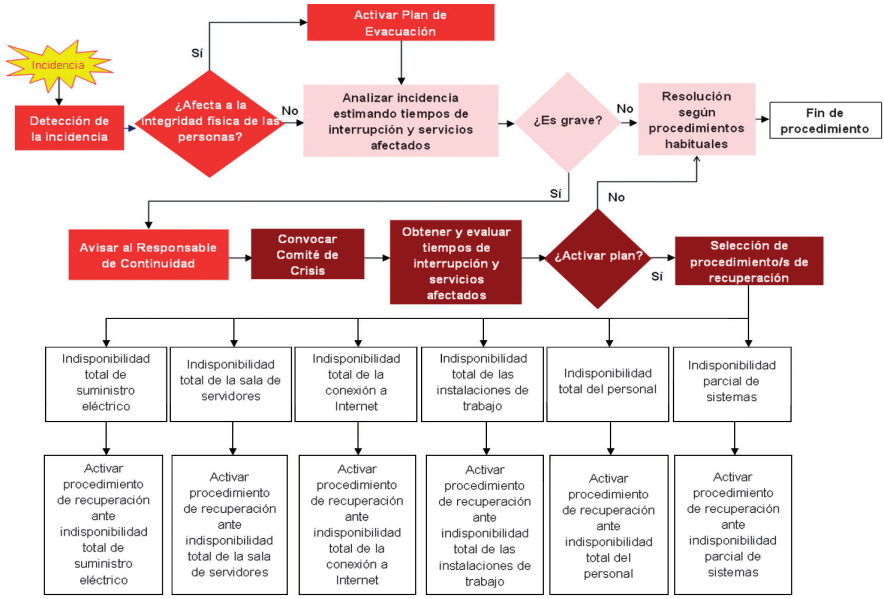
Llegados a este punto, es de suponer que la organización ha decidido poner en marcha el plan de recuperación. Dicho plan debe contener la siguiente secuencia de acciones:

- Quién, cómo y bajo qué circunstancias debe ser activado.
- Persona/s que deben ser informadas de la activación del plan de continuidad en primer lugar (es lo que se conoce como árbol de llamadas).

- Localización física de las personas que intervienen en el plan.
- Qué servicios están disponibles, cuándo y dónde (incluidos los servicios entregados por terceros).
- En qué momento y de qué forma la información que se genera en la ejecución del plan de continuidad es transmitida a responsables, empleados, unidades de dirección, etc.

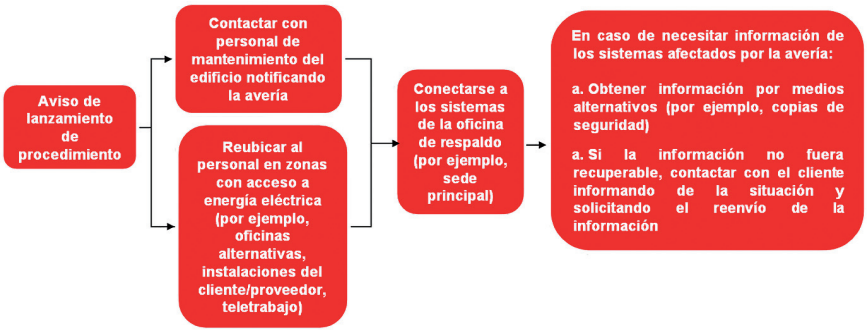
Siguiendo con el ejemplo de la ilustración anterior, en la expuesta a continuación se muestran algunos ejemplos característicos de procedimientos de recuperación ante la supuesta indisponibilidad de recursos críticos de la empresa.

Ejemplos de procedimientos de recuperación característicos



Y finalmente, a continuación se muestra un ejemplo de procedimiento de recuperación en caso de indisponibilidad del suministro eléctrico.

Ejemplo de procedimiento de recuperación en caso de indisponibilidad de suministro eléctrico



Plan de vuelta a la normalidad

Solucionada la contingencia y recuperadas las actividades críticas de la organización, deben establecerse los mecanismos necesarios para recuperar la normalidad de funcionamiento y el "día a día" de las actividades.

11.2.3. DISPONER DE LOS MEDIOS Y RECURSOS NECESARIOS PARA EJECUTAR EL PLAN DE CONTINUIDAD DE NEGOCIO

Todo plan de continuidad de negocio fracasará si previamente no se han dimensionado y provisionado los medios y recursos necesarios que permitan su ejecución. De acuerdo a las estrategias de recuperación diseñadas con anterioridad, las organizaciones deben dotarse de los recursos imprescindibles para el desarrollo efectivo de la respuesta, entre los que es posible mencionar:

- Servicios generales, medios materiales, transporte, medios de almacenamiento, etc.
- Tecnología (servidores, ordenadores de mesa, dispositivos móviles) y comunicaciones.
- Recursos humanos y puestos de trabajo alternativos.
- Información crítica redundante y necesaria para el desarrollo de las actividades de negocio.

11.3. RIESGOS ASOCIADOS AL DESARROLLO E IMPLANTACIÓN DEL PLAN

Los planes de continuidad de negocio son procedimientos de actuación en caso de crisis o desastre en los que suelen intervenir diferentes áreas de la organización. En ocasiones, el propio impacto de un desastre puede concluir en la pérdida de dichos procedimientos, por lo que la organización debe tener preparada para los mismos una estrategia de respaldo y disponibilidad.

11.4. RECOMENDACIONES

Para evitar pérdidas de los planes de continuidad de negocio deben mantenerse copias de los mismos en diferentes localizaciones. Al menos una de estas localizaciones debe estar alejada del lugar físico en el que principalmente se desarrollan las actividades críticas de la organización (oficinas o domicilios particulares).

También es importante que el plan de continuidad de negocio esté disponible para las personas que participan en el mismo en diferentes formatos (incluyendo el electrónico y el soporte papel).

12. Fase VI: Mantenimiento del plan

12.1. OBJETIVOS

El hecho de elaborar y documentar planes de continuidad de negocio y en definitiva procedimientos de recuperación en caso de paralización de las operaciones no garantiza de por sí el éxito a la hora de enfrentarse a un desastre.

De esta forma, los objetivos perseguidos en la presente fase son:

- Inculcar y promocionar una cultura de continuidad de negocio en la organización de forma que paulatinamente se convierta en un proceso crítico a gestionar bajo un ciclo de mejora continua.
- Bajo el citado ciclo, mejorar la eficiencia y la solidez del plan o planes de continuidad de negocio.
- Transmitir fiabilidad a empleados, clientes, accionistas sobre la capacidad de la organización para superar posibles interrupciones de sus operaciones.
- Minimizar la probabilidad y el impacto de las interrupciones.
- Adaptar el plan de continuidad a los cambios organizativos y de negocio que sufren las empresas, revisando periódicamente los análisis de riesgos, los Análisis de Impacto en el Negocio (BIA) y los contactos y responsabilidades asignados que deben mantenerse actualizados en las estrategias y los procedimientos.

12.2. TAREAS

12.2.1. DIFUSIÓN Y FORMACIÓN

Antes de impartir cualquier acción de formación/concienciación, es necesario que la organización determine los colectivos y grupos objetivo, qué tipo de necesidades formativas son requeridas y qué estrategia de comunicación es la más adecuada.

A partir de este esquema se desarrollará la programación de acciones formativas concretas en diversos entornos:

- En el de dirección y supervisión.
- En el de ejecución y operación.

La organización puede utilizar diversos medios para la impartición efectiva de los paquetes formativos, como por ejemplo, la inclusión de mensajes y contenidos relacionados con la continuidad de negocio en la Intranet de la organización, las plataformas online y/o soporte/s semejante/s.

Los responsables deben ser adecuadamente formados y concienciados acerca de los diferentes conceptos que contempla la continuidad de negocio (riesgos, medidas preventivas, detección temprana de incidencias, etc.).

Incluso cabe la posibilidad de extender estos programas de formación a proveedores o en general terceros con los que la organización mantiene relaciones comerciales.

12.2.2. EJECUCIÓN DE PRUEBAS

Aunque también es frecuente el uso de conceptos similares como simulacro, test o ejercicio, “Pruebas” es el término generalmente utilizado para describir el conjunto de medidas que someten a ensayo o examen el plan de continuidad de negocio.

Desarrollado e implantado el plan de continuidad de negocio, es recomendable que sea probado periódicamente debido a los siguientes motivos:

- Cada vez se descubren nuevas mejoras y eficiencias que, de ser aplicadas, perfeccionan el plan.
- Los procesos de negocio, las ya mencionadas interdependencias, el entorno tecnológico y multitud de componentes adicionales pueden cambiar con el paso del tiempo provocando que los planes de continuidad de negocio dejen de estar actualizados.
- Evaluar de forma más veraz la capacidad de respuesta de una compañía ante un desastre (tiempos de respuesta, capacidad de los responsables implicados e idoneidad de los procedimientos desarrollados).

La organización debe planificar las pruebas, su duración y alcance, los participantes (incluidos proveedores de servicios), los elementos del plan que serán evaluados (personas, comunicaciones, sistemas, procedimientos) y la secuencia de pasos a emprender durante su ejecución. Las pruebas deben simular situaciones próximas a la realidad y deben ser planificadas de forma que la exposición de las actividades de la organización ante los riesgos sea mínima.

Aunque sería lo ideal, es obvio que las compañías que deciden realizar tales pruebas no pueden permitirse el lujo de paralizar completamente su producción, por lo que las pruebas deben tener lugar en áreas y momentos específicos que no penalicen la entrega de sus productos y servicios (en definitiva, el negocio).

Existen diferentes tipos de pruebas que se describen someramente en la siguiente tabla (ordenadas de menor a mayor complejidad).

Tipos de pruebas del Plan de Continuidad de Negocio

Tipo de prueba	Descripción
Test de consistencia	El plan de continuidad de negocio es distribuido a los departamentos y/o áreas funcionales implicadas para su revisión/actualización.
Test de validez	Representantes de cada departamento y/o área funcional implicada se reúnen para revisar y discutir el plan.
Test de simulación (simulacro)	Escenario ficticio de recuperación para verificar que el Plan de Continuidad contiene la información necesaria y suficiente.
Test actividades críticas	Recuperación real de una actividad crítica bajo un entorno controlado y sin poner en peligro la operativa usual/original.
Test completo	Interrupción real de las operaciones y recuperación de las mismas a través de los procedimientos del Plan de Continuidad.

12.2.3. ACTUALIZACIÓN (CICLO DE MEJORA CONTINUA)

Los planes de continuidad de negocio deben ser mantenidos a través de un ciclo de mejora continua. Cualquier cambio a nivel organizativo (estratégico), operacional o técnico puede impactar en el negocio y por tanto en el plan de continuidad.

Consecuentemente, la empresa debe emprender un proceso para mantener al día la capacidad, eficacia e idoneidad del plan de continuidad de negocio. Algunas propuestas en ese sentido son:

- Revisión periódica en busca de cambios en la estructura de la organización, en los productos/servicios que desarrolla, en la plantilla, etc., los cuales pueden tener consecuencias en el plan de continuidad de negocio (política, BIA, procedimientos de recuperación, etc.).

- Confirmación de que el plan de continuidad de negocio es acorde y contempla los citados cambios en los diversos componentes de la organización.

- Adecuación de los planes de continuidad de negocio a requerimientos de socios, clientes, accionistas u otro tipo de requerimientos regulatorios.

- Revisión de los resultados de las pruebas realizadas y de que las mejoras identificadas en las mismas han sido aplicadas.

- Incluso auditorías internas o externas de todos y cada uno de los componentes del plan de continuidad de negocio.

En el caso de que se evidencien cambios que afecten a la organización y que tengan impacto en los procesos de negocio, puede ser necesario revisar los Análisis de Impacto en el Negocio (BIA) y Análisis de Riesgos para ver en qué medida dichos cambios pueden provocar desajustes en las estrategias y los procedimientos. De esta forma, la organización puede disponer de ciertas garantías sobre la efectividad de su plan de negocio.

12.3. RIESGOS ASOCIADOS AL MANTENIMIENTO DEL PLAN

La fase de mantenimiento del plan es vital para confirmar la completitud, viabilidad y eficacia del mismo. Sin embargo, en esta fase existen una serie de riesgos que son necesarios tener en cuenta:

- Formación/concienciación: es frecuente que las organizaciones que han implantado un plan de continuidad de negocio carezcan de ideas y estrategias precisas acerca de posibles programas de formación (¿quiénes deben ser los destinatarios del programa?, ¿qué mensajes deben ser transmitidos?, ¿qué método de comunicación es el más idóneo?).

- Falta de criterio a la hora de definir la periodicidad en la cual los planes de continuidad de negocio deben ser probados y el tipo de pruebas a realizar.

12.4. RECOMENDACIONES

Para asegurar el mantenimiento del plan de continuidad de negocio es recomendable el desarrollo de programas educativos que mezclen diferentes formas de comunicación y aprendizaje de forma que sea fácilmente asimilable por toda la organización.

Por otro lado, y como medida general, se recomienda que los planes de continuidad de negocio, aparte de ser flexibles, sean testados al menos una vez al año a través de la realización periódica de simulacros que reproduzcan de forma ficticia situaciones de emergencia o contingencia. Dicha periodicidad depende de las necesidades que determine la organización y el entorno en el que opera.

13. ¿Qué debo recordar?

Invertir en Planes de Continuidad de Negocio compensa	La gestión de la continuidad de negocio en cualquier organización es una inversión, no es un coste. El retorno de inversión (ROI) es tangible en términos de reputación y valor de imagen de la empresa.
Simplicidad	El plan de continuidad de negocio debe ser entendible y sencillo de utilizar y mantener. La aplicación del sentido común, de la experiencia y del conocimiento del negocio son componentes clave para el éxito de un plan de continuidad de negocio.
Alcance limitado y priorizado	La implantación de un plan de continuidad de negocio debe cubrir, al menos, la operativa u operativas más críticas de la organización.
Responsabilidades	Un plan de continuidad de negocio debe establecer claramente quiénes formarían parte del mismo, sus funciones, responsabilidades y autoridad.
Las copias de seguridad solo son una parte del Plan de Continuidad	Cuando se habla de continuidad de negocio, algunas organizaciones se centran principalmente en hacer copias de seguridad de su información. Aunque este aspecto es tremendamente importante, constituye una pequeña pieza del puzzle constituido por personas, documentación, vias de comunicación, proveedores de servicios, etc.
La activación del Plan de Continuidad es la opción recurrida en última estancia	La ejecución por parte de una organización de un plan de continuidad de negocio no se produce ante cualquier incidente de seguridad, sino en situaciones de crisis/emergencia perfectamente definidas y una vez que las medidas de seguridad preventivas han fallado.
No emprender tareas inabarcables	Tareas excesivamente ambiciosas generan situaciones de frustración y hacen que los proyectos fracasen. El desarrollo de planes de continuidad complejos con equipos muy elaborados y excesiva documentación de soporte es dificil de mantener actualizado.
Divide y vencerás	La definición e implantación de un plan de continuidad de negocio puede e incluso debe realizarse en muchas ocasiones en diferentes fases dentro de la organización.

POLÍTICA DE CONTINUIDAD/ ESTRATEGIA + PROCEDIMIENTOS/ PLANES + FORMACIÓN + MANTENIMIENTO/ ACTUALIZACIÓN/ PRUEBAS = CONTINUIDAD

14. Más información

La siguiente relación de estándares internacionales y guías de ayuda, aparte de ser mostrados para la consulta de los interesados, han sido explotados a modo de bibliografía para la elaboración de esta guía:

14.1. ESTÁNDARES INTERNACIONALES

Son desarrollados a través de un consenso completo entre todas las partes interesadas (gobiernos, asociaciones comerciales, consumidores) y no impuestos como obligatorios. Los estándares son herramientas empleadas por las organizaciones de cualquier tipo y tamaño.

BS 25999:2006 – *(British Standard* en inglés*)* primera norma británica para la gestión de continuidad de negocio. Desarrollada por un amplio grupo de expertos representativos de sectores de la industria y la administración. Proporciona la base para comprender, desarrollar e implantar la continuidad de negocio en una organización. Está previsto que se convierta en ISO 22301. Comprende dos partes

- **Parte 1:** Código de buenas prácticas y recomendaciones para Gestión de Continuidad de Negocio (parte que sustituye al PAS 56).

- **Parte 2:** publicada el 20 de Noviembre de 2007, como norma certificable establece los requisitos para implementar un Sistema de Gestión de Continuidad de Negocio.

En términos sencillos, la parte 1 es el "debería" y la parte 2 es el "debe". Así, muchos de los aspectos tratados en esta guía provienen del estudio y análisis de la información contenida en la parte 1.

ISO/IEC 27002:2005 – código de buenas prácticas para la Gestión de la Seguridad de la Información. Es la antigua ISO 17799 y comprende un apartado dedicado especialmente a la continuidad de negocio.

PAS 77:2006 – (*Publicly Available Specification* en inglés) guía de buenas prácticas de la continuidad de los servicios de tecnologías de la información (TI) emitida por *British Standards Institute (BSI)*. En esta norma se establecen los principios y técnicas recomendadas para la Gestión de la continuidad de los servicios tecnológicos.

ISO/IEC 20000 – gestión de los servicios relacionados con las tecnologías de la información.

14.2. GUÍAS DE AYUDA

Manual de buenas prácticas 2007: Guía para instaurar Buenas Prácticas Globales en Gestión de Continuidad de Negocio. Elaborada por *The Business Continuity Institute* y traducida al español por *ISMS Forum Spain*.

Contingency Planning Guide for Information Technology Systems: NIST SP 800-34. Publicación del *Network Information Security and Technology (NIST)*. Guía para realizar planes de contingencia sobre tecnologías y sistemas de información.

14.3. ENLACES DE INTERÉS

Si las PYME están interesadas en conocer más acerca de lo que es un plan de continuidad de negocio y de sus estándares, a continuación se expone una serie de direcciones web con información referida a este tipo de planes:

- **Http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/.** INTECO-CERT en su objetivo de sensibilizar sobre la importancia de estos sistemas de gestión, cuenta con una sección de SGSI en la que trata a lo largo de los diferentes apartados los conceptos más importantes sobre su normativa, modelo y beneficios, así como las diferentes fases de su implementación.

- **www.bsigroup.es** – *British Standards Institute* (BSI) para España: entidad dedicada a la creación de normas para la estandarización de los procesos, en este caso destaca la citada BS 25999, la cual puede ser adquirida en formato papel o digital visitando la tienda de BSI en Internet **http://shop.bsigroup.com/.**

- **http://www.thebci.org** y **www.bcispain.com**- *The Business Continuity Institute* (BCI): organismo promotor de la gestión de continuidad de negocio a nivel mundial fundado en el año 1994. Existe un capítulo de BCI en España.

- **http://www.drii.org** – *Disaster Recovery Institute International:* organismo creado con el fin de desarrollar una base de conocimiento en planeación de contingencias y gestión de riesgo.

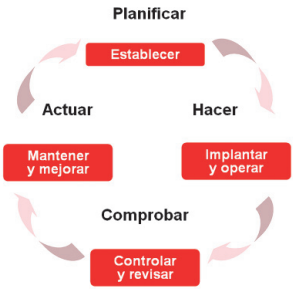
- **http://www.ismsforum.es** – ISMS Forum Spain: asociación que tiene por fin fomentar la seguridad de la información en España.

- **http://www.nist.org** – Instituto Nacional de Normas y Tecnología (NIST por sus siglas en inglés): agencia estadounidense encargada de promover la innovación y la competencia mediante avances en normas y tecnología.

- **http://pmi.org.** Página oficial del *Project Management Institute*, organización internacional que desarrolla la guía del PMBOK, la cual detalla a modo de buenas prácticas los fundamentos de la Gestión de Proyectos.

15. ANEXO I: Glosario

- **Actividad de negocio:** proceso o conjunto de procesos establecidos por una organización para producir o soportar sus productos o servicios.
- **Activo:** son los recursos que dan soporte a las actividades de negocio de una organización, necesarios para que ésta funcione correctamente y alcance los objetivos marcados por la organización (por ejemplo, los sistemas informáticos).
- **Acuerdos recíprocos:** convenio o contrato entre dos organizaciones con características funcionales y técnicas semejantes que permitirá a cada una de las partes recuperar sus actividades críticas empleando los recursos e instalaciones de la otra.
- **Alternativas de recuperación:** conjunto de actividades predefinidas que serán implementadas y llevadas a cabo en respuesta a un desastre.
- **Amenaza:** eventos que, aprovechando una vulnerabilidad, pueden desencadenar un incidente en la empresa, produciendo daños materiales o pérdidas inmateriales en sus activos. Dentro de eventos se consideran tanto acciones, como interrupciones o falta de acción.
- **Análisis de Impacto en el Negocio o *Business Impact Analysis*** (BIA por sus siglas en inglés): proceso de análisis de las actividades de negocio y las consecuencias que una interrupción sobre las mismas puede provocar en la organización.
- **Análisis de Riesgos:** proceso de identificación, análisis y evaluación de riesgos.
- **Ciclo de mejora continua:** o ciclo PDCA *(Plan, Do, Check, Act*, por sus siglas en inglés), es una estrategia de mejora continua de los procesos y sistemas de gestión de la empresa en 4 pasos.



La parte II del estándar de continuidad de negocio BS 25999:2006 establece los requerimientos de planificación, establecimiento, implementación, operación, monitorización, revisión, práctica, mantenimiento y mejora del Plan de Continuidad de Negocio bajo un proceso de gestión cíclico y no como una acción o proyecto puntual con principio y fin.

- **Conmutación:** de forma general se refiere a la acción de cambiar una cosa por otra. En el contexto de la guía hace referencia al cambio de las líneas de comunicación para establecer la conexión con el centro de respaldo alternativo.
- **Contingencia:** suceso no deseado que afecta a la continuidad normal de las operaciones de la organización.
- **Control:** mecanismo que se emplea con el fin de reducir el riesgo asociado a una o varias amenazas. Es frecuente el uso análogo del término "Medida de Seguridad".
- **Desastre:** problema o evento no planificado, cuya consecuencia es la interrupción de los procesos de negocio durante un periodo de tiempo. Este tiempo de paralización de los procesos es superior a lo que la organización puede soportar sin sufrir perjuicios considerables para el negocio.
- **Disponibilidad:** característica, cualidad o condición de un proceso de negocio/activo/recurso de encontrarse a disposición de la organización.
- **EAR/PILAR:** herramienta de análisis de riesgos que implementa la metodología Magerit, desarrollada por el Centro Criptológico Nacional (CCN – www.ccn-cert.cni.es) y de amplia utilización en la administración pública española.
- **Gestión de riesgos:** desarrollo y aplicación ordenada de políticas, procedimientos y prácticas para identificar, analizar, evaluar y controlar la respuesta a los riesgos.
- **Impacto:** consecuencia evaluada de una interrupción.

- **Incidente:** cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar una interrupción o una reducción de la calidad de ese servicio.
- **Interdependencias:** relaciones establecidas entre el conjunto de equipamiento, personas, tareas, departamentos, mecanismos de comunicación y proveedores externos que constituye una actividad de negocio.
- **Interrupción:** suspensión de las operaciones normales del negocio durante un período de tiempo.
- **ISO:** Organización Internacional para la Estandarización (www.iso.or), es el encargado de promover el desarrollo de las normas internacionales industriales y comerciales conocidas como normas ISO.
- **Magerit:** metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica (disponible en http://www.csi.map.es/csi/pg5m20.htm).
- **MiFID:** *Markets in Financial Instruments Directive*. Directiva que forma parte del Plan de Acción de los Servicios Financieros de la Unión Europea y constituye un elemento de vital importancia para crear un sólido marco regulatorio común para los mercados de valores europeos. Afecta a las empresas de servicios de inversión y a las entidades de crédito y, en relación con la continuidad de negocio exige:
    - Empleo de sistemas, recursos y procedimientos adecuados para garantizar la continuidad en la realización de los servicios y actividades de inversión.
    - Adopción, aplicación y mantenimiento de una política adecuada de continuidad de la actividad encaminada a garantizar, en caso de interrupción de sus sistemas y procedimientos, la preservación de datos y funciones esenciales.

- **OCTAVE** *(Operationally Critical Threat, Asset and Vulnerability Evaluation*, por sus siglas en inglés): es un conjunto de herramientas, técnicas y métodos (desarrollados por el CERT *Coordination Center del Software Engineering Institute* de la Universidad Carnegie Mellon de Pensilvania, Estados Unidos) empleados para el análisis de riesgos tecnológicos (disponible en http://www.cert.org/octave/.)
- **Plan de continuidad de Negocio** (PCN) o *Business Continuity Plan* (BCP por sus siglas en inglés) es un conjunto de directrices, criterios, normas de actuación y herramientas organizativas que, ante la ocurrencia de una contingencia que provocase la interrupción de alguna o todas las áreas de negocio de una organización, permiten la recuperación de la operatividad de las mismas en el menor tiempo posible, de modo que las pérdidas económicas ocasionadas sean mínimas.
- **Plan de recuperación ante desastres** (PRD) o *Disaster Recovery Plan* (DRP por sus siglas en inglés): constituye una parte del Plan de Continuidad de Negocio en aquellas compañías que dispongan de infraestructura tecnológica para soportar sus operaciones y, de forma análoga al Plan de Continuidad de Negocio, consta de todas las prácticas necesarias que, en caso de desastre, permiten recuperar en el menor tiempo posible el entorno tecnológico (sistemas, aplicaciones e infraestructuras) que soporta las actividades de una organización.
- **Problema:** causa subyacente, aún no identificada, de una serie de incidentes o un incidente aislado de importancia significativa.
- **Punto de Recuperación Objetivo** – RPO (*Recovery Point Objective* por sus siglas en inglés): cantidad de información que la organización puede llegar a perder como consecuencia de un desastre. Marca desde un punto de vista tecnológico la estrategia de realización de copias de seguridad de la información.
- **Reingeniería de procesos** actividad de rediseño de los procesos con el fin de mejorar los mismos y crear beneficios y ventajas competitivas.

- **Resiliencia:** término de origen inglés (*resilient*) referido a la capacidad de elasticidad y resistencia de una empresa para hacer frente a los impactos.
- **Riesgo:** probabilidad de que una amenaza aproveche y explote una debilidad asociada a un proceso/activo/recurso provocando daño sobre el mismo.
- **Retorno de Inversión** – ROI (*Return on Investment* por sus siglas en inglés): valor que mide el rendimiento de una inversión, para evaluar lo eficiente que es el gasto que una organización realiza o planea realizar y determinar la viabilidad de un proyecto o potencial proyecto.
- ***Stakeholders:*** anglicismo referido a todas las partes participantes o afectadas por una empresa como son accionistas, empleados, inversores, asociaciones sectoriales, Cámaras de Comercio, etc.
- **Tiempo de Recuperación Objetivo - RTO** (*Recovery Time Objective* por sus siglas en inglés): variable temporal dentro de la cual una actividad de negocio debe ser recuperada después de un desastre.
- **Tiempo Máximo Permitido de Recuperación – MTD** (*Maximum Tolerable Downtime* por sus siglas en inglés): periodo de tiempo (medido en segundos, minutos, horas o incluso meses en función de la actividad) asociado a la paralización de una actividad que, una vez superado, la viabilidad de la organización se verá amenazada irrevocablemente.
- **Teletrabajo:** desempeño de un trabajo de manera regular en un lugar diferente del centro de trabajo habitual, generalmente empleando medios informáticos.
- **Vulnerabilidad:** debilidad o falta de control asociada a un proceso o recurso que puede ser explotada provocando un daño sobre dicho proceso. Un ejemplo de vulnerabilidad es el hecho de que una organización no disponga de medidas físicas que impidan el acceso a sus instalaciones a personal no autorizado.

¿Quieres seguirnos?

en la web: http://observatorio.inteco.es

en Twitter: @ObservaINTECO

¿Quieres hacernos llegar algún comentario?

observatorio@inteco.es

Instituto Nacional
de Tecnologías
de la Comunicación

Deloitte.