JUAN GASPAR MARTÍNEZ

EL PLAN DE CONTINUIDAD DE NEGOCIO

Guía práctica para su elaboración

Madrid - Buenos Aires - México

00-indice.indd 5 22/8/06 20:13:47

© Juan Gaspar Martínez, 2006

Reservados los derechos.

No está permitida la reproducción total o parcial de este libro, ni su tratamiento informático, ni la transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, por registro u otros métodos, sin el permiso previo y por escrito de los titulares del Copyright.

Ediciones Díaz de Santos

www.diazdesantos.es/ediciones (España)
www.diazdesantos.com.ar (Argentina)

ISBN: 84-7978-778-3
Depósito legal: M. 38.984-2006

Fotocomposición: Estefanía Grimoldi
Diseño de cubierta: Ángel Calvete
Impresión: Fernández Ciudad, S. L.
Encuadernación: Rústica-Hilo, S. L.

Índice

Dedicatoria VII
Advertencia XV
Agradecimientos XVII
Prólogo XIX

1. Introducción y objetivos 1
1.1. Objetivos de esta Guía 5
1.2. Objetivos de un Plan de Continuidad de Negocio 6
1.3. Cómo usar la Guía 7

2. Definiciones previas 9
2.1. Alcance del plan 10
2.2. Premisas de partida 12
2.3. Funciones de la Dirección 13

3. Análisis de impacto 17
3.1. Introducción y generalidades del análisis 17

00-indice.indd 9 22/8/06 20:13:47

3.1.1 Puntos comunes en impactos producidos por desastres 18
3.1.2 Impactos más comunes y tiempos de recuperación.. 19
3.2 Resumen para la Dirección 22
3.2.1 Objetivos del análisis 22
3.2.2 Alcance del análisis 23
3.2.3 Resumen de resultados 23
3.3 Funciones analizadas 29
3.4 Resultados del análisis 29
3.5 Requisitos para la recuperación 31
3.5.1 Coste de la protección 31
3.5.2 Pérdidas asumibles 32
3.5.3 Umbrales de recuperación 32
3.5.4 Requisitos mínimos aceptables para la recuperación (REMAR) 33
3.5.5 Medidas a implantar 36
3.6. Anexos 45
3.6.1 Cuestionarios de valoración 45
3.6.2 Resultados BIA 52

4. Elementos críticos .....
4.1. Funciones 57
4.1.1 Funciones críticas del departamento Financiero .. 57
4.1.2 Funciones críticas del departamento de Sistemas de Información 58 60
4.1.3 Funciones críticas de otros Departamentos 61
4.2. Aplicaciones 62

4.2.1 Aplicación A 62
4.3. Recursos críticos 63
4.3.1 Registros vitales y *backups* 63
4.3.2 Necesidades de personal 64
4.3.3 Necesidades de espacio 65
4.3.4 Necesidades de impresos y suministros 66
4.3.5 Necesidades de hardware 67
4.3.6 Necesidades de comunicaciones 68
4.3.7 Necesidades de software 69
4.3.8 Necesidades de otros recursos 70

5. Estrategia de continuidad 71
5.1. Centro de control 72
5.2. Centro alternativo 72
5.2.1. Otra localización dentro de la organización 73
5.2.2. Acuerdos de ayuda mutua 74
5.2.3. Acuerdos con los proveedores de equipos 75
5.2.4. Empresas de servicios 75
5.3. Comunicaciones alternativas 78
5.4. Procedimientos de *backup* 78
5.5. Centro de almacenamiento externo 80
5.5.1. Solución propia 80
5.5.2. Solución externa 83

6. Equipos de recuperación 87
6.1. Composición de los equipos 88

6.1.1 Equipo de Gestión de Incidentes 88
6.1.2 Equipo de Operaciones Informáticas 89
6.1.3 Equipo de Administración 91
6.1.4 Equipo de Atención a Usuarios 92
6.1.5 Equipo de Inmuebles 93
6.1.6 Equipo de Servicios Generales 94
6.2. Funciones de los equipos 95
6.2.1 Equipo de Gestión de Incidentes 95
6.2.2 Equipo de Operaciones Informáticas 96
6.2.3 Equipo de Administración 97
6.2.4 Equipo de Atención a Ususarios 98
6.2.5 Equipo de Inmuebles 99
6.2.6 Equipo de Servicios Generales 99

7. Plan de acción 101
7.1. Definiciones de desastre 102
7.2. Activación de procedimientos de emergencia 103
7.2.1 Notificación de primera alerta 104
7.2.2 Escalado de problemas 106
7.2.3 Evaluación de daños 110
7.3. Procedimientos de respuesta 112
7.3.1 Coordinación de actuaciones por el equipo de Gestión de Incidentes 113
7.3.2 Procedimientos del departamento de Administración 117
7.3.3 Procedimientos del departamento de Asesoría Jurídica 121

7.3.4 Procedimientos del departamento Comercial.... 125
7.3.5 Procedimientos del departamento de Fabricación 125
7.3.6 Procedimientos del departamento de Gestión de Materiales 127
7.3.7 Procedimientos del departamento de Inmuebles .. 128
7.3.8 Procedimientos del departamento de Logística. 132
7.3.9 Procedimientos del departamento de Recursos Humanos 133
7.3.10 Procedimientos del departamento de Relaciones Públicas 139
7.3.11 Procedimientos del departamento de Seguridad 143
7.3.12 Procedimientos del departamento de Sistemas de Información 145
7.3.13 Procedimientos del servicio de Archivo Central.. 148
7.3.14 Procedimientos del servicio de Cafetería..... 150
7.3.15 Procedimientos del servicio de Correos..... 151
7.3.16 Procedimientos del servicio de Viajes..... 154
7.3.17 Procedimientos del servicio de Telecomunicaciones 155
7.4. Procedimientos de recuperación..... 157
7.4.1 Coordinar la preparación del lugar de recuperación..... 157
7.4.2 Traslado al centro de respaldo..... 158
7.4.3 Procedimientos de restauración del Sistema Operativo..... 158
7.4.4 Procedimientos de restauración de aplicaciones. 159
7.4.5 Procedimientos de recuperación de datos 159

8. Plan de vuelta a la normalidad 161

9. Pruebas y actualización 163
9.1. Pruebas y entrenamiento del plan 163
9.1.1 Revisiones periódicas 164
9.1.2 Ejercicios de entrenamiento 164
9.1.3 Pruebas técnicas 172
9.2. Mantenimiento del plan 172
9.2.1 Revisión y validación de necesidades y estrategias . 173
9.2.2 Actualizaciones 174

10. Lista de distribución 177

11. Anexos 179

Bibliografía 181
Glosario 187
Relación de términos en inglés y su equivalente en español .. 215
Apéndice 223

Advertencia

Con la publicación de esta Guía, ni el autor ni los editores asumen ninguna responsabilidad sobre los daños que se pudieren producir en personas físicas o jurídicas, o bienes tangibles o intangibles, de cualquier naturaleza, sean directos, indirectos o consecuenciales, directa o indirectamente resultantes del uso de esta Guía, o referencia a ella, para la realización de Planes de Contingencia o de Continuidad de Negocio. Cualquier persona física o jurídica que utilizare esta Guía para la realización de Planes de Contingencia o de Continuidad de Negocio, lo hace bajo su entera responsabilidad y su propio criterio.

En cualquier caso, cualquier persona física o jurídica que utilizare esta Guía debe hacerlo para el desarrollo de su propio plan de continuidad de negocio. La utilización de esta Guía por consultores para el desarrollo de planes de continuidad de negocio para terceros debe contar con la autorización escrita del autor.

00-indice.indd 15 22/8/06 20:13:48

Agradecimientos

No tengo experiencia suficiente como autor, pero me atrevería a decir que un libro no es nunca obra de una sola persona. Y menos, un libro técnico. Los conocimientos y experiencia que permiten la redacción de una obra de estas características son, al menos en mi caso, fruto de una infinidad de vectores que han ido dejando un poso del que, con un poco de aportación personal, ha nacido esta obra.

Por ello, considero de justicia agradecer explícitamente a quienes han contribuido de manera más o menos directa a su elaboración.

En primer lugar, y como ya hice en la obra anterior, quiero agradecer a mis clientes, (reales o potenciales), su capacidad de intercambio de conocimientos y experiencias, tanto en visitas personales como en asistencia a mis seminarios, de los cuales, a lo largo de los últimos veintidós años, obtuve no pocos de los conocimientos que he utilizado.

También a aquellos con quienes he tenido la suerte de trabajar. Muy en particular, quiero agradecer a José María de Acuña, mi primer lazarillo en este apasionante mundo, la magnífica crítica que me hizo del primer libro, de la cual he tratado de extraer las máximas enseñanzas al escribir éste; a José Luis Lucero sus buenos oficios para hacer más útiles algunos de los formularios que se incluyen en el CD, y a Miguel Ángel Ramos sus siempre equilibradas opiniones y juicios y su magisterio subliminal.

00-indice.indd 17 22/8/06 20:13:48

Prólogo

Me ha pedido que escriba el prólogo de su último libro mi, en primer lugar, amigo, y en segundo lugar gran profesional, con el que tengo la suerte en coincidir desde hace bastante tiempo colaborando en temas que nos son comunes, y que profesionalmente nos preocupan: la Seguridad y más específicamente su prevención mediante los Planes de Continuidad del Negocio.

Con este prólogo no pretendo ensalzar la obra que tenéis en vuestras manos, porque no lo necesita, será el propio lector quien lo haga, ni tampoco alabar las innegables virtudes profesionales que tiene su autor, porque son suficientemente conocidas por todos los que estamos en estos temas.

Juan ha puesto a disposición de nosotros, los profesionales de este sector, una parte de sus muy amplios conocimientos y dilatada experiencia a través de la publicación de un primer libro "Planes de Contingencia, la Continuidad del negocio en las organizaciones". Pero su espíritu perfeccionista no quedó contento con los muchos conocimientos que en ese libro se vertían, sino que quiso además mostrarnos de una forma práctica, casi llevándonos de la mano, de qué forma se pueden convertir en realidad esos planes, y ha sacado este libro, que ahora tenemos en la mano "El Plan de Continuidad de Negocio. Guía práctica para su elaboración"

00-indice.indd 19 22/8/06 20:13:48

Por desgracia tenemos pocos libros en español que aborden estos temas, y tenemos que acudir a publicaciones en inglés, de las que tampoco hay muchas con el carácter eminentemente práctico de esta obra. Este libro cubre este gap de información, y su enfoque empírico le hace especialmente útil.

Además, seguramente pensando en que los profesionales del sector estamos normalmente muy atareados con el devenir diario, nos ha facilitado su uso mediante un CD, que nos permite aplicar sus enseñanzas de una manera inmediata y con el menor esfuerzo.

La mayoría de las organizaciones de todos los sectores, con sus honrosas excepciones, no han tomado conciencia de la imprescindible necesidad de tener estudiados los pasos que habría que dar y las acciones que habría que tomar para que si, por desgracia, hubiera una interrupción en las funciones críticas del negocio, supiera cada miembro de la organización que es lo que tendría que hacer para acortar al máximo esa inactividad.

No cabe duda que pensando fríamente lo que se debía hacer, quien debía hacerlo y en que secuencia, se va a conseguir el objetivo con mayor facilidad y en un menor tiempo que si se hace acuciado por la presión del momento y por la indudable posible desorganización que una contingencia puede provocar.

Aunque cada vez nos vamos concienciando más en los aspectos de la Seguridad, y concretamente en los Planes de Continuidad del Negocio, la realidad es que casi nadie escarmienta en cabeza ajena.

Cuando nos enteramos de que ha sucedido una contingencia importante a alguna organización próxima, sentimos inmediatamente un aldabonazo, y nos ponemos a evaluar como tenemos nuestra organización y nos preguntamos si hubiéramos podido superar el impacto de esa contingencia si nos hubiera ocurrido a nosotros.

En gran parte de las ocasiones la respuesta es NO, y nos hacemos el propósito de poner manos a la obra para remediarlo. Pero los acontecimientos urgentes de cada día nos hacen irlo posponiendo repetidamente, y como además pensamos que “eso les pasa a otros”,

vamos envolviendo nuestra memoria en una niebla adormecedora que nos hace dejar el problema muy difuminado.

Por otra parte al plantear la necesidad de realizar un Plan de Continuidad del Negocio a los órganos directivos de nuestra organización, nos preguntan por su rentabilidad, y al final nos encargan que nos preocupemos de las actividades que repercuten de una manera directa y positiva en la cuenta de resultados, y que sin abandonar la idea, que se vaya haciendo en los ratos libres. Esos ratos libres nunca los tenemos.

A mayor abundamiento, hasta el momento no hay apenas ninguna reglamentación que nos obligue a tener, y mantener, un Plan de Continuidad (esperemos que los Órganos Legislativos correspondientes se conciencien también y que se remedie), y por tanto no incumplimos nada si no lo tenemos, es más, parece que el tenerlo puede ser un lujo y un derroche.

Algunas organizaciones como pueden ser las entidades financieras, lo tienen como parte de sus procesos de seguridad, porque son conscientes de que su negocio se puede venir abajo si dejan de dar el servicio incluso durante un lapso de tiempo breve, otras en cambio, prefieren hacer como el avestruz.

Este libro, estoy seguro, que dará un campanillazo en las conciencias adormecidas, y sembrará la inquietud de que tenemos pendiente de hacer algo que puede ser absolutamente vital para la organización. Es más, que puede hacer que su carencia haga peligrar la supervivencia de la misma.

Pero no se debe hacer como otras veces, que esa inquietud vaya decayendo, sino que debe servir para que empecemos en este mismo momento a elaborar ese Plan de Continuidad del Negocio, ya que son muchas las puntadas a dar, puesto que en un Plan de estas características no somos autosuficientes. Tenemos que involucrar en primer lugar a todos los órganos directivos de nuestra organización, realizar acuerdos formales o contratos con nuestros proveedores, con las compañías proveedoras de energía eléctrica, de telefonía de voz, de datos, etc. etc., y eso requiere dedicar tiempo y recursos.

El libro que tiene en sus manos el lector, estoy seguro, que le va proporcionar esas pautas y los aspectos prácticos de las "lecciones aprendidas" fruto de la experiencia de muchos años de su autor.

De nuevo, gracias Juan por este libro en el que vuelcas tu acervo profesional para facilitar nuestra tarea.

José Luis Lucero
Licenciado e Ingeniero en Informática
Socio Director de IEE, Informáticos Europeos Expertos

1

Introducción y objetivos

La primera vez que tuve en mis manos mi libro *Planes de Contingencia. La continuidad del negocio en las organizaciones* [1], aun con la ceguera propia del padre incapaz de ver los defectos de sus hijos, me planteé la duda de si su lectura aportaría alguna luz a los posibles lectores interesados en estas materias. Sus objetivos no eran sino dar una visión general y estructurada del proceso de elaboración de un plan de contingencia, acompañándolo al mismo tiempo de unas pautas para la revisión de posibles planes existentes.

Como decía la revista *SIC* en su número de febrero de 2005: "Desde una óptica ciertamente clásica, realiza un recorrido por las diversas fases para la elaboración de un plan de contingencia, o lo que es lo mismo, un conjunto de estrategias y procedimientos preventivos y reactivos que permiten un rápido retorno a una situación suficientemente normalizada para que la actividad de la organización recupere un nivel aceptable después de una interrupción no prevista de sus sistemas de información. En este sentido, las fases propuestas están inspiradas en los principios difundidos por el *Business Continuity Institute* británico, para la gestión de la continuidad del "negocio" corporativo, y se desarrollan ..."[2].

[1] *Planes de Contingencia. La continuidad del negocio en las organizaciones*. Juan Gaspar Martínez. 2004. Editorial Díaz de Santos.

[2] *SIC. Seguridad en Informática y Comunicaciones.* Nº 63, febrero 2005. Bibliografía.

01-cap1.indd 1 13/8/06 11:15:21

Lo cual agradezco a los editores de este clásico de la literatura del sector.

No obstante, en entrevistas realizadas posteriormente con profesionales interesados en estas materias, bien simplemente lectores del libro, bien asistentes a seminarios o conferencias en los que he participado, me daba cuenta de que si alguno de ellos iba buscando en el libro un "manual de elaboración", podría quedar frustrado al no encontrarlo.

De este modo, fue germinando en mi cabeza la idea de complementar el libro anterior con algo mucho más cercano al mundo práctico. Algo que diera respuesta a tantos profesionales que bien por la petición de sus superiores, bien por su propia iniciativa y profesionalidad, se plantean la elaboración de un plan y, como dice más de uno, "no saben por dónde empezar".

La tarea podría considerarse superflua a estas alturas. Cuando todo el mundo admite que, de forma más o menos directa, las tecnologías de la información están presentes en casi cualquier actividad de la vida cotidiana. Cuando todas las organizaciones depositan su gestión y, lo que es más importante, uno de sus principales activos, la información, en soportes que son tratados por estas tecnologías, los planes de contingencia deberían ser de uso común en cualquier organización, grande o pequeña. En definitiva, no son sino medidas preventivas, de buena práctica empresarial, que garantizan que la actividad de esa organización está debidamente salvaguardada y su continuidad, garantizada.

Sin embargo, la realidad es terca y nos hace enfrentarnos a situaciones en las que queda patente que tal suposición se muestra, cuando menos, atrevidamente optimista.

Es conocido el dicho de que existen verdades, mentiras y estadísticas. Evidentemente, estas últimas se acercarán más a las primeras o a las segundas, en función del rigor con que se plantean y elaboran. Y en el sector de la seguridad de la información en España, ni existen muchas estadísticas, ni la mayor parte de las veces se conoce su proceso de elaboración. Por eso hemos de confiar en la solvencia de las organizaciones que las publican para intentar sacar alguna conclusión.

Hace relativamente poco tiempo, el diario *El País* publicaba los resultados de un barómetro realizado acerca de la existencia de planes de continuidad de negocio en empresas españolas. En el artículo citado [3], no se citaba la metodología empleada para la realización de dicho barómetro ni el número de empresas a las que se había presentado la encuesta, pero se llegaba a conclusiones realmente desoladoras.

En primer lugar, a la pregunta de si la empresa cuenta con un plan de continuidad de negocio, un 55,4% respondía que no, porcentaje al que yo añadiría el 13,8% que contestaba que no, pero que está previsto en los próximos meses. He oído muchas veces esa respuesta tan prometedora, pero después no se materializa nunca o casi nunca. Es decir que, según esos datos, dos de cada tres empresas no tienen un plan de continuidad, concentrándose el mayor número de ellas en la franja de entre 30 y 60 M¤ de facturación anual.

Dadas las fechas en que estos datos se publicaban, hay que pensar que todavía estaban recientes en la memoria los detalles del incendio en el edificio Windsor, por lo que la disposición de todo el mundo sería positiva, pero la memoria humana es frágil y la presión del día a día hace posponer, algunas veces de forma indefinida, cuestiones que son de hecho vitales y que su ausencia puede poner en peligro la vida de la organización.

Ante actitudes similares, uno tiende a caer en la tentación de considerar que estas actitudes sólo ocurren entre nosotros, que por ahí fuera las cosas se hacen mejor. Y sin embargo, aun admitiendo nuestro retraso en mentalización de seguridad, de vez en cuando te encuentras con que "en todas partes cuecen habas", aunque ello no sirva ni de consuelo, ni mucho menos, de ejemplo.

En el informe anual que publica Ernst & Young sobre seguridad de la información a nivel global, en el correspondiente a 2004, se dice lo siguiente:

"El Informe ha encontrado que ante las crecientes amenazas a la seguridad de su información, las organizaciones de todo el mundo están fallando en su protección. Aunque los más altos responsables de las compañías están cada vez más concienciados de los riesgos a

[3] *El País*, 24 de abril de 2005. Suplemento de *Economía.*

los que está expuesta su información, no actúan consecuentemente. Más del 70% de las 1.233 organizaciones encuestadas, que representan las principales compañías de 51 países, fallan en sus políticas de entrenamiento y sensibilización de sus empleados acerca de la seguridad de la información. A medida que las organizaciones se mueven hacia modelos de negocio más descentralizados a través de la externalización de los sistemas de información y otros servicios, se hace cada vez más difícil para la dirección retener el control de la seguridad de la información y ser conscientes del nivel de riesgo a que se exponen".[4]

Por otra parte, según el informe "El Estado de la Seguridad de la Información 2004", elaborado por PriceWaterhouseCoopers a partir de 8.000 encuestas a responsables TIC de 62 países, la seguridad de la información es una preocupación creciente para las empresas porque afecta directamente a su reputación, su cuenta de beneficios y su desarrollo. Sin embargo, de todo el gasto en TIC, sólo el 11,3% se destina a soluciones de seguridad [5].

Mucho más recientemente, con motivo de la explosión sucedida el domingo 11 de diciembre de 2005 en los almacenes de combustible de Buncefield - Hertfordshire, cerca de Londres, un periodista de la BBC, entrevistando el lunes a Lyndon Bird, Director de los Servicios Técnicos del British Continuity Institute, deducía que la "continuidad del negocio" había funcionado perfectamente ya que las primeras notas de prensa indicaban que el impacto en su continuidad había sido prácticamente nulo en las entidades afectadas por la explosión.

Sin embargo, continúa Lyndon Bird*, mis reservas expresadas al entrevistador por la mañana, comenzaron a verse confirmadas el mismo lunes por la tarde.* Una de las compañías afectadas suspendió su cotización en Bolsa, el martes por la mañana, la prensa daba noticia de que otra compañía afectada había perdido diez millones de libras por la caída de sus acciones; otras dos habían cerrado dos grandes depósitos de mercancías cerca del lugar del siniestro; otra más tuvo que reubicar a 1.500 empleados; y otra dedicada a dar servicios de

[4] Ernst & Young. *Global Information Security Survey* 2004.

[5] Red Seguridad. Marzo 2005.

logística, aún habiendo puesto en marcha su Plan de Contingencia Informático, no pudo reanudar sus actividades por encontrarse sus camiones en la zona acordonada por la policía [6].

La situación, como puede verse, dista mucho de ser satisfactoria incluso para un observador tolerante. Por ello, al inferir que esta situación es reflejo de la cantidad de camino que todavía falta por recorrer, me lancé a la siempre estimulante tarea de escribir otro libro. Pero esta vez algo en forma de manual, de guía que respondiera a la clásica pregunta de "por dónde empiezo".

Es seguro que los muchos y muy buenos consultores con que cuenta este sector harían las cosas de otra manera con unos resultados similares o mejores. La sincera intención por parte del autor no es dar lecciones a nadie, sino poner en manos de los responsables de las organizaciones una herramienta más, no excluyente, que facilite su trabajo.

1.1. OBJETIVOS DE ESTA GUÍA

Al igual que no hay dos organizaciones iguales, no hay dos planes de continuidad de negocio iguales. Voy más allá, un mismo plan, desarrollado por dos equipos diferentes o en dos momentos diferentes, no tienen por qué coincidir. Con ello quiero advertir que, si bien la guía proporciona unas pautas a seguir, el contenido que se dé a cada fase, jalón o tarea, será función no solamente de la organización en cuestión, sino de una serie de parámetros que probablemente variarán de acuerdo con los objetivos individuales de la organización en particular y de las premisas que se establezcan en los pasos iniciales.

Los objetivos de esta Guía son, por tanto, proporcionar un esquema de elaboración, tanto en secuencia como en contenidos, dejando para los responsables de cada organización las decisiones de qué se debe incluir en cada documento. Sin embargo, con objeto de facilitar la tarea de incorporación de contenidos, la Guía propone modelos que, convenientemente adaptados a las necesidades individuales, pueden facilitar esa tarea.

[6] Continuity Central Newsletter. Enero 2006

1.2. OBJETIVOS DE UN PLAN DE CONTINUIDAD DE NEGOCIO

Un Plan de Continuidad de Negocio debería hacer frente a estos objetivos específicos:

- Aumentar la probabilidad de continuidad de las funciones críticas de la organización en caso de que un incidente interrumpa las operaciones informáticas en las que se apoyan.
- Proporcionar un enfoque organizado y consolidado para dirigir actividades de respuesta y recuperación ante cualquier incidente o interrupción de trabajo imprevista, evitando confusión y reduciendo la situación de tensión.
- Proporcionar una respuesta rápida y apropiada a cualquier incidente imprevisto, reduciendo así los impactos resultantes de interrupciones de trabajo a corto plazo.
- Recuperar las funciones críticas de negocio de manera oportuna, aumentando la capacidad de la organización para recuperarlas ante un incidente que haya dejado las instalaciones informáticas dañadas o destruidas.
- Aumentar la probabilidad de continuidad del servicio informático de la organización en caso de que un incidente interrumpa sus operaciones normales.
- Reducir el tiempo de recuperación, y como consecuencia, las pérdidas económicas, directas e inducidas, como resultado de un desastre.
- Reducir el impacto, tangible o intangible, en las áreas funcionales como consecuencia de una interrupción del servicio informático.
- Realizar la recuperación de las funciones críticas, mediante el desarrollo de los procedimientos necesarios para:
  - — reducir la duración de la recuperación;
  - — minimizar el coste de la recuperación;

— evitar la confusión y reducir el riesgo de errores;

— evitar la duplicación de esfuerzos.

1.3. CÓMO USAR LA GUÍA

La secuencia que siguen los capítulos de esta Guía responde a grandes rasgos a la secuencia lógica de desarrollo de un plan. Cada capítulo contiene una serie de ayudas que ofrecen:

- Pautas para la elaboración de documentos.
- Alternativas para la toma de decisiones.
- Modelos de formularios para la incorporación de datos.
- Modelos de documentos para su uso, adaptación o modificación.

De esta forma, siguiendo las indicaciones de cada capítulo, se va construyendo el plan.

Con objeto de facilitar la tarea a quienes quieran utilizar la Guía para el desarrollo de su Plan de Continuidad de Negocio, todos los formularios y modelos presentados en ella se recogen en un CD que les permitirá un uso más amigable y flexible de los mismos.

Sin embargo, esta secuencia de elaboración no termina al llegar al final del proceso. Determinadas decisiones que se van tomando a lo largo de su desarrollo pueden obligar a la revisión de otras decisiones ya tomadas a medida que el desarrollo progresa. Por ejemplo, la definición del alcance se hace en las primeras etapas, sin embargo, en función de dicho alcance, la disponibilidad o coste de las soluciones de continuidad pueden obligar a la revisión del alcance para reducirlo o ampliarlo. De esta forma, el proceso será un desarrollo y revisión reiterativos hasta completar un diseño final. En cualquier caso, el diseño nunca será definitivo ya que, como se explica más adelante, el plan debe mantenerse vivo mediante actualizaciones que respondan a la evolución de necesidades, consecuencia de la evolución de la propia organización.

2

Definiciones previas

Antes de acometer la elaboración propiamente dicha del plan, es muy importante esta fase previa de definiciones. La sensatez y el pragmatismo deben imperar en la definición de los objetivos y el alcance del proyecto. Una cosa es lo que se debería hacer y otra lo que se puede hacer. Los recursos siempre son limitados, lo cual no impide implantar medidas encaminadas en la dirección correcta. Demasiadas veces se dan los casos de organizaciones (o personas), que pretenden pasar del cero al infinito, casos en los que no se dispone de las más elementales medidas que garanticen la continuidad de sus operaciones y se pretende llegar a la solución mágica que resuelva cualquier problema "con solo apretar un botón".

Hay que conocer muy bien las propias necesidades, pero también las propias limitaciones y definir claramente desde el principio para qué se está planificando y para qué NO se está planificando, mediante la definición de los llamados supuestos de partida. Es la única manera de definir un proyecto a la medida de las necesidades (aunque no se puedan cumplir todas de una vez), pero teniendo en cuenta los recursos de que se dispone. Si en una primera aproximación solamente se puede cumplir con un determinado porcentaje de las necesidades y dar un alcance limitado al plan, siempre será preferible esto a "dejarlo para mejor ocasión". Aunque resulte

02-cap2.indd 9 13/8/06 11:20:32

una obviedad, si ocurre un incidente, es mejor tener copias de seguridad correctamente realizadas y custodiadas, aunque sea ésta la única medida del plan que se ha implementado.

2.1. ALCANCE DEL PLAN

El Plan de Continuidad de Negocio debe ser diseñado para crear una situación de preparación que proporcione una respuesta inmediata diseñada en función de una serie de posibles escenarios previamente definidos.

En primer lugar, será preciso definir qué departamentos, dependencias, instalaciones, etc., van a ser incluidas en el plan. No es lo mismo abarcar solamente las instalaciones de un CPD centralizado que incorporar otras dependencias que puedan contener centros satélites. No es lo mismo desarrollar un Plan de Contingencia Informático, que abarque solamente la recuperación y continuidad de las actividades informáticas que un Plan de Continuidad de Negocio que considere todas las funciones críticas de la organización.

Después, será preciso elegir, entre todo el catálogo de posibles amenazas, cuáles de ellas son más probables y descartar aquellas que, aun siendo posibles, su probabilidad de ocurrencia es mucho menor. Aquí juega un papel muy importante el presupuesto disponible para la implementación del plan. La consideración de algunas amenazas puede entrañar la necesidad de implementación de medidas que supongan unos costes importantes. Es decir, a la hora de definir el alcance del plan se deben tener muy en cuenta las limitaciones presupuestarias y dimensionar el mismo de acuerdo con esas limitaciones. Cada uno de los supuestos elegidos puede requerir soluciones muy diferentes en su diseño y coste. Por otra parte, como muchas otras que habrá que tomar a lo largo del desarrollo e implementación, la decisión del alcance del plan debe estar aprobada por la dirección.

Formulario 2.1

2.1. Alcance del plan

1. El plan abarca las siguientes instalaciones... (oficinas centrales, sucursales, centro de proceso de datos, informática distribuida, etc.) y las siguientes áreas funcionales... (financiero, comercial, RR HH, fabricación, etc.).
2. Se consideran los siguientes tipos de incidentes:
   - Los que causen un daño físico en las instalaciones o equipos, como fuego, humo o daños por agua.
   - Los que afecten de forma indirecta la posibilidad de acceso a las instalaciones, como evacuación de emergencia por amenaza de bomba, o amenazas externas tales como incendios en instalaciones cercanas, fuga de gases tóxicos, etc.
   - Desastres regionales no previstos o inesperados, tales como huracanes o inundaciones, que puedan causar daños en las instalaciones y equipos.
   - Desastres regionales no previstos o inesperados, que puedan impedir el acceso normal al personal encargado de las operaciones informáticas, aunque las instalaciones estén intactas, tales como grandes nevadas, inundaciones, etc.
   - Cualquier incidente externo que pudiera potencialmente causar una interrupción de las operaciones del negocio, tales como la pérdida de los servicios de suministro eléctrico o de telecomunicaciones.
   - Cualquier incidente que afecte al funcionamiento del hardware o del software y que suponga una interrupción superior a las 24 horas.
   - Cualquier incidente que suponga la paralización de actividades de la organización por motivos ajenos a la tecnología, tales como problemas laborales propios o del sector o problemas laborales que afecten al área geográfica donde se encuentra ubicada la organización.
   - ..... (*)
3. Se descartan los siguientes tipos de incidentes:
   - ..... (**)

(*) Ejemplos genéricos. Sustituir por datos potencialmente probables.
(**) Relacionar aquí las amenazas descartadas y razones para ello (probabilidad o coste)

Preparado por:	Conforme:	Aprobado por:
Fecha:	Fecha:	Fecha:

2.2. PREMISAS DE PARTIDA

Aparte de la definición del alcance del plan, es preciso definir y acotar una serie de supuestos sobre los cuales basar todas las actuaciones en las que se fundamenta el plan. La posibilidad de aplicación de las medidas planificadas puede depender de múltiples factores externos. En la medida que esos factores se comporten de una u otra forma, las medidas previstas serán aplicables o no. Conviene pues, enumerar esos supuestos para, si la dirección considera que son excesivamente optimistas o pesimistas, corregir el plan a la baja o al alza, ya que ello repercutirá, como siempre, no sólo en el coste de las medidas a implantar, sino en un mayor o menor índice de cobertura.

Como siempre, sin ánimo de ser exhaustivo, algunas de esas premisas podrían ser como las que se reflejan en el formulario que se muestra a continuación, debiendo elegir las más adecuadas a la organización.

Formulario 2.2

2.2. Premisas de partida

El plan se ha desarrollado sobre los siguientes supuestos:

- Sólo el área habitual de trabajo ha sido afectada por el incidente; todos los lugares alternativos predesignados están intactos.
- Los almacenes externos de archivos críticos de *backup* e información están intactos y accesibles.
- El personal cualificado en cantidad suficiente (identificado en los capítulos correspondientes) está disponible para realizar los trabajos de recuperación.
- Los trabajos de recuperación se están realizando de acuerdo con los procedimientos que han sido descritos en el Plan de Continuidad del Negocio.
- Las copias de seguridad y su correspondiente rotación (incluyendo papel, fichas, películas, y soportes electrónicos) se han realizado correctamente, y se ha corregido cualquier riesgo identificado.
- El *backup* de las telecomunicaciones y las estrategias de recuperación identificadas en otros capítulos del plan están completamente realizadas y comprobadas.

(continúa)

(continuación)

- Las estrategias de recursos y soluciones de recuperación (por ejemplo: soluciones de reposición de ordenadores) están disponibles, realizadas y comprobadas satisfactoriamente.
- Las organizaciones externas como clientes, suministradores y organismos públicos, cooperarán razonablemente durante el periodo de los trabajos de recuperación.
- Se han realizado adecuadamente los programas de pruebas del plan y las modificaciones pertinentes como consecuencia de su resultado.
- La revisión del plan, mantenimiento, y actualizaciones están realizadas con periodicidad para asegurar que responde a las necesidades de cada momento.
- Se han realizado adecuadamente los programas de sensibilización y entrenamiento.

Preparado por:	Conforme:	Aprobado por:
Fecha:	Fecha:	Fecha:

2.3. FUNCIONES DE LA DIRECCIÓN

El proceso de elaboración e implementación del plan debe ser cuidadosamente realizado y previamente propuesto a la Dirección para su aprobación, por tanto, para la mayor parte de los incidentes, los procedimientos de respuesta y recuperación están previamente estudiados y aprobados. Las funciones de la Dirección se limitan a la revisión y aprobación de cualquier acción que exceda de las estrategias de respuesta y recuperación planificadas y previamente aprobadas.

Solamente en aquellos casos en los que el incidente haya sobrepasado las previsiones será precisa la intervención directa de los órganos directivos.

En esos casos, el equipo de Gestión de Incidentes es responsable de la preparación de informes para la Dirección, con la que ayudar a la gestión del día a día y a la toma de decisiones acerca de cuestiones no previstas en el plan. Ese informe podría contener los datos que se recogen en el Formulario 2.3.

Formulario 2.3

2.3. Informe a Dirección

En el supuesto de suceder cualquier incidente, el equipo de Gestión de Incidentes, una vez atendidas las decisiones más urgentes descritas en el Plan de Acción, emitirá un informe a la Dirección con el contenido siguiente:

1. Estado de las actividades de respuesta a la emergencia.
   - Evacuación del edificio.
   - Respuesta de los organismos públicos.
2. Descripción del incidente:
   - ¿Qué ocurrió?
   - Localización del suceso.
   - Hora del suceso.
   - Supuesta causa.
3. Informe de heridos y víctimas mortales (si los hay):
   - Nombre de las víctimas mortales.
   - Nombre y estado de los heridos.
   - Victimas potenciales adicionales.
4. Áreas afectadas:
   - Departamentos / áreas afectadas.
   - Ocupantes.
   - Edificios adyacentes.
   - Estado actual.
   - Posibilidad de acceso a corto plazo.
   - Impacto en las operaciones del negocio.
5. Estado del Plan de Acción.
   - Localización del Centro de Control.
   - Situación de las comunicaciones.

(continúa)

(continuación)

- ¿Qué se ha hecho hasta ahora?
- Planes a corto plazo.

6. Atención prestada por los medios de comunicación y reacciones que se van produciendo.

7. ..... (*)

(*) Ejemplos genéricos. Sustituir por la información adecuada a la organización.

Preparado por:	Conforme:	Aprobado por:
Fecha:	Fecha:	Fecha: