TEMA 5: RECUPERACIÓN DE SISTEMAS INFORMÁTICOS EN SITUACIONES DE DESASTRE

5.0 Introducción

La labor de Gestión, en todos sus campos de aplicación, tiene como objetivo el uso racional y efectivo de recursos. En una organización, después del personal, el recurso más importante es la información.

La gestión de la información, o de los recursos informáticos, significa hoy el desarrollo, implementación y refinamiento de herramientas para recolectar, procesar y distribuir información en tiempo y forma. Estas actividades consumen una gran cantidad de esfuerzo y dinero, y se consideran una inversión que retornará los datos precisos para el soporte de la toma de decisiones.

Sin embargo, un aspecto a menudo olvidado es la dependencia entre el funcionamiento del negocio y el funcionamiento de los recursos informáticos, es decir, la imposibilidad de continuar las labores productivas si se produce un fallo (de algún tipo) lo suficientemente grave en el sistema de información. Este tipo de fallos, que afectan o imposibilitan el desarrollo de las actividades productivas, se denominarán en lo que sigue un *desastre*.

Las situaciones de desastre se producen, por lo tanto, en el momento en que una actividad productiva se ve parada por la falta de apoyo informático y por la imposibilidad de su realización por otros medios. Incluso en el caso de que dicha actividad pueda realizarse manualmente, puede ocurrir que la duración de la caída de los sistemas sea lo suficientemente larga como para convertir la solución manual, inicialmente buena, en inviable por las repercusiones posteriores sobre la organización.

De hecho, las empresas, dependiendo de su grado de informatización, son muy sensibles a la caída de sus servicios informáticos. Un estudio del año 1979 [Aasgaard, 79] muestra la caída en el porcentaje de negocio (base 100) ante un desastre de una determinada duración en las empresas financieras (Figura 5.1) Como dato representativo, una organización ve disminuir su capacidad de negocio al 4% del total después de una caída de 10 días en su sistema informático.

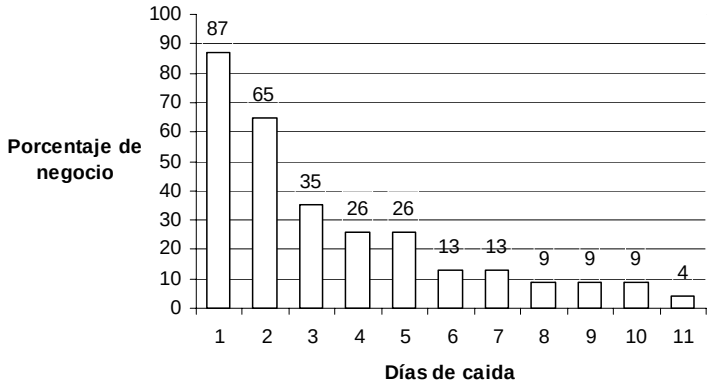


Fig. 5.1 Caída de las actividades del negocio en empresas financieras ante un fallo de sistemas de una determinada duración. [Aasgaard, 79]

Aunque las empresas financieras son un caso extremo dentro de la vulnerabilidad ante un desastre proporcionan una buena visión de conjunto. Aún más, aunque los datos proporcionados sean de 1979, siguen siendo asombrosamente vigentes, cuando no optimistas. Con la proliferación de la informática personal y departamental, redes de ordenadores y en general con la implicación de la informática en todas las labores productivas, las posibles fuentes de problemas se multiplican y su prevención y valoración se hace más difícil.

Así, en lo que sigue, se mostrará una metodología de desarrollo de planes de recuperación, los cuales permitirán poner un orden en las actividades de recuperación y puesta en marcha de los servicios informáticos después de un desastre.

5.1 El entorno del plan de recuperación

Siguiendo con lo que se ha indicado en la introducción, un plan de recuperación (ante desastres) permite poner un orden en las actividades de recuperación y puesta en marcha de los servicios informáticos de una organización después de una caída. Sin embargo, esto es sólo una visión estática de lo que es esencialmente un problema dinámico. En realidad, un plan de recuperación implica un compromiso de la organización para desarrollar y mantener en el tiempo los recursos necesarios para recuperarse de una caída de sus sistemas, así como fomentar una política de responsabilidad del personal frente al correcto funcionamiento de los servicios informáticos y, por ende, de las actividades productivas. En concreto, un buen sistema de recuperación de desastres debe relacionarse con:

- Las administraciones públicas (debido a directrices específicas de seguridad, como ocurre con las empresas financieras)
- Casas aseguradoras.
- Auditores.
- Proveedores de sistemas de recuperación.
- Usuarios de los sistemas.
- Directivos.

La bondad del sistema de recuperación dependerá en buena medida de cómo poder coordinar todos los elementos anteriores de forma coherente con el objetivo de supervivencia de los servicios informáticos de la organización. El recurso humano que tendrá la responsabilidad de la coordinación de los esfuerzos se denomina coordinador de recuperación. Esta persona tiene la responsabilidad de, además de desarrollar el plan, y mantenerlo en el tiempo, relacionarse con todas las personas o instituciones anteriores para lograr efectividad en las tareas de recuperación.

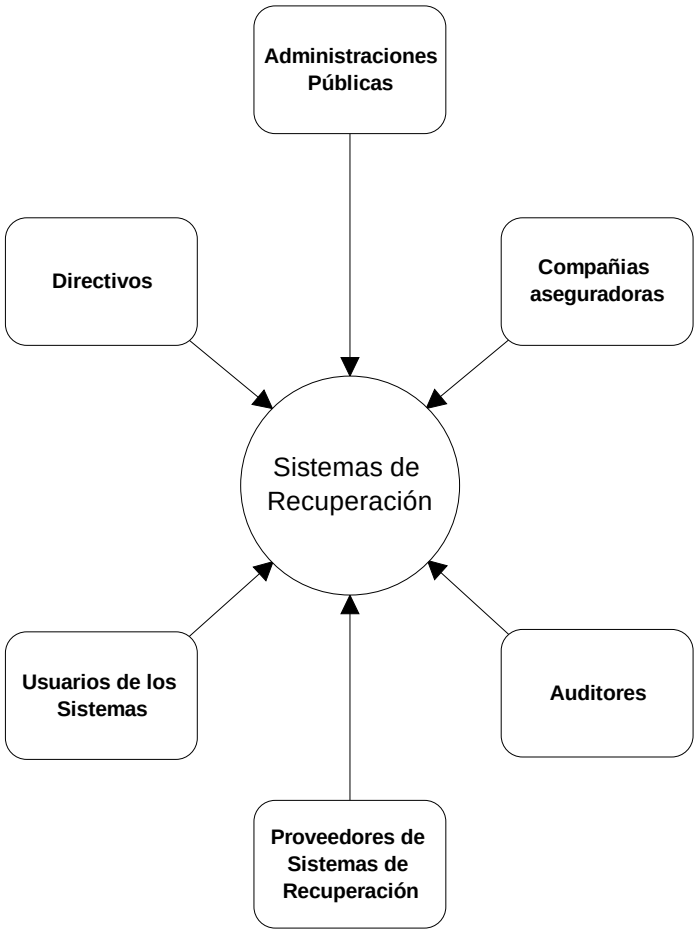


Fig. 5.2 Entorno de los sistemas de recuperación de desastres.

5.1.1 El coordinador de recuperación

El coordinador de recuperación es la persona encargada de realizar y mantener en el tiempo el plan de recuperación. No existe un perfil específico que defina este puesto, pero debido a sus funciones debe ser capaz de:

- Trabajar de forma metódica.
- Comunicarse adecuadamente con clientes internos o externos, así como con proveedores de servicios y organismos oficiales.
- Evaluar ofertas de productos y servicios.
- Conocer y aplicar los principios básicos de planificación y gestión de proyectos.

- Ser perseverante en sus funciones, y asumir la responsabilidad que le concierne en la supervivencia de los servicios informáticos de la organización.

Naturalmente, para realizar sus funciones, que muchas veces se verán como una "perdida de tiempo", ya que interrumpe el desarrollo de aplicaciones sin aportar ningún tipo de trabajo "productivo", el coordinador debe estar respaldado por la dirección de informática, y ésta le debe proporcionar la autoridad suficiente para que pueda desarrollar su trabajo.

Lo dicho anteriormente implica que el coordinador debe pertenecer a la Organización; pero no siempre existe el personal específico para ocupar el puesto de coordinador, o la organización no desea emplear a un recurso a tiempo completo en esa función. Otras veces, la organización no posee el conocimiento suficiente para desarrollar adecuadamente el plan. En estos casos intervienen los consultores externos.

Muchas casas consultoras ofrecen a sus clientes planes de recuperación. Esta es otra posibilidad para conseguir la seguridad de los sistemas. En este caso, no existe exactamente un coordinador, sino que un analista externo realiza el trabajo de construcción del plan y, probablemente, sus revisiones periódicas.

5.2 Metodología

No existe un método comúnmente aceptado en el desarrollo de planes de recuperación. A diferencia de otros métodos, por ejemplo el diseño e implementación de aplicaciones, el concepto de plan de recuperación es relativamente nuevo y no existe demasiada literatura al respecto.

Por otra parte, la naturaleza del plan de recuperación es coyuntural. Sólo se manifiesta totalmente cuando todo falla, es decir, cuando caen los servicios informáticos de la organización, que es precisamente lo no deseado.

No obstante, existen una serie de etapas genéricas, y un conjunto de técnicas y recomendaciones que pueden servir como base en la construcción de un plan de recuperación. Las etapas que proponemos son las siguientes:

1 - Definición de objetivos y recursos.

- Definición de metodologías.
- Definición de objetivos.
- Nombramiento del coordinador.

2 - Análisis de riesgo.

- Construcción y distribución de cuestionarios.
- Identificación de funciones críticas.
- Definir objetivos de recuperación.

3 - Desarrollar sistemas de prevención.

- Desarrollar protección de recursos informáticos.
- Desarrollar estrategia de backup.
- Desarrollar protección de sistemas.
- Desarrollar protección de redes.

4 - Definir equipos de recuperación y aprobar el plan.

- Definir equipos de recuperación.
- Escribir el plan.
- Probar el plan.
- Aprobar formalmente el plan.

Con posterioridad al desarrollo y aprobación del plan de recuperación, éste debe mantenerse en el tiempo. Así, como última (y continua) actividad de la metodología podríamos incluir:

5 - Mantenimiento del plan.

- Registro de cambios.
- Pruebas periódicas.

La figura 5.3 muestra gráficamente la secuencia de tareas, y a continuación, se describe en detalle cada una de las etapas genéricas de la metodología propuesta.

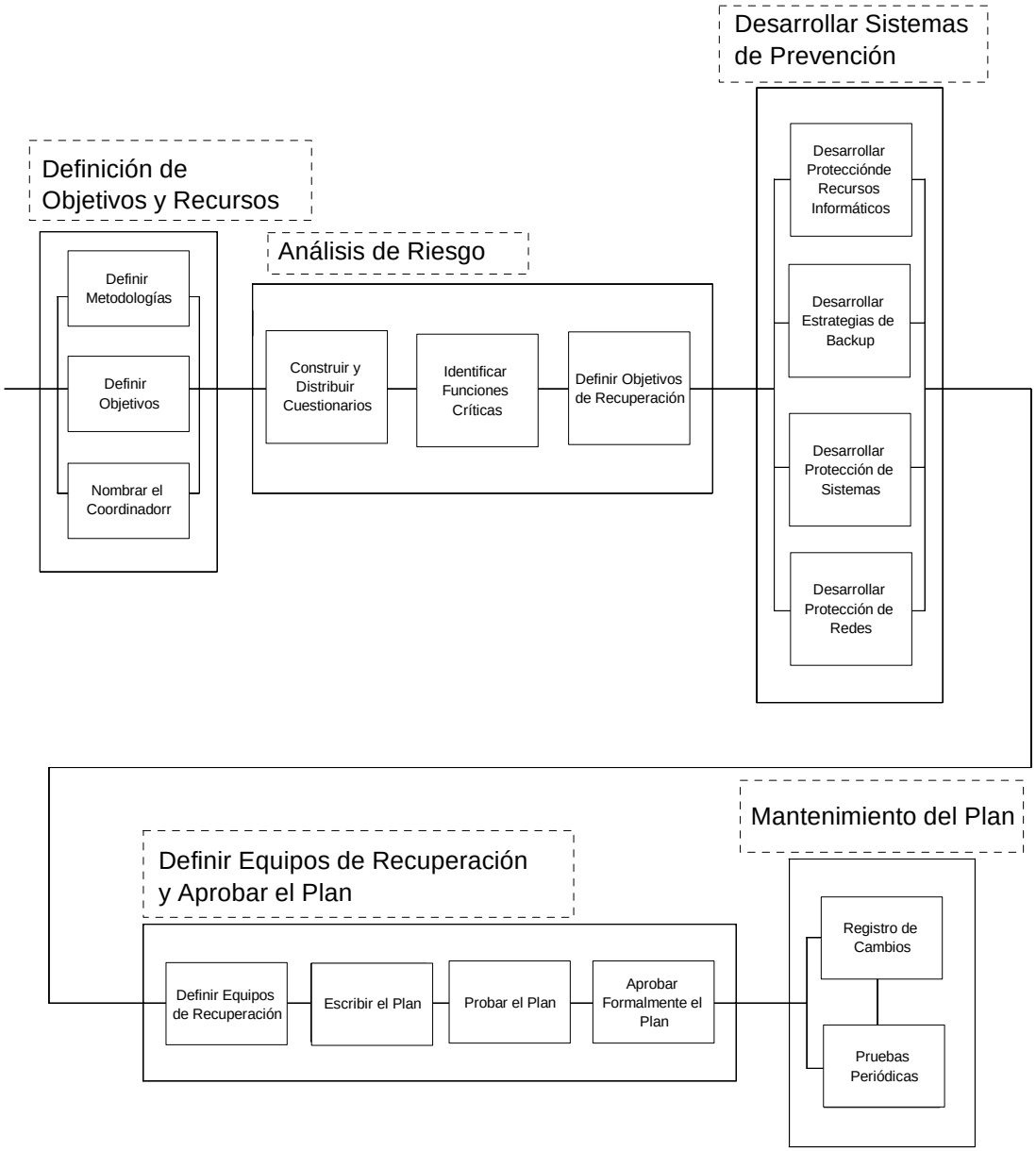


Figura 5.3 Secuencia de Tareas de la Metodología

5.2.1 Definición de objetivos y recursos [1]

La primera fase de la metodología propuesta tiene como objetivo definir las líneas generales del proyecto. Al igual que en el desarrollo de aplicaciones, se establecen los mecanismos a utilizar (metodologías), objetivos a conseguir y se define el equipo que las realizará, en este caso, el coordinador de recuperación.

5.2.1.1 Definición de metodologías

[1] Esta primera fase es independiente de la metodología, es decir, forma parte más del proceso de gestión que del técnico. Así, en lo que sigue se podría describir cualquier metodología que abordase la construcción de planes de recuperación. La metodología aquí propuesta no pretende ser exhaustiva, sino crear un marco de referencia para la comprensión de otras metodologías comerciales o particulares de una organización.

Esta tarea se realiza si la organización no tiene implantada una metodología de desarrollo de planes de recuperación. Consiste en evaluar y escoger una metodología específica, entre las disponibles en el mercado, para la realización del plan de recuperación. Tiene especial relieve en el momento en que el plan va a realizarse por analistas externos, o por un equipo formado por personal de la organización y apoyo externo.

En el caso de que el plan de recuperación vaya a ser realizado por analistas externos, esta tarea debería contemplar también la evaluación de la metodología presentada para la realización del proyecto y la comparación con otras metodologías presentadas por otras casas consultoras.

5.2.1.2 Definición de objetivos

Esta tarea define aquellos objetivos que se deben alcanzar al final del proyecto. Estos no tienen por qué estar restringidos al ámbito del sistema de información, sino que pueden abarcar a los recursos humanos, políticas de la organización, etc. Ejemplos de objetivos podrían ser:

- En el caso de desastre, el plan debe prever una recuperación de los sistemas en un plazo máximo de siete días.

- Todo el personal de la organización debe ser entrenado y debe estar preparado para actuar correctamente en el caso de desastre.

- Paralelamente al desarrollo del proyecto, debe formarse a personal interno para el mantenimiento en el tiempo del plan.

5.2.1.3 Nombramiento del coordinador

Esta tarea tiene como objetivo nombrar al coordinador de recuperación. Como ya se ha indicado anteriormente, el coordinador es la persona que desarrolla y mantiene el plan.

El coordinador no tiene por qué ser necesariamente personal interno de la organización. Debido a que las labores de realización pueden confiársele a un consultor externo, en esta etapa se puede también decidir a qué casa consultora se le confía el proyecto de desarrollo del plan de recuperación.

Los aspectos de mantenimiento dependen de los objetivos marcados en el inicio del proyecto. Así, el mantenimiento puede confiársele a la misma casa consultora mediante revisiones periódicas, o puede formarse a personal interno para desarrollar estas funciones.

5.2.2 Análisis de riesgo

La fase de análisis de riesgo tiene como objetivo analizar las funciones productivas y crear un baremo de "criticidad". Este baremo clasifica las funciones productivas respecto a su resistencia a la caída de los servicios informáticos y, por lo tanto, respecto a su posible realización manual o por otros medios en el caso de desastre.

Además de la criticidad ante la caída de los servicios informáticos, en la fase de análisis de riesgo se deben identificar los peligros a los que están sometidas las funciones productivas (fuego, caídas de corriente, corrupción de los medios magnéticos, etc.) Por último, se deben fijar objetivos que servirán de base a procedimientos para:

- Eliminar los riesgos evitables.
- Minimizar el impacto de los riesgos, si éstos no se pueden evitar.

5.2.2.1 Definición y distribución de cuestionarios

Esta tarea, con la siguiente, forman el ciclo de investigación/análisis de la metodología propuesta. En esta tarea se preparan cuestionarios que posteriormente serán distribuidos al personal que usa y dirige los sistemas en el trabajo diario. Los cuestionarios se dirigen a todos los usuarios de un sistema o aplicación específico, así como a aquellos responsables de administrarlo o mantenerlo.

Otro medio de obtención de datos es la entrevista. Esta puede usarse en sustitución o de forma complementaria con la aplicación de cuestionarios, ya sea para la obtención de datos como para esclarecer aquellos puntos que puedan considerarse oscuros y se desee obtener mayor información.

Los cuestionarios cubren los trabajos que se realizan en cada departamento, frecuencia de realización, uso de los sistemas informáticos y de comunicaciones y consideraciones de criticidad. El objetivo perseguido es obtener la información suficiente para clasificar y asignar prioridad a las funciones. La información obtenida con los cuestionarios debe incluir una lista completa de hardware, ya sea de sistema o de telecomunicaciones, y un inventario completo de aplicaciones y de sistemas software.

Además de las funciones hardware y software, existe otro elemento de los sistemas de información que no puede ignorarse, los datos. Identificar y clasificar los registros basándose en su importancia para la organización y las aplicaciones puede ser una tarea de enormes proporciones, sobre todo debido a la tendencia actual de dispersión de los datos en LAN's y PC's. El método de los cuestionarios puede ser válido para identificar los datos críticos, pero sin embargo se necesitarán fuentes complementarias de información, como la documentación de las aplicaciones o entrevistas a los responsables de administración y operación de sistemas. Si la organización dispone de un administrador de datos, esta tarea se verá notablemente simplificada.

No existen cuestionarios estándar definidos. Al final del tema se presentan una serie de ocho cuestionarios que pueden servir como base para que cada Organización desarrolle los suyos.

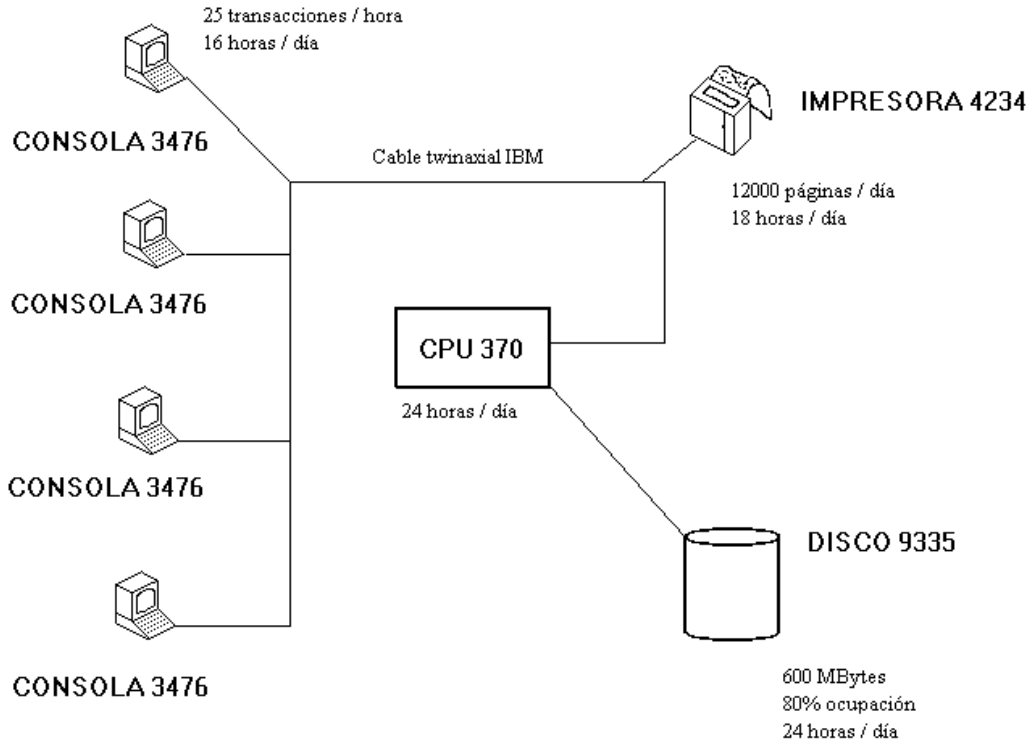
5.2.2.2 Identificación de funciones críticas

A partir de la información obtenida mediante los cuestionarios (y/o mediante las entrevistas realizadas), en esta etapa se crean diagramas de configuración del sistema, que son completados con datos de actividades (por ejemplo, 10 transacciones por segundo), datos de tráfico (60 Kbps) o datos de uso (20 horas/día)

Los diagramas de configuración del sistema muestran los elementos que son soporte de las actividades productivas conjuntamente con su uso. Un sencillo ejemplo (no existe una notación que defina cómo se deben hacer tales diagramas) podría ser el mostrado en la figura 5.4.

Fig. 5.4 Ejemplo de un diagrama de configuración.

Se pueden añadir al diagrama todos los detalles que se consideren relevantes para el desarrollo del proyecto.



Después se establecerá la tolerancia de cada aplicación o sistema, la cual definirá su criticidad. Por último, se identificarán los peligros a los que están expuestos, durante la actividad normal, los servicios informáticos.

5.2.2.2.1 Tolerancia y criticidad

La tolerancia es la medida que se utiliza para definir la criticidad de un sistema hardware o software. Representa el coste que supone para la organización el prescindir del uso de un determinado elemento de la configuración durante un tiempo específico.

De forma práctica, se utiliza el valor monetario para cuantificar la tolerancia de un determinado elemento. De esta forma, se cuantifica la pérdida económica que supone la caída de un sistema durante uno, dos, tres días, una semana, etc. Así, estableciendo cortes en una escala desde 0 a n, según lo estimado por la organización, se puede determinar la criticidad de un determinado elemento. Se dice que la tolerancia de la organización ante la pérdida de una determinada función es muy baja cuando el coste de la pérdida es muy alto. Típicamente, se establece una escala de cuatro tipos de criticidad, que se presenta esquemáticamente en la figura 5. Esta escala es la siguiente:

- Funciones críticas: Son aquellas funciones que no se pueden realizar aunque se puedan conseguir equipos idénticos a los utilizados en las actividades normales. Estas funciones no se pueden realizar manualmente de ningún modo. La tolerancia de la organización ante la pérdida de estas funciones es muy baja y, por lo tanto, el coste de la pérdida es muy alto.

- Funciones vitales: Son funciones o bien no realizables manualmente o bien difícilmente realizables de forma manual, en cuyo caso sólo se pueden realizar durante un corto período de tiempo. La recuperación de la información (generada a posteriori) en el Sistema de Información supone un trabajo considerable. La tolerancia de la organización ante estas funciones es un poco más alta que en el caso anterior.

- Funciones sensibles: Pueden realizarse manualmente, aunque con dificultades, durante un período extenso de tiempo. Necesitan un considerable trabajo de recuperación, como en el caso anterior.

- Funciones no críticas: Estas funciones pueden realizarse manualmente durante el tiempo que sea necesario. Apenas suponen coste de recuperación para la organización.

En lo referente a los datos manejados por las aplicaciones, debemos indicar que puede usarse la misma clasificación para definir su criticidad. En este caso se cambiaría dentro de la definición el concepto de uso de un determinado elemento por el de disponibilidad de un determinado ítem de información.

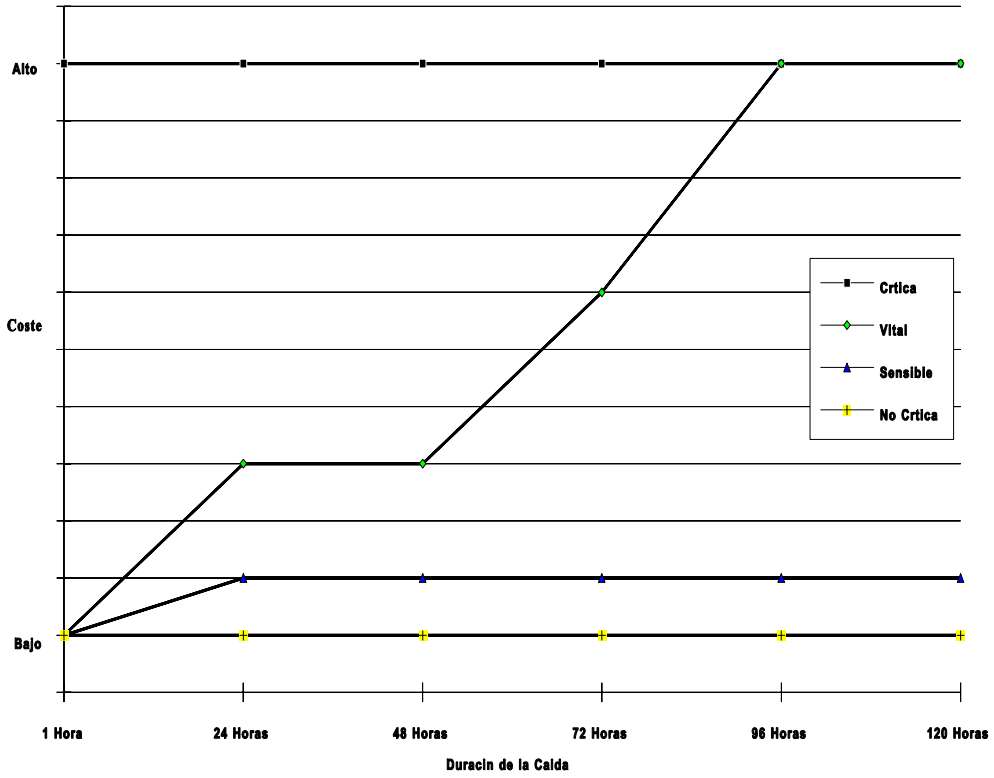


Fig. 5.5 Tolerancia de las funciones ante una caída de los sistemas de una determinada duración.

5.2.2.2.2 Identificación de peligros

Una vez clasificados los sistemas según su criticidad, se deben identificar aquellos "peligros" que existen durante la actividad normal de los sistemas. El mejor método para identificar peligros es buscar aquellos hechos que afectan normalmente al funcionamiento de los sistemas. Estos pueden resumirse, sin pretender ser exhaustivos, en: [2]

- Agua.
- Fuego.
- Problemas de alimentación.
- Fallos hardware o errores software.
- Destrucción accidental o intencionada de hardware o software.

Aunque parecen evidentes por sí mismos, popularmente no se da la importancia exacta a cada uno de estos factores. El agua y el fuego, por sí solos, son fuentes de más del 60% de los desastres que ocurren en centros de proceso de datos. El porcentaje es muy alto, máxime teniendo en cuenta que el daño debido al fuego ha disminuido en los últimos años debido a las mejoras de los sistemas de extinción.

[2] Para mas detalles, ver Anexo: Seguridad Física en Centros de Proceso de Datos.

Una vez identificados los posibles agentes que pueden causar disfunciones, se deben asociar a los elementos hardware o software que se pueden ver afectados. De esta manera, se tendrán identificados los "puntos débiles" de cada sistema o aplicación para, en la próxima tarea, enunciar objetivos con el propósito de eliminar los riesgos evitables y minimizar el impacto de aquellos que no se pueden evitar.

5.2.2.3 Definir objetivos de recuperación

Una vez identificada la criticidad de los sistemas, calculada su tolerancia o criticidad e identificados los peligros a los que están expuestos, tanto los sistemas como los datos, se deben definir objetivos que guiarán la construcción del plan de recuperación y el desarrollo de los sistemas de prevención.

Se identifican los peligros que afectan a los sistemas con el fin de evitarlos o paliar sus efectos si no son evitables. Los objetivos pretenden definir las tareas que deben abordar el plan de recuperación y los sistemas de prevención. La figura 5.6 expone los objetivos de esta tarea. Una vez identificados los peligros, debemos eliminar los evitables o prevenir los no evitables mediante los sistemas de prevención o el plan de recuperación. Los objetivos definen las tareas a realizar para lograr lo anteriormente expuesto. En este sentido, su definición es pareja a la creación de un análisis de requerimientos en un proyecto de ingeniería. Los objetivos definen los que hay que hacer, identificando las condiciones, tareas y estándares a aplicar.

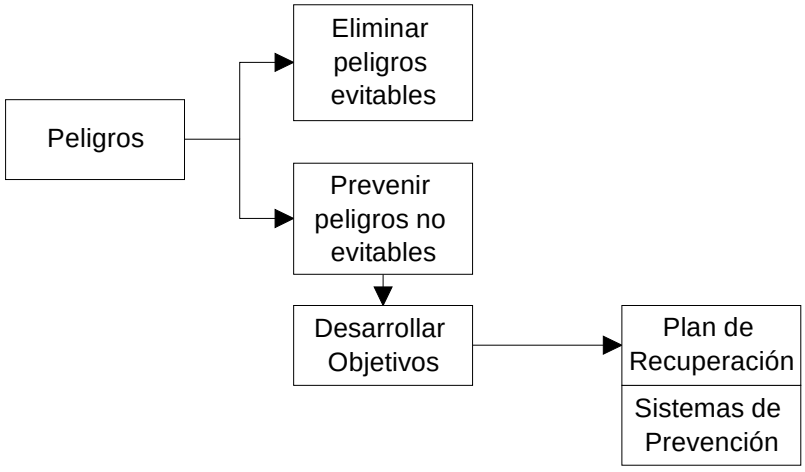


Fig. 5.6 Resumen de los objetivos de esta tarea

Un ejemplo de lista de objetivos puede ser la que se presenta a continuación. Esta lista es todavía demasiado genérica para servir de base a un plan de recuperación real, por lo que debería completarse con los detalles que aparezcan durante todo la fase de Análisis de Riesgo.

Objetivo principal

1. El coordinador de recuperación desarrollará una estrategia de protección de personas, propiedades y activos de la organización, que será aprobada por la dirección.

Mantenimiento del plan

2. El coordinador de recuperación establecerá una planificación temporal para revisión y mantenimiento del plan de recuperación. Deberá informar al personal de sus funciones en el marco del sistema de recuperación, así como fijar fechas y procedimientos para recoger sugerencias y comentarios.

3. El coordinador de recuperación usará los comentarios y sugerencias para revisar el plan de recuperación a intervalos periódicos.

4. El coordinador de recuperación realizará pruebas, planificadas o sin planificar, del plan de recuperación para verificar su validez.

5. El coordinador de recuperación planificará el entrenamiento del personal en lo referente al plan de recuperación.

6. Todas las actividades de prueba y formación deben estar convenientemente documentadas y archivadas para su revisión.

Entorno

7. El coordinador de recuperación revisará los sistemas de prevención de fuego, agua, etc., para asegurar su validez.

Control de la organización

8. El coordinador de recuperación trabajará con los responsables de los departamentos para desarrollar programas donde se advierta al personal de las funciones que tienen que proteger, las incidencias que deben comunicar y las acciones inmediatas que deben realizar en el caso de desastre.

9. El coordinador de recuperación trabajará con los responsables de los departamentos para desarrollar un programa que asignará responsabilidades concretas dentro del plan de recuperación al personal de cada departamento.

Recursos humanos

10. El coordinador de recuperación estará en contacto con el departamento de recursos humanos para registrar contrataciones o despidos de personal de la organización.

11. El coordinador de seguridad mantendrá un listín telefónico de los integrantes de los distintos equipos de recuperación.

Control de operaciones y accesos

12. El coordinador de recuperación trabajará con los responsables del sistema para coordinar las copias de seguridad de datos y aplicaciones.

13. El coordinador de recuperación identificará toda la documentación necesaria para el trabajo normal y comprobará que existan repuestos suficientes.

14. El coordinador de recuperación documentará las medidas obtenidas de los sistemas y redes acerca de su seguridad.

15. El coordinador de recuperación controlará todos los dispositivos de seguridad, claves de acceso, etc.

Desarrollo de aplicaciones

16. El coordinador de recuperación desarrollará un plan para la copia de seguridad de las aplicaciones en desarrollo.

Redes y sistemas

17. El coordinador de recuperación cuantificará las posibles pérdidas por fallo de los sistemas hardware.

18. El coordinador de recuperación desarrollará un plan para la recuperación de aplicaciones críticas en un intervalo de X horas.

19. El coordinador de recuperación documentará las responsabilidades de cada miembro de un equipo de recuperación en el caso de un desastre.

20. El coordinador de recuperación desarrollará una configuración mínima para asegurar la funcionalidad de los sistemas en el caso de desastre.

21. El coordinador de recuperación implantará procedimientos manuales para la sustitución de funciones del sistema en un intervalo de X horas en caso de desastre.

22. El coordinador de recuperación contactará con proveedores de servicios que puedan suministrar equipos de la configuración en un plazo de tiempo aceptable en el caso de un desastre.

Copia de seguridad

23. El coordinador de recuperación contratará los servicios de proveedores de almacenamiento externo de copias de seguridad.

24. El coordinador de recuperación definirá todos los elementos de la configuración que deben ser almacenados periódicamente de forma externa.

25.El coordinador de recuperación hará inventarios periódicos de los elementos de la configuración almacenados de forma externa.

Acciones de emergencia

26. El coordinador de recuperación tendrá en cuenta todas las restricciones legales que puedan afectar al plan de recuperación y a las acciones de emergencia que se puedan realizar.

27. El coordinador de recuperación desarrollará procedimientos que cubrirán todas las acciones que deban desarrollarse en el contexto de un desastre.

28. El coordinador de recuperación es el responsable de poner en marcha todas las acciones reflejadas en el plan de recuperación en el caso de un desastre.

29. El coordinador de recuperación realizará todas las acciones destinadas a pasar de la situación de emergencia a los niveles de trabajo normal en la organización.

5.2.3 Desarrollar sistemas de protección

En la fase anterior, Análisis de Riesgo, se han analizado y clasificado los sistemas atendiendo a su criticidad. De la misma forma, se han identificado los peligros que pueden afectar a los sistemas. Con esta información, y basándose en los objetivos desarrollados, deben establecerse mecanismos de protección y recuperación de sistemas frente a posibles desastres, es decir, implementar sistemas de protección.

Los sistemas de protección se pueden clasificar en cuatro tipos. En primer lugar, estarían aquellos que intentan proteger a los sistemas físicos frente al agua, fuego, polvo, caídas de corriente, etc. En segundo lugar, estaría la protección de los datos, formularios, documentos y aplicaciones, es decir, los sistemas de backup. En tercer lugar estaría la protección de la configuración de los sistemas hardware. En cuarto y último lugar estaría la protección de redes de telecomunicaciones.

5.2.3.1 Desarrollar protección de recursos informáticos

El objetivo de esta tarea es considerar todos aquellos peligros físicos (agua, fuego, etc.) que pueden afectar a los sistemas informáticos y evaluar los mecanismos disponibles en el mercado (extintores, sistemas de halón, detectores de fugas, etc.) para minimizar su impacto.

El coordinador de recuperación, para realizar esta tarea, debe evaluar cada problema potencial que afecta a cada elemento de la configuración y buscar en el mercado equipos específicos que lo eliminen. Si es necesario, debe consultar a expertos en el área para escoger aquellas ofertas que cubran determinados estándares del área u ofrezcan la suficiente seguridad.

5.2.3.2 Desarrollar estrategia de backup

Esta tarea es, probablemente, la más crítica en el entorno del plan de recuperación. La estrategia de backup debe cubrir tanto los datos de la organización como todos los documentos, formularios, aplicaciones, manuales, procedimientos, etc. que sean necesarios para poner en marcha las actividades en el caso de un desastre. Todos los elementos a los que se debe aplicar una estrategia de backup deben haber sido localizados durante el análisis de riesgo y estar clasificados respecto a su criticidad.

Como en el caso anterior, el coordinador de recuperación debe desarrollar procedimientos internos de copia de seguridad o relacionarse con proveedores de servicios de almacenamiento externo.

Existen muchas opciones de seguridad para los medios magnéticos y papel necesario para el trabajo normal en las organizaciones. Pueden desarrollarse servicios internos basados en copias redundantes, zonas de seguridad, etc. También pueden contratarse servicios externos. En este caso, los parámetros más importantes que se deben negociar son los siguientes:

- Intervalos de recogida de medios.
- Intervalo de entrega en caso de desastre.
- Mecanismos de manipulación de los medios.
- Seguridad del almacenamiento.
- Coste de todos los servicios anteriores.

5.2.3.3 Desarrollar protección de sistemas

Esta etapa tiene como objetivo poner los medios necesarios para sustituir los sistemas informáticos en el caso de un desastre. La protección de sistemas cubre tanto a los mainframes, miniordenadores como a los ordenadores personales. Es decir, la protección de sistemas pone los mecanismos necesarios para sustituir a los elementos hardware de la configuración.

En primer lugar, para desarrollar esta etapa, deben definirse las configuraciones mínimas necesarias para soportar las funciones productivas. La información para realizar esta tarea se basa en la clasificación de criticidad de las funciones productivas. Por lo tanto, la configuración mínima debe cubrir aquellas funciones denominadas críticas o vitales, para que puedan ser rápidamente recuperadas en caso de caída de los sistemas.

Existen cuatro estrategias básicas en la protección de sistemas que se pueden utilizar en el plan de recuperación:

- Hardware redundante. En este caso la organización adquiere las máquinas necesarias para sustituir a los sistemas de producción en el caso de desastre.

- "Cold site". Esta estrategia se basa en contratar los servicios de una compañía externa que asegura la disponibilidad de los equipos utilizados por la empresa en caso de desastre. Para poner en funcionamiento los servicios informáticos, la organización debe, simplemente, cargar su configuración software para reanudar su actividad productiva.

- "Hot site". Esta estrategia es similar a la anterior. La diferencia estriba en que, en este caso, la configuración software ya está disponible. De esta forma, la actividad puede reanudarse en un intervalo muy corto. La actividad incluso puede reanudarse inmediatamente si se ha desarrollado una estrategia de redireccionamiento de líneas de comunicación. La desventaja respecto a la estrategia anterior se basa en el mantenimiento de la configuración y en su mayor coste.

- Suministro de equipos. Esta opción consiste en la compra o alquiler de equipos a proveedores. Puede usarse cuando no existen restricciones de tiempo o cuando los equipos pueden ser suministrados muy rápidamente. En esencia es muy parecida a la primera opción,

la de hardware redundante, excepto por la falta de inversión inicial en equipos informáticos, y porque los equipos que se adquieran siempre serán de la última tecnología disponible.

5.2.3.4 Desarrollar protección de redes de telecomunicación

Esta etapa tiene como propósito definir medios para mantener las comunicaciones en el caso de un desastre. Incluye la previsión de hardware redundante, líneas de comunicación y documentación de la configuración de los servicios de telecomunicación.

Al igual que en el caso anterior, deben desarrollarse configuraciones mínimas que soporten el rendimiento necesario de líneas de telecomunicaciones, actividades de terminales, uso de comunicaciones de área extensa, etc.

Una forma típica de análisis se basa en la construcción de "escenarios" (scripts) Estos escenarios son situaciones hipotéticas que describen diversos tipos de incidencias que pueden afectar a las líneas de comunicaciones. Con la información del análisis de riesgo y la aportada por la construcción de los escenarios se prevén los elementos hardware redundantes necesarios, así como la necesidad de líneas de backup, etc.

5.2.4 Definir equipos de recuperación y escribir el plan

Una vez desarrollados los sistemas de prevención, y antes de escribir el plan de recuperación, la primera tarea es definir qué personas participarán en las labores de recuperación de los servicios informáticos tras un desastre. A continuación, se puede escribir y probar el plan de recuperación para su revisión y aprobación por la Dirección.

5.2.4.1 Definir equipos de recuperación

El objetivo de esta etapa es crear equipos de trabajo para soportar las estrategias que han sido desarrolladas para la recuperación del negocio. Lo que menos importa en este momento es asignar personas concretas a equipos basándose en sus conocimientos o experiencia, sino crear un marco de trabajo para el soporte de los procedimientos de recuperación.

Cada equipo de trabajo soporta una (o varias, si es posible) de las acciones contempladas en el plan de recuperación. Así, es normal que los equipos se definan en concordancia con las acciones previstas en el plan. Por ejemplo, si existe una estrategia de backup, un equipo debe ser capaz de soportar las acciones planteadas en dicha estrategia.

A continuación se proporciona una lista de los posibles equipos que pueden definirse en el marco de un plan de recuperación. Dependiendo de las estrategias de recuperación planteadas en una Organización concreta, se puede tomar esta lista como base para definir los equipos necesarios.

1. Equipo de emergencia.
2. Equipo de evaluación de daños.
3. Equipo de dirección.
4. Equipo de backup.
5. Equipo de software.

6. Equipo de aplicaciones.
7. Equipo de operación.
5. Equipo de recuperación de redes.
9. Equipo de comunicaciones.
10. Equipo de transporte.
11. Equipo de hardware.
12. Equipo de datos.
13. Equipo administrativo.
14. Equipo de suministros.

La lista presentada no pretende ser exhaustiva, ni adecuada a todas las organizaciones. Algunas organizaciones pueden asignar varias funciones a un determinado equipo, otros pueden desglosarlos más. Cada organización debe desarrollar los equipos que le parezcan más adecuados, según sus necesidades.

Un problema que aparece tras la definición de los equipos es la asignación de personal y el entrenamiento de éstos. Respecto al primer problema, el coordinador de recuperación debe analizar, posiblemente de forma conjunta con el departamento de recursos humanos de la empresa, cuáles son los candidatos más adecuados para cada equipo. En lo referente al segundo problema, el coordinador debe desarrollar, conjuntamente con los responsables de los distintos departamentos implicados, programas de entrenamiento en las labores de recuperación. Este entrenamiento debe prolongarse durante toda la vida del plan.

5.2.4.2 Escribir el plan

Una vez desarrollados los sistemas de prevención, y definidos los distintos equipos que participarán en las labores de recuperación, sólo falta escribir el plan. De forma usual, el plan de recuperación estará formado por un conjunto de procedimientos organizados a través de un "árbol de decisión" u organigrama. Un ejemplo de organigrama puede verse en la figura 5.7.

Escribir procedimientos es siempre una tarea complicada por dos factores; El primero es definir una serie de actividades que permitan desarrollar correctamente un trabajo. El segundo es expresarlo de forma que se entienda.

Hay que tener en cuenta que en el marco de un plan de recuperación, cuando haya que ejecutar los procedimientos, la situación para la organización será de desastre. Esto significa que el entorno donde se ejecutarán los procedimientos de recuperación va a ser caótico, lo que añadirá confusión a las acciones a realizar.

Todos estos factores deben estar previstos por el coordinador de recuperación en el momento de escribir el plan, y debe lograr que su efecto sea el menor posible.

De forma general, el plan de recuperación contiene tres partes:

- Proyecto de Evacuación. Se refiere a todas aquellas acciones destinadas a salvar los elementos de la configuración, usuarios, etc. de los efectos de un desastre. Comprende, además, aquellas acciones encaminadas a evaluar los daños e invocar formalmente el plan de recuperación.

- Proyecto de Recuperación. Comprende todas las acciones encaminadas a reiniciar, mediante los sistemas de prevención definidos con anterioridad, las actividades productivas.

- Proyecto de Reentrada. Se refiere a todas las acciones encaminadas a pasar a la organización, desde la situación de desastre, a la situación de actividad normal.

Estos tres "proyectos" proporcionan un marco conceptual para desarrollar los procedimientos de recuperación. Un esquema de plan, que cada Organización puede adaptar según su conveniencia, es el siguiente:

1. Acciones de emergencia. Procedimientos para reaccionar ante situaciones de crisis, desde sistemas de extinción hasta evacuaciones de emergencia.

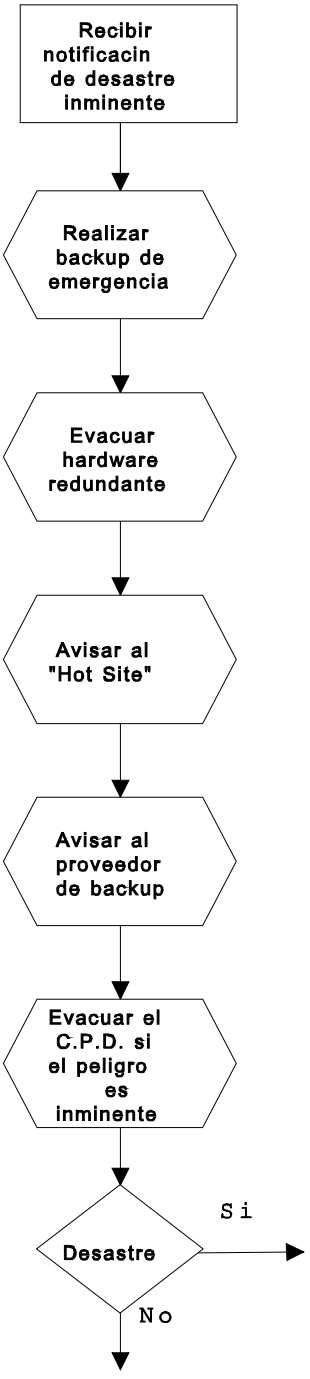


Fig. 5.7 Ejemplo de Organigrama

2. Notificación. Procedimientos para comunicar a la dirección la situación de desastre. Normalmente incluye una lista de direcciones y teléfonos de las personas implicadas en el plan de recuperación.

3. Declaración de desastre. Procedimientos de valoración de daños, criterios de invocación del plan de recuperación y procedimientos de declaración de situaciones de desastre.

4. Procedimientos de recuperación de sistemas. Procedimientos para recuperar la funcionalidad de los sistemas informáticos en un tiempo específico, de acuerdo con los objetivos marcados para el plan.

5. Procedimientos de recuperación de comunicaciones. Procedimientos para recuperar las comunicaciones de voz y datos.

6. Procedimientos de recuperación de funciones de usuario.

7. Procedimientos de protección de recursos. Procedimientos para salvaguardar los recursos informáticos y/o recuperar las configuraciones.

8. Procedimientos de reentrada. Procedimientos para recuperar los niveles normales de servicio.

Los puntos 1, 2 y 3 cubren el Proyecto de Evacuación. Los puntos 4, 5, 6 y 7 el Proyecto de Recuperación y, finalmente, el punto 8 cubre el Proyecto de Reentrada. Cada procedimiento debe ser desarrollado por un equipo de recuperación, debidamente coordinado por la Dirección.

5.2.4.3 Probar el plan

Una vez desarrollado el plan de recuperación, este debe ser probado para verificar si cumple con los objetivos planteados para su realización. El método normal de prueba es construir escenarios (scripts) donde se simule la existencia de un desastre.

Las pruebas pueden ser planificadas (con conocimiento de los recursos de la organización) o no planificadas. Estas últimas son más adecuadas para las pruebas periódicas, donde se comprueba el nivel de "sensibilidad" de los recursos humanos frente a la supervivencia de la empresa.

Los resultados de las pruebas deben ser documentados y comparados con los objetivos. Esta comparación definirá la concordancia del plan con los objetivos definidos y, por lo tanto, su viabilidad.

5.2.4.4 Aprobar el plan

Por último, la Dirección debe dar el visto bueno de modo formal al plan de recuperación. Este paso es importante, pues proporciona el respaldo de la Dirección a las acciones contempladas en el plan. No debería implantarse ningún plan de recuperación si no cumple esta formalidad.

5.2.5 Mantenimiento del plan

Una vez realizado el plan, éste debe mantenerse en el tiempo para que sea operativo. La razón es que los servicios informáticos están habitualmente en permanente cambio y esto hace que una previsión inicialmente buena sea inadecuada a corto plazo.

El mantenimiento del plan se lleva a cabo mediante dos acciones: el registro de cambios y las revisiones periódicas.

5.2.5.1 Registro de cambios

Esta tarea está encaminada a localizar y controlar los cambios que ocurren en todos los elementos de la configuración. Normalmente, el coordinador deberá identificar aquellos elementos sometidos a cambio. Entre estos podemos citar:

- Datos
- Aplicaciones
- Documentación
- Formularios
- Hardware
- Personal
- Etc.

y realizar un seguimiento de todos estos elementos. En la medida en que un cambio afecte a la estrategia del plan, este debe ser modificado para adaptarse a la nueva situación. Las modificaciones pueden afectar a todos los elementos del plan, ya sean las estrategias, los equipos, los procedimientos de prevención, etc., pudiendo generar un nuevo ciclo global de la metodología. Si en la Organización existe Control de Cambios, se seguirán las normas que allí se estipulen.

5.2.5.2 Revisiones periódicas

A medida que el plan se modifica, se deben realizar pruebas para comprobar que se cumplen los objetivos planteados. También es necesario mantener un ambiente de "recuperación" dentro de la organización. Esto se consigue realizando pruebas no planificadas que midan la sensibilidad de la organización a los procedimientos de recuperación de sus sistemas. Naturalmente, todos los resultados deben ser registrados para su análisis, ya que son importantes en la medida en que definen la adecuación del plan a los objetivos, y pueden sugerir cambios o mejoras en el propio plan de recuperación.

5.3 Resumen

Las actividades que se realizan en el contexto de la prevención y recuperación de la organización ante desastres forman un conjunto que va desde la definición de objetivos de recuperación hasta la definición de procedimientos y equipos de trabajo.

La metodología presentada pretende ser un marco general en que las organizaciones puedan definir su propia metodología de prevención y recuperación de desastres.

No obstante, algunos puntos no han sido presentados en toda su amplitud a lo largo de este tema. No se han incluido otras alternativas de seguridad, servicios existentes en el mercado, ejemplos de planes de recuperación, etc., por superar el ámbito planteado.

Queda a la discreción del lector el estudio de estas alternativas.

5.4 Anexos

En las páginas siguientes figuran las distintas Secciones de un Cuestionario de Recuperación de Sistemas, las cuales se muestran aquí como ejemplo, y un extracto de la conferencia sobre Seguridad Física en Centros de Proceso de Datos, impartida en la Facultad de Informática de La Coruña en Abril de 1.996 por Carlos Taboada Presedo, responsable de Seguridad Física del Centro de Proceso de Datos de Banco Pastor, y reproducida aquí con su permiso.

CUESTIONARIO DE RECUPERACION DE SISTEMAS

DEPARTAMENTO:

NOMBRE DEL DIRECTOR O SUPERVISOR:

EXTENSION:

FECHA:

SECCION I: TAREAS

INSTRUCCIONES:

Identificar las tareas/trabajos ejecutadas por su departamento que utilicen los servicios informáticos (incluidos los PC's). Añadir las páginas que sean necesarias para describir, brevemente, todas las tareas. Como ejemplo se describe la tarea ficticia 0.

TAREA 0

Introducir los datos de pedidos realizados por los clientes en el sistema de Pedidos.

TAREA 1

TAREA 2

TAREA 3

TAREA 4

TAREA 5

SECCION II: IDENTIFICAR LAS ENTRADAS Y SALIDAS DE LAS TAREAS

INSTRUCCIONES:

Para cada una de las tareas enumeradas en la sección anterior, indicar todos los formatos, documentos, informes y otras fuentes de información utilizadas para ejecutar una tarea. Después, enumerar las salidas obtenidas de la ejecución de la tarea: informes, actualizaciones de ficheros informáticos, documentos impresos, etc. Utilizar una página para cada una de las tareas.

EJEMPLO: La tarea 0, Introducir los datos de pedidos realizados por los clientes en el sistema de Pedidos, tiene las siguientes entradas y salidas.

ENTRADAS	SALIDAS
(Información y material necesario para ejecutar la tarea.)	(Resultados o productos tras la ejecución de la tarea.)
1. Código o nombre del artículo solicitado.	1. Actualización del fichero de pedidos.
2. Cantidad del producto.	
3. Acceso al sistema de Pedidos para crear el pedido.	2. Obtención de un albarán de pedido.

SECCION III: FRECUENCIA DE LA TAREA

INSTRUCCIONES: Indicar la frecuencia (diaria, semanal, mensual, etc.) de ejecución de cada una de las tareas enumeradas en la Sección I. Añadir las páginas que sean necesarias.

TAREAS	FRECUENCIA	COMENTARIOS
0	4 veces por día	Entrada media: 100 pedidos por sesión (400 por día)
1		
2		
3		
4		

SECCION IV: UTILIZACIÓN DEL SISTEMA

INSTRUCCIONES: Responder a las siguientes cuestiones:

1. Identificar el número y tipo de terminales de ordenador instalados en su departamento (por ejemplo, 23 IBM, 3 Data General, 10 AT&T, etc.)

---

2. ¿Los usuarios comparten los terminales? Si es así, ¿cuántos usuarios comparten un mismo terminal?

---

3. ¿Cuántos PC están instalados en su departamento?

---

4. ¿Qué software se utiliza en estos PC?

---

5. ¿Con qué frecuencia se realizan copias de seguridad de los datos de estos PC? (Por ejemplo, una vez al día, a la semana, al mes, etc.)

---

6. ¿Dónde se guardan los datos y software de los PC cuando no se utilizan?

---

7. ¿Las copias de seguridad se almacenan en habitaciones, archivadores con llave, en lugares a prueba de fuego o se guardan en las casas de los empleados o en almacenes externos especiales para esta función concreta?

---

5. Enumere todos los equipos periféricos instalados en su departamento, incluyendo impresoras, modems, dispositivos de cinta, discos externos, etc.

SECCION V: CRITICIDAD DEL SISTEMA

INSTRUCCIONES: En páginas separadas, responder a las siguientes cuestiones. Tener en cuenta las tareas enumeradas anteriormente.

1. Para cada tarea, identificar los costes en que incurriría su departamento si el sistema (o PC) utilizado para ejecutar cada tarea no estuviese disponible durante un período de 24 horas. Expresar los costes en pesetas, e identificar los parámetros utilizados en el cálculo. Repetir los cálculos para un período de 48 horas.

2. Para cada tarea, identificar cómo se efectuarían si el sistema (o PC) utilizado para ejecutarlas no estuviese disponible por un período prolongado de tiempo. Por ejemplo, ¿podría ejecutar un procedimiento manual para efectuar la tarea? Indique si NO puede ejecutar una tarea sin acceder al sistema (o PC) normalmente utilizado. Asimismo, si el método o procedimiento manual sólo se puede utilizar por un breve período de tiempo, notifíquelo, por favor.

SECCION VI: COMUNICACIONES

INSTRUCCIONES: Responda a las siguientes cuestiones relacionadas con las tareas identificadas anteriormente.

1. ¿Alguna de las tareas indicadas anteriormente requiere la utilización de teléfonos, FAX o terminales de comunicación de datos? En caso afirmativo, por favor especifique qué tareas utilizan los dispositivos de comunicación y cuáles son estos dispositivos.

2. ¿Cuántos dispositivos de telecomunicación (incluyendo teléfonos, FAX, terminales de comunicación de datos) están instalados en su departamento?

3. Para cada tarea, identificar el impacto, respecto a la ejecución total de la tarea, si no se pudiesen disponer los servicios de telecomunicación durante 24 horas. Si es posible, estimar los costes en pesetas en que incurrirá su departamento si se produce esta situación. Explicar los cálculos realizados para obtener estos costes.

SECCION VII: OPERACIONES DE EMERGENCIA

INSTRUCCIONES: Responda a las siguientes cuestiones teniendo en cuenta las tareas y procedimientos identificados en la sección V.

1. Para cada tarea, indicar el número mínimo de personal necesario para obtener un nivel aceptable de rendimiento del trabajo si se produjese una caída del Sistema. Explicar la respuesta.

2. Para cada tarea, identificar el número mínimo de recursos de ordenadores y telecomunicación necesarios para obtener un nivel aceptable de rendimiento del trabajo ante una emergencia. (Indicar número de terminales, PC, teléfonos, FAX, terminales de comunicaciones de datos, etc.).

SECCION VIII: CONSIDERACIONES GENERALES

INSTRUCCIONES: Las siguientes cuestiones intentan reflejar la importancia de determinados parámetros ante una situación de emergencia. Por favor, responda a las cuestiones detalladamente.

1. Para cada tarea, identificar el impacto en el rendimiento de la tarea si, en situación de emergencia, se dispusiese de una fotocopiadora. Indicar si la fotocopiadora sería necesaria, deseable o no necesaria.

2. Para cada tarea, identificar el impacto en el rendimiento de la tarea si se utilizase correo ordinario en situación de emergencia. Aplicar los mismos criterios que en el apartado anterior.

3. Para cada tarea, identificar el impacto de redireccionar las llamadas telefónicas a la nueva localización. Si son necesarias las llamadas telefónicas para la ejecución correcta de la tarea, la respuesta será "Es importante". Si las llamadas telefónicas no influyen en la ejecución de la tarea, la respuesta será "No es importante".

4. ¿Se mantiene en su departamento un listín telefónico de sus directivos (teléfono del domicilio y de emergencia)? ¿Existe una copia de este listín guardada fuera de la compañía, en almacén externo especial o en el domicilio del supervisor?

5. ¿Cuál es el horario normal de trabajo en su departamento? ¿Existen turnos u horarios de fin de semana?

SEGURIDAD FISICA EN CENTROS DE PROCESO DE DATOS

" ... En la actualidad, la necesidad de seguridad en un Centro de Proceso de Datos es tan evidente que prácticamente no es necesario justificarla. No obstante, si fuera necesario bastaría con pensar en la pérdida de imagen, y lo que es más importante, la pérdida del volumen de negocio que experimenta una organización financiera después de sufrir un daño importante en su sistema de proceso de datos.

Prueba de ello es la utilización, cada vez mas generalizada, de Centros de Backup para el almacenamiento de los datos en una ubicación distinta de su lugar de origen. Esto implica la labor de duplicar cintas y discos para transportarlos a otro local debidamente acondicionado para recibirlos, que incorpore medidas antisísmicas, cámaras acorazadas e ignífugas, etc., y abordar el traslado como si se tratase de dinero, contratando a empresas de seguridad para realizarlo, y encriptando los datos para evitar su utilización por personas no autorizadas. Dado el alto coste de utilización de estos Centros de Backup, la solución cada vez más común en nuestros días es compartirlos por diferentes entidades.

Los Centros de Proceso de Datos se encuentran expuestos a una gran variedad de peligros, que es conveniente conocer para ser capaz de prevenirlos y de contrarrestar los problemas que ocasionan. Pasaremos revista ahora de los mas relevantes, indicando las medidas de prevención y recuperación que se pueden aplicar en cada caso.

Se puede hacer una primera clasificación de los "enemigos" de un CPD separando los que podríamos considerar enemigos naturales, incendios, seismos, inundaciones, etc., de los enemigos técnicos, entre los que se pueden destacar los fallos en el suministro eléctrico y la electricidad estática entre otros.

Uno de los "enemigos naturales" más importantes para un CPD lo constituye el incendio. Frente a este enemigo, lo principal es detectarlo, ya que la prevención es pasiva y depende del tipo de construcción del CPD. Precisamente las características de un CPD (falso suelo, con gran cantidades de cables, aire acondicionado funcionando constantemente y que puede avivar las llamas, etc.) pueden facilitar el inicio de un incendio.

Además, hay que tener en cuenta que los productos utilizados en la construcción, como por ejemplo el PVC, son normalmente venenosos e inflamables. Los cables eléctricos contienen cianhídricos y al arder producen cianuros, las moquetas y pinturas contienen contaminantes, etc. Por lo tanto, una detección rápida de un incendio es primordial.

Por eso, mas que evitar un incendio, que siempre es por supuesto deseable pero no siempre es posible, lo más importante es detectarlo a tiempo. Para ello se dispone de una serie de medidas, como pueden ser los analizadores / detectores de humo, que detectan partículas de humo en el aire, los detectores de incendio, normalmente colocados en los techos y conectados a un sistema de extinción por agua pulverizada (aunque ésta es dañina para los ordenadores) y a las correspondientes alarmas, cámaras de televisión situadas en puntos estratégicos para vigilancia, etc.

Ante un incendio, una de las primeras labores a realizar es la detención del sistema de aire acondicionado para evitar la facilitación de la combustión, y, por supuesto, el desalojo del personal para evitar la contaminación por inhalación de gases.

Una vez detectado un incendio hay que proceder a su extinción. Para ello se pueden utilizar descargas de CO_2 (aunque este método es muy peligroso por ser un gas mortal si se inhala), uso de agua presurizada, que como ya se ha comentado es perjudicial para los equipos, extintores manuales, etc. Otra posibilidad para la extinción consiste en descargas de Halón, un gas ávido del oxígeno y que en la actualidad está prohibido fabricar por dañar seriamente la capa de ozono y que por tanto las existencias actuales tienen un precio muy elevado, del orden de 15.000 pesetas el kilo. Existe un producto similar al Halón y un poco menos problemático que éste, denominado NAF, y que el Protocolo de Montreal admite su utilización hasta el año 2010.

Como se puede ver, la extinción de un incendio implica tomar medidas problemáticas y potencialmente perjudiciales para las personas, por lo que es imprescindible disponer de un Plan de Emergencia y Evacuación para ser utilizado en estos casos.

Otro de los enemigos naturales, aunque más raro en nuestro país, lo constituyen los seismos y terremotos. No obstante, y aunque en España no suelen producirse terremotos capaces de destruir un edificio, hay que tener en cuenta que los movimientos ocasionados, aunque pequeños, pueden afectar al funcionamiento de los discos de la instalación, ocasionando pérdidas de datos, y en ocasiones el “aterrizaje” de las cabezas de lectura / escritura, dañando definitivamente el dispositivo. La única prevención posible en este caso es disponer de una copia de seguridad de los datos y hardware redundante que realice la función de los discos averiados.

Consideremos ahora las inundaciones. Los daños ocasionados por el agua no pueden considerarse como graves, aunque obligan a parar los equipos y esperar hasta que se sequen. Para detectar las inundaciones se dispone de sensores de agua, colocados en el suelo y en el falso suelo, flotadores y capacitivos eléctricos, entre otros.

El siguiente enemigo natural de un CPD lo constituyen los rayos. Aunque no se produzca una caída directa de un rayo (que probablemente ocasionaría un incendio), la fuerte carga eléctrica puede causar la desconexión de interruptores

diferenciales que podrían causar paros en los sistemas. Una medida de prevención la constituyen, lógicamente, los pararrayos.

Por desgracia podríamos incluir también en este grupo de enemigos naturales los atentados y actos terroristas. Ante este tipo de "enemigos" solo caben medidas de prevención, de las que, por fortuna, se dispone de bastantes. Podemos citar, entre otras, los controles de mercancías con detectores de metales, para la detección de bombas o artefactos explosivos, las mantas antiexplosivas, las puertas con sensores y alarmas conectadas a una sala de seguridad, cámaras de televisión, vigilantes, sensores de intrusismo (radar), el control de los ascensores, para saber su ubicación exacta en cada momento, timbres de alarma general, control del personal y de visitantes en la entrada (se dispone de "chips" de solapa que permiten saber la situación del visitante en cualquier momento), teléfono directo con la policía, etc., etc.

Un punto clave a proteger dentro de un CPD es la sala de ordenadores. Para ello, además de poseer unas características de construcción que la hagan especialmente fuerte (puertas y cristales blindados, paredes reforzadas, etc.), lo mas usual es permitir el acceso sólo al personal autorizado, reduciendo éste al mínimo indispensable. Para ello se utilizan controles de acceso con tarjeta magnética, controles de huella digital combinados con el uso de palabras de paso, control de huella facial y scan de retina en las instalaciones mas sofisticadas. Estas medidas van encaminadas no sólo a prevenir un atentado sino a evitar accidentes causados por personas que, por negligencia o desconocimiento, puedan ocasionar pérdidas de datos o daños en los equipos informáticos.

El último de los enemigos naturales, pero no por ello el menos problemático, lo constituyen las ratas y ratones. Estos roedores normalmente anidan al calor producido por los cables y además suelen comerlos en ocasiones, causando no pocos problemas en instalaciones del tipo de un CPD. Las medidas de prevención consisten básicamente en el uso de cebos y de ultrasonidos, aunque éstos últimos pueden ocasionar interferencias en los equipos sensibles a ellos. Y, aunque pueda parecer raro, se ha dado el caso de un gato que ocasionó un cortocircuito en un transformador, provocando una caída de tensión y una avería de varias horas.

El otro grupo de enemigos lo hemos definido como "enemigos técnicos". Entre ellos, el mas importante a destacar lo constituyen, paradójicamente, las empresas de suministro eléctrico. Es habitual que se produzcan microcortes en el suministro e incluso cortes de gran duración, normalmente ocasionados por averías en la red eléctrica. Como los ordenadores soportan mal estos cortes (un disco duro está girando a muchas revoluciones y un corte puede ocasionar graves fallos en sus mecanismos), lo que se debe de hacer es evitarlos. Para ello se dispone en el mercado de Sistemas de Alimentación Ininterrumpida (formados por un rectificador mas un ondulador y una serie de baterías en la parte de corriente continua) que, unidos a un grupo electrógeno normalmente preparado para arrancar a los dos o tres minutos del corte, permiten la disponibilidad continuada de energía eléctrica.

Otro de los enemigos técnicos lo pueden constituir el calor y la humedad. Los ordenadores necesitan, para su correcto funcionamiento, una temperatura y una humedad controladas y estables, normalmente 20º centígrados y un 60% de humedad relativa. Para conseguirlo, se debe de disponer de un buen sistema de aire acondicionado que permita mantener estas características de humedad y temperatura. Es conveniente notar que los efectos de un sobrecalentamiento no se manifiestan de inmediato en los equipos informáticos, sino que producen una fatiga del material que ocasiona problemas a la larga.

Podemos considerar también dentro de este grupo la electricidad estática, presente habitualmente en las salas de impresoras o de otros equipos que la produzcan. Para evitarla es aconsejable disponer de una buena toma de tierra o de equipos especializados que la eliminan.

Debemos de incluir aquí también las sobretensiones transitorias, normalmente producidas por conexiones y desconexiones en la red de alta tensión, que pueden originar picos del orden de miles de voltios que son altamente perjudiciales para los equipos. Normalmente, los Sistemas de Alimentación Ininterrumpida ya incorporan filtros especiales de tiristores para eliminar estos picos.

Otro de los enemigos técnicos lo constituye el polvo, altamente perjudicial para los equipos electrónicos. Entre las medidas para evitarlo están las pinturas especiales antipolvo y una buena limpieza anual del falso suelo y del falso techo.

Por último, podemos considerar como un peligro potencial el fallo de los sistemas de mantenimiento, como pueden ser los enfriadores de agua, formados por compresores, bombas y tuberías, normalmente ubicadas en el falso suelo, y que pueden originar inundaciones o causar averías en otros sistemas. Además, su parada suele ser crítica en los ordenadores enfriados por agua.

Hemos revisado hasta aquí una serie de peligros potenciales de los sistemas informáticos, pero no debemos de concluir sin tener en cuenta una consideración final. Es posible disponer de todas las medidas de prevención imaginables y de todos los sistemas de recuperación posibles, pero no debemos de olvidar que, aunque los sistemas de seguridad sean los correctos y funcionen adecuadamente, éstos están manejados y supervisados por personas, que pueden asimismo fallar en cualquier momento, por lo que es tan importante prestar atención tanto a los unos como a los otros para disponer realmente de un CPD a prueba de fallos.

Y considerar a partir de ahora que no sólo los ordenadores son importantes, sino que el conjunto de servicios auxiliares que los soportan y las personas que los mantienen operativos son, al menos, igualmente importantes...”

5.5 Bibliografía

[Aasgaard, 79] D.O. Aasgaard, et al. *An Evaluation of Data Processing "Machine Room" Loss and Selected Recovery Strategies*. Minneapolis; MISRC, University of Minessota. 1979.

[Browne, 84] Peter S. Browne. Survey of Risk Assestment Methodologies. *Data Security Management*. New York. Auerbach Publishers. 1984.

[Rowe, 77] W. D. Rowe. *Anatomy of a Risk*. New York. John Wiley and Sons. 1979.

[Toigo, 89] Jon William Toigo. *Disaster Recovery Planning. Managing Risk and Catastrophe in Information Systems*. Prentice Hall. 1989.

[USDC, 79] U.S. Department of Commerce, National Bureau of Standards. *Guidelines for Automatic Data Processing Risk Analysis*. FIPS PUB 65, Washington DC. June, 1979.

[USDC, 84] U.S. Department of Commerce, National Bureau of Standards. *Guidelines of Automatic Data Processing Physical Security and Risk Management*. FIPS PUB 31, Washington DC. June, 1984.