UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FES ARAGÓN

TÉCNICAS PARA LA PLANEACIÓN DE RECUPERACIÓN DE DESASTRES PARA SISTEMAS INFORMÁTICOS Y REDES DE CÓMPUTO

TESIS
QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN
PRESENTA
MARIO LUIS OLIVOS ROJAS

DIRECTOR DE TESIS:
ENRIQUE GARCÍA GUZMÁN

MÉXICO D.F. 2006

TÉCNICAS PARA LA PLANEACIÓN DE RECUPERACIÓN DE DESASTRES PARA SISTEMAS INFORMÁTICOS Y REDES DE CÓMPUTO

RESUMEN

Lo que se espera es justificar los gastos para conducir de una manera formal el análisis de riesgos y así identificar el nivel actual de preparación de la compañía, y sus riesgos específicos. De esta forma se pueden desarrollar sugerencias para realizar un plan que proveerá seguridad a los empleados y dará continuación a los negocios en el momento de un desastre.

Las empresas financieras son las menos tolerantes a las interrupciones, sólo unas 48 horas, antes de que las pérdidas de las funciones de negocios se vuelvan irrecuperables. Las industrias encargadas de distribución pueden mantener sus operaciones hasta 72 horas, mientras que en las industrias de manufactura, compañías aseguradoras, y otras pueden sobrevivir hasta 6 días después de la interrupción. Ésta información representa un porcentaje basado en estimaciones hechas por inspectores del tema. Los encargados de las funciones de negocios pueden ayudar para obtener mayor información para poder calcular el tiempo estimado de interrupción para la empresa

Según los expertos, 72 horas son consideradas ideales para el tiempo de recuperación. Algunos negocios pueden soportar interrupciones más prolongadas, mientras que otras deben realizar los cálculos completos de las pérdidas financieras en el menor tiempo posible. El marco de tiempo para la recuperación que se presentará a la gerencia debe corresponder a los requerimientos de la compañía y no a las 72 horas recomendadas por expertos.

Las grabaciones críticas son aquellas que son requeridas para la recuperación y que sin ellas la recuperación sería imposible. Para los requerimientos legales y auditorias, se recomienda cierto tipo de grabaciones (reportes administrativos, datos de contabilidad, contratos, los libros de la compañía), también deben ser protegidos de una pérdida. También, documentos de propiedad, código fuente del software, patentes en trámite de la compañía, etc. representan una inversión de tiempo y recursos de la empresa, por lo tanto ésos documentos ameritan ser protegidos. Éstos datos también son críticos, aunque no se requieran para mantener las operaciones diarias de la empresa.

El caso más claro en la PLRD reside en una evaluación de riesgo del desastre y los correspondientes potenciales de pérdidas para la compañía. Se debe hacer notar que es difícil o imposible establecer una estadística confiable para saber la probabilidad de que exista un desastre que afecte a una empresa.

Las estrategias de recuperación de sistemas vienen en todas las variedades de gastos y complejidad. La estrategia apropiada para cualquier empresa, es la estrategia que dará la restauración de las funciones mínimas aceptables, periodos de tiempo, y costos.

Se debe tener en cuenta que las estrategias de recuperación de sistemas no son como recetas de cocina. Están inexorablemente relacionadas al usuario final, y a estrategias de recuperación de redes que deben ser revisadas siempre que ésta u otras estrategias, sean armadas completamente.

Las empresas localizadas en pequeñas ciudades que carecen de instalaciones comerciales con éstos servicios, deben hacer acuerdos cooperativos con otras empresas.

Una PLRD no tiene como objetivo recuperar todo en su forma original, en vez de éso, se busca mantener una organización eficiente y temporal diseñada para mantener los requerimientos necesarios hasta que la crisis termine. El objetivo principal es recuperar las configuraciones mínimas tanto de redes como de sistemas que darán soporte a los requerimientos específicos para funciones de negocios que han sido identificados como críticos y vitales.

Las aplicaciones del software deben ser legibles independientemente de las diferentes plataformas que se tengan para facilitar la comunicación entre las aplicaciones, nuevos dispositivos y diferentes tipos de terminales.

Los archivos de información deben estar en un formato compatible con el sistema de operación de destino.

Aunque esto es más complejo de lo que parece, todo esto debe ser examinado meticulosamente y es una tarea más en el esfuerzo para reunir la información.

TÉCNICAS PARA LA PLANEACIÓN DE RECUPERACIÓN DE DESASTRES PARA SISTEMAS INFORMÁTICOS Y REDES DE CÓMPUTO.

I. INTRODUCCIÓN

1.1 Definición de Desastre.

Un desastre es definido como la interrupción, en una misión crítica importante de los servicios de información, y por un período de tiempo prolongado inaceptable.

El desastre es caracterizado por una interrupción de los procesos con los cuales la información de la empresa o negocio es producida, procesada y/o distribuida.

La naturaleza de un desastre es relativa y contextual. Lo que constituye un desastre para cierta empresa no significaría un desastre para alguna otra.

Ejemplos:

Para una pequeña empresa, se consideraría como un desastre, la falla del disco duro de la computadora encargada de administrar la contabilidad.

Para el caso de una empresa mayor, se consideraría como un desastre a la pérdida del procesamiento de datos debido a un incendio, terremoto o huracán.

Por lo tanto, sería un desastre, si el evento provoca la interrupción de los servicios de información en una misión crítica a una empresa.

Un corte de energía de muchas horas afectaría por mucho la capacidad de procesar la información de la compañía sin una planta de electricidad de emergencia, pero con un esfuerzo en el trabajo y algo de gastos, la compañía debe ser capaz de absorber el evento sin tener muchos daños. De cualquier forma, un corte en la energía eléctrica de varios días, debido al corte de un cable o a un cataclismo, por ejemplo; no serían tan fáciles de tolerar y tendrían consecuencias desastrosas.

Lo que constituye "un período de tiempo inaceptable" de interrupción de los servicios de información es algo relativo. Está basado simplemente en un efecto de tolerancia-costos. En un problema de corte de electricidad, entre más dilate el corte, los costos de la compañía aumentan, y la tolerancia de la compañía empieza a decrecer.

Pero, ¿cómo se determina lo que en realidad constituye un desastre para una empresa?

Hay muchos factores por considerar y muchas formas de interpretar y presentar la información, pero éste es un cálculo que es muy específico para cada compañía. Al final, cada encargado de la PLRD (Planeación y Recuperación en Caso de Desastre) debe tener su propia conclusión acerca de la tolerancia de su compañía en caso de tener una interrupción de los servicios de información.

Límites de la Planeación de Recuperación de Desastres.

Los planes para la recuperación en desastres no son perfectos. Aún con pruebas constantes, los planes siempre tienen errores que solamente se descubren en un desastre. Lo bueno es que, la PLRD proporciona la mayoría de la logística requerida para recuperarse de una interrupción. Se deben hacer pruebas de manera regular y entrenar al equipo que participará en el plan con la mentalidad de que ayudarán, para manejar y controlar la realidad de un desastre. Aún así, los planes de acción de emergencia y procedimientos de recuperación son guías y no modelos, que están sujetos a cambiar con el tiempo, basados en las consecuencias actuales de un desastre.

1.2 Importancia de la protección y seguridad al material de trabajo en una red/sistema de cómputo: (Información) y de la Calidad-Grado de Servicio para los clientes y usuarios.

Una de las razones más importantes para tener un Plan de Recuperación de Desastres es, que aquellas compañías con un plan, tienen mayor posibilidad de recuperarse que aquellas que no lo tienen. Se han hecho estudios que demuestran que las compañías que sobreviven a desastres atribuyen su éxito a la implementación de estrategias planeadas con anticipación por personal que ha sido entrenado y preparado en sus puestos de recuperación.

Beneficios.

Las razones para una PLRD deben incluir ética para contratos, recomendaciones de auditores, y órdenes legales.

Las empresas con PLRD previamente probadas tienden a sobrevivir sin problemas, contrario a las que no las tienen probadas.

Beneficios adicionales:

1. Reducciones en los costos de seguros para los negocios.

Esto se logra de dos maneras. Primero el desarrollo del análisis de riesgo formal en la PLRD puede afinar las coberturas, compradas a una compañía aseguradora de interrupciones de negocios. Frecuentemente, con la ausencia de una evaluación formal de los riesgos, la identificación de riesgos asegurables es llevada en términos totales, resultando en la adquisición de coberturas inapropiadas o demasiado caras. Debido a esto, la PLRD nos da la información más detallada para mejorar los objetivos de aseguramiento de negocios y por medio de esto reducir los costos agregados del seguro.

Otra forma en la que la PLRD puede ayudar en la reducción de costos es a través de enfatizar la prevención de desastres; identificando los riesgos e instalando sistemas de supresión y detección (sistemas como extinguidores, sistemas de detección de agua, etc.) para manejarlos, la PLRD puede dar las pruebas que se tienen de las capacidades de prevención de desastres. Así, éstas capacidades deben dar las suficientes razones para convencer a los aseguradores y hacer que reduzcan sus precios.

2. Usos alternos de las instalaciones para recuperación de desastres. En algunos casos, los equipos e instalaciones obtenidos para facilitar la recuperación en desastres debe ser aprovechada para dar capacitación al personal u otros propósitos. También, ciertos sistemas para evitar desastres, tales como reguladores de electricidad, o plantas de emergencia para energía eléctrica, dan servicios que mejorarán el rendimiento de sistemas protegidos durante su uso normal, etc.

3. Promoción de una cultura asertiva de la empresa.

A una compañía que retoma la PLRD, le puede ayudar ésta actividad de diferentes maneras. Las áreas de mercadotecnia pueden enfatizar la atención de la compañía para la planeación de contingencias como una demostración de compromiso de su disponibilidad de servicio. Los encargados de la planeación deben hablar en convenciones, conferencias o en los medios acerca de los méritos de la PLRD, promoviendo a la compañía como a una líder del campo. Parte de la PLRD debe incluir (si es posible) el establecimiento de un refugio de emergencia comunitario (albergue) en los edificios de la compañía, que sería una plataforma excelente para demostrar y dar publicidad con el valor que la compañía ofrece a la ciudadanía. Esto también significa una manera válida y benéfica para diseminar la información acerca de la PLRD e influenciar a otras compañías a hacer lo mismo.

1.3 Justificación.

La justificación para retomar la PLRD se deriva de la información previamente resumida. A éste punto, el encargado de la planeación solamente puede retomar los siguientes hechos:

1. Los riesgos a los cuales la compañía está expuesta.

2. Los riesgos de la industria, promedian "x" pérdida de dinero y los costos del desastre se incrementarán mientras la interrupción continúe.

3. La empresa mantiene cierta cantidad de dinero perdido de acuerdo a una cantidad "x" correspondiente a la duración de la interrupción, pero la recuperación se debe a la PLRD.

4. Además de los factores de los negocios que ayudan a la PLRD, debe haber requerimientos legales o regulatorios que den soporte y retomen el plan.

Lo que se espera es justificar los gastos para conducir de una manera formal el análisis de riesgos y así identificar el nivel actual de preparación de la compañía, y sus riesgos específicos. De esta forma se pueden desarrollar sugerencias para realizar un plan que proveerá seguridad a los empleados y dará continuación a los negocios en el momento de un desastre.

Juntar y organizar la información.

La información obtenida en la PLRD tiene los siguientes propósitos:

- Es la base para estimar las pérdidas potenciales, para justificar y explicar la PLRD a los directivos de la empresa.-
- Se usa para identificar las aplicaciones y los productos que se utilizarán y deberán comprarse para la prevención de un desastre.
- Encontraremos una definición clara de la información que se necesita y los requerimientos de almacenamiento de información.
- Ayuda a organizar los objetivos y parámetros en estrategias que serán desarrolladas para recuperar las funciones de los negocios en el momento del desastre.

1.4 Servicios afectados en una situación de desastre.

El plan de recuperación por sí mismo provee cierto apoyo para una recuperación que podría ser difícil de levantarse en el momento en que ocurra el desastre. Estas estrategias deben incluir pre-arreglos para un sitio de procesamiento de datos alterno, redireccionar el tráfico de comunicaciones de datos, para la energía eléctrica, tener áreas de trabajo alternas y para recuperar bases de datos desde respaldos.

Más aún, un plan de entrenamiento y pruebas a aquellos individuos que jugarán un papel en la implementación del plan para confrontar la posibilidad de un desastre y así estar mejor preparados para responder correctamente al caos que viene regularmente con el problema.

La efectividad de la Planeación de Recuperación de Desastres (PLRD), debe ser medida tomando como referencia otros desastres que han sido minimizados o eliminados.

Para el caso de las redes, pueden ser interrumpidas debido a fallas en los equipos, cortes de línea, incendios en las compañías telefónicas, fallas en los gateways, fallas en las comunicaciones y conmutadores, por nombrar algunas.

Posibles interrupciones:

1. Falla en la compañía que provee los servicios de PBX.

2. Cortes de línea o enlaces de la compañía telefónica.
3. Daño al proveedor de la red de área amplia.
4. Interrupción de los gateways.

Lista de los puntos más comunes para tomar en cuenta en una situación de desastre.

- Evaluar la seguridad.

Lo primero a realizar es una evaluación de la situación de la compañía con respecto a la seguridad. Las grandes compañías tendrán un experto en seguridad o por lo menos algún contrato con alguna compañía de seguridad.

Para salvaguardar todos los aspectos de las operaciones de negocios, por ejemplo:
/

Seguridad Física
Seguridad en Redes
Redundancia
Comunicaciones
Habilidad para continuar operando. (Disponibilidad).

- El personal.

Para este aspecto, será necesario saber si el departamento de recursos humanos por ejemplo, investiga al personal recién contratado por si tienen antecedentes penales. Se debe hacer un esfuerzo por conocer en lo mayor posible a los compañeros de trabajo. Muy importante también, es que se debe saber cómo contactar a los empleados y sus respectivas familias en caso de alguna emergencia para saber si se encuentran bien.

- Acceso a las instalaciones.

Se debe saber quién es el que tiene acceso a ciertos servicios y quién no. Se debe asegurar que los servicios de información crítica sólo sean disponibles para el personal autorizado. El personal debe usar identificación para ingresar a la compañía. Para el caso de que algún empleado sea despedido de la compañía se le debe recoger su identificación para evitar sabotajes. En caso de tener visitas, estas deben ser acompañadas por alguien de la compañía.

- Las computadoras.

Se deben actualizar los antivirus constantemente, las contraseñas de acceso deben cambiarse regularmente.

Instalación de alarmas de seguridad para detección de intrusos, parches y actualizaciones del sistema operativo, firewalls para las redes.

- Reservas.

Revisar el inventario de accesorios, refacciones, y ver si se tienen materiales como, cable, fibra óptica, conectores, fuentes de poder, baterías, servidores, antenas de transmisión, etc.

- Planta de energía eléctrica.

Como bien se sabe los apagones suelen ser muy comunes, por ello es necesario tener una planta de energía alterna en buenas condiciones para seguirles suministrando energía y en general a las partes críticas de la compañía, todo esto para asegurar la disponibilidad sin caídas de servicios. Sería conveniente, por ejemplo, realizar simulacros para ver si realmente está trabajando la planta de energía, simulando un apagón de energía eléctrica.

- Redundancia.

Es de gran importancia que los datos con información crítica y los equipos principales sean protegidos, además de revisar el estado actual de las redes que se utilizan en la compañía,

es necesario revisar los servicios contratados a otras compañías como por ejemplo el servicio de internet vía cable módem, etc.

Un detalle importante en la redundancia es que ésta no sólo es útil en un caso de emergencia; por ejemplo, si se necesita una pieza de hardware para operaciones críticas de negocios y que además, sería muy difícil encontrar un reemplazo de la misma en una emergencia, es necesario entonces adquirir otra pieza igual que nos serviría tanto como refacción o como un aparato de entrenamiento, lo cual justificaría por mucho el gasto que esto implicaría.

Desde luego la lista continúa, pero esto es lo principal a proteger, que de cierta forma es muy vulnerable.

Planeación Efectiva.

Para llevar a cabo lo anterior se recomienda tener un punto de vista pragmático, lo cual significa imaginar el peor de los casos. Un plan diseñado para el peor de los casos facilita las cosas cuando hay que enfrentarse ante una situación menos devastadora.

Por lo tanto en una PLRD se debe tomar en cuenta lo siguiente:

Se deben desarrollar procedimientos para evacuar al personal en situaciones inseguras, como en casos de temblores, incendios, etc., para recuperar las áreas de trabajo, sistemas, redes, para salvaguardar registros e información vital, para restaurar instalaciones afectadas o instalar otras y equiparlas.

Estos procedimientos pueden aplicarse totalmente o en partes según sea la magnitud del desastre. Por ejemplo, si un incendio daña el centro de información de la compañía, pero deja intactas las áreas de usuarios, y la red de datos o de voz, la PLRD sería implementada sólo en la parte del sistema de operaciones de información crítica. De igual forma, si la oficina de servicio de una compañía telefónica local fuera golpeada por un desastre, pero las otras instalaciones quedaran intactas, solo la parte correspondiente sería activada.

Un plan diseñado de ésta manera es administrable y efectivo. Además su diseño por partes es más eficiente. Personal encargado de la PLRD puede ser asignado en algunas partes del plan, para aprender, probar, y mantener acorde al puesto al que se espera que trabajen en un caso de emergencia. Más aún, cuando una interrupción ocurra, secciones del plan deben ser distribuidos a los líderes de equipo de la PLRD, en vez de, reproducir muchas copias de todo el documento.

1.5 Clasificación de amenazas de desastres.

- Desastres naturales contra desastres provocados por el hombre.

Ésta clasificación puede ser un poco confusa para hacer aclaraciones, por ejemplo: Si una inundación ocurre en una oficina del edificio debido a las fuertes lluvias o a un colapso del techo, es un caso de desastre natural (lluvia) o provocado por el hombre (una construcción defectuosa del techo.)

- Desastres de acuerdo a la geografía.

Si un edificio de la compañía se incendia, éste se consideraría como desastre local, y si este fuego es parte de una gran conflagración que consuma muchos edificios (por ejemplo, terremoto, erupción volcánica o tumulto), se consideraría como regional.

- Causa de un desastre.

Este esquema busca clasificar a los desastres por sus causas. En el caso anterior en donde se vieron los desastres naturales contra los hechos por el hombre, la causa del desastre no se puede clasificar de manera precisa. Por ejemplo, si un incendio daña el centro de operaciones, la causa exacta podría requerir más información acerca de los orígenes del incendio para propósitos de clasificación. ¿Acaso el fuego fue premeditado, alguna falla en el equipo, combustión espontánea, o alguna otra causa? Para hacer la clasificación, la causa debe ser identificada.

Dados los anteriores inconvenientes, existe un manera más efectiva para llevar a cabo una clasificación precisa y es la de clasificar los desastres por sus efectos.

Clasificación por efectos.

Los efectos de cualquier desastre provocan dos distintos casos: ó todas las funciones de negocios son interrumpidas o solamente algunas de las funciones de negocios son interrumpidas. También hay que considerar la duración de la interrupción (por cuánto tiempo la compañía será afectada en los servicios o recursos que requieren los negocios); esto es lo que califica al evento como un desastre.

La causa del desastre es solamente importante para aclaraciones con algunas compañías de seguros y también para el desarrollo de un programa de prevención.

Aún así, dos escenarios son lo único que se necesita considerar para la PLRD: pérdida total o pérdida parcial. El escenario de una pérdida total involucra una interrupción que afecta todo (o la mayoría) de las funciones de negocios críticas y vitales de los recursos que se requieren. Por lo tanto, una falla en la compañía telefónica que ofrece el servicio a la compañía que interrumpa el tráfico de las comunicaciones tanto de entrada como de salida debe ser considerada como un evento de pérdida total, a pesar del hecho de que los recursos e instalaciones de la compañía queden intactas. Lo mismo se debe decir para un incendio que provoque que el edificio de la compañía quede inhabitable.

El escenario de una pérdida parcial indica que solo algunas funciones de negocios críticas han sido interrumpidas, mientras unas queden intactas. El colapso del techo en un área de la compañía donde una computadora importante esté localizada, interrumpirá las operaciones de las unidades de trabajo que dependan de éste recurso de automatización. El impacto en este caso es desastroso en el sentido de las funciones de negocios críticas, aún así, la respuesta requerida para recuperarse de éste desastre podría ser menos extensa, en comparación con la respuesta requerida para un escenario con pérdidas totales.

El esquema del efecto parcial contra el de pérdida total en el diseño del plan se debe hacer por medio de módulos. Los objetivos de la recuperación, en funciones de negocios, deben hacerse con módulos del plan. De ésta forma, todo el plan o cualquiera de sus partes puede ser activada, dependiendo de la naturaleza y tiempo de la interrupción. Trabajar por módulos tiene otras ventajas además de su flexibilidad. Así que para uno, las pruebas del plan son más legibles. Además, los módulos del plan organizados por funciones son más legibles manteniendo las funciones de negocios en evolución.

1.6 *Potenciales de desastre.*

Es importante saber las causas comunes de un desastre para seleccionar detectores que valgan la pena, alarmas, y sistemas de supresión que ayuden a prevenir desastres, a continuación una lista de potenciales de desastre.

- Inundación- La intrusión de agua (o de otros líquidos) en las áreas de trabajo es la causa más común de desastres.
- Incendios- Provocados por incontables causas, el daño del fuego provoca pérdidas millonarias cada año. Una de las peores amenazas para los encargados de la PLRD.
- Huracanes- Un potencial de desastre natural, que no son necesariamente la causa directa de apagones, pero crean condiciones para otro tipo de desastres dañando las instalaciones, disminuyendo la luz eléctrica, afectando los cables telefónicos, etc.

- Cortes en la Infraestructura- Cambios en la energía eléctrica, pérdidas de agua o servicios de drenaje, fallas en la planta de aire acondicionado, y cortes en las líneas telefónicas son cortes en la infraestructura que pueden hacer inhabitables las instalaciones de la empresa o perjudicar la operación de las redes y sistemas vitales.
- Fallas en software y hardware- Los sistemas y el hardware de las redes tienen un cierto período de vida, que se puede ejemplificar de dos formas: tiempo que tardarán en fallar y tiempo que tardarán en repararse. Un mantenimiento preventivo regular prolongará la vida del equipo, pero el uso, los efectos de contaminación ambiental, o errores de los operadores mismos pueden provocar fallas, mientras que las fallas de software son resultado de innumerables causas.
- Destrucción accidental y sabotajes- Daños a propósito o sin intención a las instalaciones, provocados por personal de la compañía, la competencia, o errores provocados por la curiosidad de algunas visitas en la empresa.

Consideraciones ambientales.

A algunos potenciales de desastres se les debe poner más atención en el proyecto de planeación debido a cuestiones ambientales. Por ejemplo, ciertas áreas geográficas son más susceptibles a huracanes o temblores que otras. Además de potenciales de desastre provocados por la naturaleza, la proximidad de la compañía con algunas fábricas que elaboren, procesen o almacenen cosas de peligro, como plantas de energía nuclear, pinturas y procesos químicos, etc., detalles que deben ser considerados por los responsables de la planeación. Estos potenciales pueden ser mejor identificados con la ayuda de alguna institución de protección civil. Estas organizaciones por lo regular tienen información acerca de los peligros locales que puede ser de gran ayuda.

Los encargados de protección civil deben ser consultados para poder realizar de manera correcta una evacuación en caso de que se requiera. Ya que éstos planes son típicamente desarrollados por estas organizaciones, en eventos como huracanes, temblores o desorden civil.

Los encargados de la planeación deben saber bajo qué condiciones se encuentran las instalaciones que deberán ser evacuadas y qué procedimientos existen para volver a reinstalarse después del siniestro. Todos estos procedimientos deben ser tomados en cuenta para realizar el plan.

El factor tiempo.

El tiempo es un multiplicador de pérdidas. Entre más tiempo se quede una compañía sin sus funciones críticas y vitales de los negocios, mayores serán los costos y difícilmente se podrá llevar a cabo una recuperación total. La temporada en la que ocurre un desastre, es decir, un día en específico, semana, mes o año, es también determinante en cuanto a pérdidas para la compañía. Una interrupción que ocurra el fin de semana o en las vacaciones no tendrá las mismas consecuencias desastrosas en comparación con un desastre que ocurra en los procesos de fin de mes o de año.

Reconociendo éstos puntos, muchos encargados de realizar la PLRD buscan determinar un tiempo estimado de interrupción, antes de que la interrupción se vuelva realmente desastrosa. Algunos otros buscan identificar períodos de tiempo específicos en los cuales la interrupción es perjudicial y costosa para calcular los daños y administrar una exposición de ésta índole basada en un escenario con el peor de los casos.

Máxima interrupción aceptable.

De acuerdo con estudios realizados, las empresas financieras son las menos tolerantes a las interrupciones, sólo unas 48 horas, antes de que las pérdidas de las funciones de negocios se vuelvan irrecuperables. Las industrias encargadas de distribución pueden mantener sus operaciones hasta 72 horas, mientras que en las industrias de manufactura, compañías aseguradoras, y otras pueden sobrevivir hasta 6 días después de la interrupción. Ésta

información representa un porcentaje basado en estimaciones hechas por inspectores del tema. Los encargados de las funciones de negocios pueden ayudar para obtener mayor información para poder calcular el tiempo estimado de interrupción para la empresa. Deben ser cuantificadas algunas encuestas, resumidas en hojas de trabajo de evaluación crítica preliminar, para demostrar qué proporción de costos agregados resultarán para las primeras 24 horas, y qué cantidad para las siguientes 24, y así sucesivamente.

Según los expertos, 72 horas son consideradas ideales para el tiempo de recuperación. Algunos negocios pueden soportar interrupciones más prolongadas, mientras que otras deben realizar los cálculos completos de las pérdidas financieras en el menor tiempo posible. El marco de tiempo para la recuperación que se presentará a la administración debe corresponder a los requerimientos de la compañía y no a las 72 horas recomendadas por expertos.

1.7 Detalles a tomar en cuenta en un caso de desastre.

- Instalaciones, incluyendo áreas de trabajo de usuarios, centros de datos, etc., deberán ser evaluados para su seguridad.
- Los sistemas de distribución de energía eléctrica de la compañía, pero especialmente en el centro de datos, deben ser revisados para saber que tan resistente es, y para conocer los riesgos posibles.
- Detección de fuego e inundaciones, etc. (o la necesidad de éstos detectores) debe ser identificada.
- Los controles de acceso físicos y electrónicos existentes, deben ser evaluados desde dos perspectivas. Los encargados de la PLRD deben juzgar la efectividad de éstos controles para reducir los riesgos de seguridad. También deben saber cómo los controles de seguridad deben ser probados para cumplir con los objetivos de recuperación en el momento de un desastre.

La adquisición de sistemas para prevenir incendios, fallas en el equipo de energía eléctrica o restringir el acceso a hackers en los sistemas y redes de la compañía, es claramente justificado en el contexto de la PLRD y ofrece muchos beneficios que ayudan a justificar su adquisición.

Dos beneficios son obvios, el primero, las compañías de seguros tienden a dar crédito con descuento anual, por cada sistema de prevención instalado en la compañía. Por ejemplo: la adquisición de un UPS (proveedor de energía eléctrica sin interrupciones), éste tiene dos funciones.- obviamente reduce la probabilidad: de falla debido al uso de equipo, pérdida de datos, errores en programas y otros potenciales de desastres asociados con cambios en la corriente eléctrica y apagones. Esto lo hace, proporcionando la energía eléctrica suficiente para los equipos conectados en caso de apagón, o hasta que se reactive otro generador de luz eléctrica.

Esta ayuda, hace las operaciones más eficientes superando cortes de luz menores que ocurren cada vez que hay una tormenta o cuando falla la compañía de luz. Claramente un UPS puede ofrecer lo necesario para mantener las operaciones normales bajo éstas circunstancias y proporcionar una eficiencia mejorada en las diversas operaciones del centro de datos.

Para preparar la adquisición de un UPS, es importante poner en una lista el equipo o lugares que necesitarán ser protegidos por el sistema:

- Iluminación en áreas clave de trabajo.
- Hardware del Centro de Datos, y ciertos controladores de terminales y redes.
- Aire acondicionado en el cuarto del UPS, cuarto de conmutadores de teléfono y en el centro de datos.
- Central privada de conmutación (PBX) y otros sistemas de telefonía.
- Sistemas de control de acceso alimentados por electricidad (tales como lectores de tarjetas de identificación).
- Sistemas de prevención de desastres alimentados por electricidad carentes de baterías de emergencia.
- Elevadores.

Otro ejemplo de beneficio en sistemas de prevención de desastres es una política de no fumar, a menudo principalmente implementada como un programa para prevenir incendios, ésta política no sólo reducirá el riesgo de fuego accidental o minimizará el riesgo de contaminación ambiental que puede acortar la vida de algunos equipos de procesamiento de datos, también nos da la ventaja de crear un lugar de trabajo más saludable, reduciendo los gastos médicos, y si las estadísticas son correctas, reduce el gran número de empleados enfermos anualmente.

Donde sea posible, estos beneficios prácticos de sistemas de prevención de desastres deben ser incluidos para justificar los costos de su adquisición. Todo esto dándonos entonces, reducciones de seguros y ahorros de costos operacionales. Debe ser obligatorio justificar la implementación de ciertas estrategias de reducción de riesgos y tecnologías de prevención.

Otro tipo de información que debe ser solicitada a los representantes del gobierno concierne a los riesgos naturales o hechos por el hombre que se puedan presentar por la cercanía de las instalaciones de la compañía. Si plantas de procesamiento químico o edificios nucleares se encuentran cerca de la compañía, los encargados de la PLRD deberán considerar un método obligatorio de evacuación. Por ejemplo, si una fábrica de químicos tiene un incendio y se empieza a contaminar el aire, los oficiales encargados de mantener la seguridad deben evacuar áreas de empresas y hogares, por un período de tiempo hasta que el fuego quede controlado y comprobar que el riesgo ha terminado, si a una empresa, por el perímetro de evacuación, se impide el acceso a las instalaciones por varios días, se necesitaría aplicar la PLRD y temporalmente reinstalar sus operaciones a un centro de datos de respaldo. Este potencial de riesgo, que viene con el lugar donde esté instalada la empresa, necesitará ser considerado en la PLRD; inspectores locales son generalmente la mejor opción para identificar tales potenciales de amenaza en el vecindario.

Controles Ambientales.

Los controles de pureza de aire y clima son ignorados en discusiones de prevención de desastres, a pesar de estar muy asociados con sistemas de prevención. Se debe enfatizar la necesidad de controles de temperatura como el aire acondicionado, que mantienen los niveles de temperatura y humedad del centro de datos con las especificaciones propuestas de los fabricantes de equipos. Aún así, muy pocos tratan el tema de contaminación ambiental, que se ha identificado como una de las fuentes de fallas en equipos y hasta incendios.

La siguiente lista muestra algunos tipos de contaminantes y sus daños potenciales.
Contaminantes y sus daños potenciales.

TIPO	EFECTOS DAÑINOS
Metales	Conductores de electricidad, magnéticamente atraídos por circuitos electrónicos.
Partículas de carbón	Absorben humedad, conductores de electricidad, inflamable.
Partículas de fibra sintética	Se derriten con facilidad, absorben humedad, algunos tipos son inflamables, conductores eléctricos.
Polvo de cemento y Partículas cristalinas	Causan sobrecalentamiento, fallas generales en medios como discos duros, flexibles, etc.

Conociendo los tipos y niveles de partículas contaminantes que se presentan con el flujo del aire, se pueden tener pistas acerca del origen de contaminación, entonces algunas medidas deben ser tomadas en cuenta para eliminar ciertas fuentes contaminantes.

A continuación una lista de fuentes de contaminación.

Los contaminantes ambientales que se meten en el cuarto de equipos debido al tráfico humano. Piel, pelo, fibras de ropa, colillas de cigarro, así como la presencia de impresoras, papel para impresión, y botes de basura en el cuarto de cómputo son bien conocidos como contribuidores de contaminación provocada por carbón, fibras sintéticas y orgánicas. Estas partículas tienen la tendencia a regarse por la superficie de los equipos, incluyendo circuitos electrónicos y filtros. Desde que las partículas pueden conducir electricidad debido a la absorbencia de humedad, las consecuencias de ésta contaminación incluyen incendios y cortos circuitos. Peor aún, el bloqueo en los filtros y la penetración de contaminación microscópica en los diferentes medios de almacenamiento de datos, pueden llevar al sobrecalentamiento y fallas generales, en la superficie de los medios que dan como resultado errores de lectura-escritura y hasta la falla total del medio.

Lista para reducir contaminación ambiental.

1. Verificar que el piso falso del centro de cómputo no esté gastado, y que el piso esté propiamente sellado. Cuando el trabajo sea realizado en el espacio del piso original, asegurarse de que el piso falso sea colocado en al misma posición en la que estaba. El uso del piso y superficies de concreto son conocidos como fuentes de contaminación.
2. Inspeccionar las plantas de aire acondicionado para evitar las partículas metálicas en el ambiente. También, asegurarse de que el aire acondicionado no esté infiltrando partículas del exterior del edificio, porque puede introducir contaminación al centro de datos y centro de cómputo. Tomar medidas para utilizar los filtros adecuados.
3. Establecer y reforzar la prohibición de no fumar en el cuarto del equipo.
4. Usar otro lugar u otras tecnologías para colocar impresoras de impacto o láser, y sus respectivos accesorios fuera del centro de datos.
5. Quitar los calentadores con compuestos de nicron y todos los purificadores de aire que trabajen con ion del cuarto de equipos. Ambos pueden llenar el aire de partículas y así contaminar los circuitos.
6. Asegurarse de que todo el equipo funcione con filtros de alta calidad, para que filtren hasta un nivel de micro partículas. Inspeccionar y cambiar los filtros regularmente.
7. Asegurarse de que exista una presión positiva del aire en el cuarto de equipos (el aire debe soplar del centro hacia afuera siempre que se abra una puerta. Si este no es el caso, consultar con un especialista ambiental para que determine qué presión es la adecuada).
8. Establecer un programa regular para pruebas ambientales usando un método confiable que recolecte muestras y haga evaluaciones. Usar los resultados de las pruebas para identificar cualquier contaminación.
9. Dar mantenimiento regularmente al equipo de cómputo. Las compañías de mantenimiento deben usar limpiadores adecuados y nunca engrasar los pisos de los cuartos de equipos.
10. Si los problemas de contaminación se vuelven crónicos, buscar la posibilidad de un purificador de aire mantenido por un equipo de filtración ambiental.

Daños provocados por agua.

Aún si el equipo ha sido tapado con alguna lona y si hay tiempo suficiente para que se seque completamente (se sugiere usar una secadora de pelo para acelerar el tiempo de secado) las redes y sistemas tendrán un funcionamiento dudoso.

Las pequeñas filtraciones con el paso del tiempo traen consecuencias desastrosas. Para prevenir ésta posibilidad, los encargados de la planeación deben considerar la instalación de un detector de agua con alarma para que notifique al centro de datos y demás personal la presencia de agua o algún otro líquido antes de que llegue a dañar el equipo.

Se debe entender que los detectores de inundación no darán protección en caso de una inundación mayor debida al mal clima u otros factores, pero ayudarán a identificar filtraciones

menores, entonces se tomarán medidas para minimizar un problema aún mayor. Debido a esto, los encargados de la planeación, cuyas instalaciones utilicen enfriadores de hardware por medio de agua o que estén construidos cerca de algún espacio de descanso (un comedor, gimnasio, etc.) o tuberías de agua en las paredes del cuarto de equipo, deben buscar un subsistema de alarma de detección de agua específico para el cuarto de equipo. Aquellos, cuyas instalaciones no presenten estos riesgos, deben considerar otro tipo de sistema detector de agua.

Daños provocados por el fuego.

- La temperatura ante la cual el fuego empieza a dañar el equipo de cómputo es de 79.4 grados centígrados (no los 232 grados con los cuales el papel se quema) y estos son 10 grados de más con los que se derriten las cintas y los discos de almacenamiento.
- El humo generado aún por un papel pequeño, se quema rápidamente y produce tremendas cantidades de partículas contaminantes dentro del centro de datos que puede dar como resultados la falla en equipos y el subsecuente incendio.
- El fuego en combinación con algunos cables revestidos de material inflamable (generalmente es PVC lo que se usa para aislar los cables de computadora), produce una mezcla gaseosa de fosgeno, hidrógeno, cloro y cianuro de hidrógeno, una combinación de ácidos y humos mortales que pueden dañar al equipo y matar al personal.
- Los transformadores de poder pueden contaminar tanto la atmósfera, y pueden convertir, por un prolongado período de tiempo, inhabitables los lugares de trabajo, debido a la gran contaminación térmica y riesgos en la salud.

Lista para prevenir el fuego.

1. Establecer una regla de no fumar.
2. Inspeccionar regularmente las instalaciones y quitar los combustibles de la proximidad de encendedores potenciales.
3. Identificar riesgos de la salud relacionados con el fuego, ciertos tipos de alfombras sintéticas y tapicería, plásticos, aislantes de PVC, etc. y reemplazarlos con sus equivalentes menos dañinos.
4. Inspeccionar todos los dispositivos eléctricos, extensiones, para ver si cumplen con la norma UL.
5. Contactar a los bomberos locales y contratar un peritaje, para así identificar los riesgos de fuego en las paredes, techos y pisos.
6. Asegurarse de que las salidas de emergencia estén libres de estorbos y claramente señaladas. Identificar a los detectores de fuego, humo y probar su propia operación.
7. Conducir simulacros regulares de evacuación e iniciar un programa, en toda la compañía, de Prevención de Desastres.
8. Localizar las capacidades para suprimir el fuego tales como bombas de agua contra incendios, sistemas de regaderas, y extinguidores. Tomar en cuenta el estado en el que se encuentren y ver que cumplan con las normas.
9. Tener extinguidores químicos de fuego en los cuartos de equipos.

Daños provocados por personal de la empresa o ajenos.

La destrucción o daño de los recursos puede ser resultado de acciones de personas con acceso a los cuartos de equipos. Más aún, medios con datos importantes de la empresa pueden ser dañados sin intención o a propósito por poner los medios en lugares inadecuados, como en dispositivos electromagnéticos, (podría ser un clip). Por eso, además de mantener afuera a los intrusos, los controles de acceso físico son necesarios para restringir el acceso a los cuartos de equipos y dar permiso solamente al personal con el conocimiento necesario en electrónica, para prevenir errores obvios que puedan perjudicar al equipo o a los medios con datos importantes.

Debido a esto, hay una cantidad de razones válidas para retomar la planeación de seguridad física y varios métodos han sido desarrollados. Estos métodos se dividen en tres tipos.

1. Controles de autenticación. - Estos son usados para verificar, a las personas que busquen la entrada a las áreas sensibles de la empresa que realmente estén autorizadas en hacerlo. La autenticación debe llevarse a cabo por medio de algún tipo de identificación y a su vez que ésta sea evaluada por una persona o algún sistema electrónico antes de entrar al cuarto de equipos. La forma más simple de control de autenticación es una cerradura para la cual solo individuos autorizados deberán tener la combinación o la llave.

2. Monitores y alarmas. -Algo que también concierne a la seguridad física, son las actividades de las personas que han ingresado a un área sensible. Esto puede ser monitoreado por medio de sistemas de acceso con contraseñas, los movimientos de los individuos en áreas sensibles, son controlados por las grabaciones de los circuitos cerrados y/o alarmas cuando actividades impropias son detectadas por medio de alarmas de intrusión, censores de interferencias, etc.

3. Controles de salida. -Éstas son usadas para seguir los traslados de información importante o equipo desde el centro de cómputo a otros lados. Estas técnicas deben tener inspecciones de portafolios y otros contenedores, la disposición de sistemas seguros, por ejemplo trituradoras de papel, controles electrónicos de voz y líneas de comunicación de datos, o dispositivos que prevengan la duplicación de datos en discos.

Lista de controles de acceso físico.

1. Identificar los dispositivos de autenticación usados para controlar el acceso al centro de datos o al cuarto de equipo telefónico. Evaluar los controles por completo y sugerir seguridad adicional en caso de que sea necesario.
2. Identificar las cerraduras electrónicas y manuales en puertas y ventanas. Asegurarse de que en la salida exista un control. Sugerir cerraduras adicionales si es necesario.
3. Obtener copias de llaves o combinaciones de cerraduras para ser usadas en casos de emergencia.
4. Identificar controles de acceso de almacenamiento de materiales sensibles. Obtener copias de llaves o combinaciones requeridas para evacuar los materiales sensibles en una emergencia. Sugerir controles de acceso adicionales si es necesario.
5. Establecer métodos para asegurar que el control de acceso a la información no sea revelado excepto en una emergencia.

Controles de acceso electrónico.

Además de los controles físicos, muchas compañías emplean una variedad de controles de software y hardware para prevenir el acceso desautorizado a los sistemas y redes de la empresa. Como con los controles físicos, la intención es bloquear a los vándalos, hackers, y otros criminales de computadoras de las redes y bases de datos.

Éstas son algunas categorías de protección que existen:

1. Protección de puertos.

Esto consiste en proteger el acceso a redes y sistemas, asegurando los puertos de acceso. Una combinación de controles de hardware y software son regularmente usados para proteger los puertos de comunicación, incluyendo módems y validación de código de hardware.

2. Protección con contraseñas.

Ésta es la forma más común de control de acceso a redes y sistemas. Se les proporciona una contraseña de autenticación única a los usuarios legítimos de la compañía para utilizar

los servicios de teléfonos o aplicaciones computacionales. Cuando quieran acceder al sistema o al servicio de red, deben ingresar su contraseña, la cual es validada por medio de software en la computadora. Si la contraseña coincide, el acceso es permitido y se pueden utilizar programas e información para lo cual, ha sido autorizado de acuerdo a su perfil de usuario asociado con su contraseña. Después de eso es indispensable monitorear las actividades del usuario una vez que se le ha autorizado el uso de los diferentes recursos. Los intentos del usuario para acceder a programas o archivos desautorizados, para borrar archivos, e instalar o modificar nuevos programas (por ej. los virus), deben ser monitoreados, y el usuario debe ser advertido de que su actividad no está permitida, de acuerdo con su perfil, y avisarle que será desconectado.

Controles en las áreas de usuario.

Indiscutiblemente, prevención de incendios, prevención de robos, y controles de acceso son aún más importantes en el ambiente de usuario, ya que es aquí donde la mayoría de desastres y robos ocurren más que en los centros de información o centros de telefonía.

Daños en las computadoras.

- Cuando los componentes de las computadoras tienen alguna falla, el tiempo que toma su reparación es muy corto. Las fallas en discos duros ocurren, en promedio, de 20 a 30 mil horas (si su uso es rudo de 2 a 4 años). Uso inapropiado y factores ambientales pueden reducir su tiempo de vida.
- Frecuentemente las computadoras son alimentadas directamente del enchufe de luz convencional que es utilizado para suministrar electricidad en el edificio. Variaciones en el voltaje, corriente, y apagones, son causas potenciales de fallas en los componentes, sistemas, y de errores de lectura-escritura.
- Los niveles de contaminación ambiental en las áreas de trabajo de usuarios son casi imposibles de controlar, sin haber establecido cuartos limpios previamente. Debido a esto, la contaminación en aumento podría dañar la operación de las computadoras con el paso del tiempo.
- Las áreas abiertas de trabajo no proveen la seguridad necesaria para las computadoras, sobre todo si no tienen contraseña. Esto provoca que las PCs, estén disponibles para todos, exponiéndolas a los virus y otros ataques basados en software.
- Los incendios en los centros de procesamiento de datos, sólo se dan en porcentajes muy pequeños. La mayoría comienzan en las áreas de trabajo. Las computadoras generalmente se dañan al momento en que los sistemas contra incendios se activan, como por ejemplo; extinguidores, o el uso de mangueras utilizados por los bomberos.

Daños en redes LAN.

Los servidores de archivos no necesitan ser colocados en el mismo lugar con las estaciones de trabajo en red. En algunas configuraciones, el servidor debe ser colocado en el centro de datos y no en el de usuarios, en donde estará en un lugar más seguro y menos propenso a un desastre.

Daños en otros equipos.

Switches de telecomunicaciones, extensiones de hardware para trabajar con un mainframe distante, y periféricos de computadoras para los cuales su operación es crítica (por ejemplo: módems, multiplexores, controles de dispositivos, procesadores, etc.) deben ser minuciosamente revisados para su protección y requerimientos preventivos.

II CONSIDERACIONES IMPORTANTES PARA LA RECUPERACIÓN DE INFORMACIÓN.

2.1 *Selección de información a proteger. (Identificando la información crítica en los datos.)*

¿Qué tipo de información necesita protegerse? Ésta pregunta supone que algunos datos son más importantes que otros. Claramente, hay diferencias en la importancia de grabaciones con información basadas en su uso o propósito. Algunos respaldos se necesitan para dar soporte a las actividades diarias de los negocios, otros tienen una importancia histórica y deben estar sujetas a auditorias especiales o para retención en caso de requerimientos legales, y otras podrían contener, información sensible, clasificada, y secreta. Estas diferencias las debe entender muy bien el encargado de la planeación, para así desarrollar un plan apropiado en realizar los respaldos, almacenamientos y accesos.

Debido a esto, uno de los primeros pasos en la planeación de almacenamiento externo es identificar qué tipo de grabaciones y datos son producidos por las unidades de trabajo de la compañía y de qué manera los datos son utilizados. Una vez que se haga esto, se implementarán regularmente algunos esquemas para asignar criticidad relativa a las grabaciones e información, indicando qué es lo que se incluirá en un programa de almacenamiento seguro y si serán almacenadas permanentemente o actualizadas periódicamente.

2.2 *Definición de criticidad.*

Una grabación o conjunto de datos es crítica cuando se requiere para el rendimiento de una función crítica de negocios y aplicaciones empresariales. Por ejemplo; un conjunto de datos activo que es usado y activado cada vez que la orden de un cliente se ingresa en un sistema de entrada de órdenes automático, podría ser un conjunto de datos críticos. De manera breve, sería cualquier conjunto de datos o grabaciones que se usen en conjunto con un sistema de información o red que se ha definido previamente como crítica, entonces comparte la misma clasificación del sistema o red, y eso hace a un conjunto de datos crítico.

Pero desde el punto de vista de la PLRD, las grabaciones críticas son aquellas que son requeridas para la recuperación y que sin ellas la recuperación sería imposible. Para los requerimientos legales y auditorias, se recomienda cierto tipo de grabaciones (reportes administrativos, datos de contabilidad, contratos, los libros de la compañía), también deben ser protegidos de una pérdida. También, documentos de propiedad, código fuente del software, patentes en trámite de la compañía, etc. representan una inversión de tiempo y recursos de la empresa, por lo tanto ésos documentos ameritan ser protegidos. Estos datos también son críticos, aunque no se requieran para mantener las operaciones diarias de la empresa.

Debido a esto, la identificación de las grabaciones o datos críticos, se hace mejor aplicando los siguientes criterios:

1. ¿La grabación/información se requiere para realizar o dar una función crítica de negocios?

2. ¿La grabación/información se requiere para una orden legal o auditoria?

3. ¿La grabación/información incluye propiedades, secretos de la empresa, o alguna otra información sensible que podría ser difícil o costoso reproducir o reconstruir?

Si éstas preguntas son tomadas en cuenta por el equipo de la PLRD, la información crítica se podrá distinguir mejor de la menos importante. ¿Cuál es la ventaja de tal distinción? Es el ahorro de costos. De acuerdo con las estadísticas de la industria, más del 75% de la información retenida por el personal de la empresa son duplicados de originales, documentos obsoletos, o que ya no se utilizan. Si las grabaciones críticas o vitales se distinguen de las que no son importantes, seguramente el resultado será un volumen menor de grabaciones que se deban guardar en un site externo de respaldos. De ésta manera se reducirán los costos.

2.3 *Redundancia.*

Claramente, cualquier estrategia de recuperación para una red de trabajo implicaría llevar a cabo la redundancia. Se tendrían que tomar en cuenta enrutamientos de las comunicaciones o los reemplazos de hardware. Desde luego que no todos los aspectos de la redundancia en la estrategia deben ser adquiridos o establecidos en el momento del desastre. Algunas compañías de servicios de redundancia estarían disponibles para ayudar inmediatamente después de una interrupción.

Servicios para dar redundancia a redes.

De manera simple, la redundancia sugiere que una red de trabajo de respaldo debe ser usada si la red principal falla. En la práctica, éste escenario involucraría el cambio de la red amplia de trabajo privada de la compañía a una red pública o híbrida de alguna compañía que ofreciera éste servicio. La mayoría de las áreas metropolitanas tienen a su alcance los servicios de empresas encargadas de dar redundancia a redes, y sería buena idea contar con su disponibilidad, dependiendo de la empresa, en la estrategia para cambiar a una red de trabajo alterna.

Es conveniente investigar cuáles son las mejores compañías que dan éstos servicios de redundancia para así estimar los costos y llevar a cabo ésta opción.

Si la redundancia es lo único efectivo para asegurar la recuperación de una función crítica, se necesita un alcance pragmático para justificar los gastos que frecuentemente incluyen otro tipo de redundancia. Por ejemplo: si una compañía utiliza la pieza de una computadora que es de suma importancia y necesaria para llevar a cabo las operaciones de los negocios y para la cual es muy difícil encontrar la refacción, sobre todo en una emergencia, obtener una segunda unidad sería lo correcto. Así, éste gasto estaría justificado no sólo en términos de su utilidad en caso de emergencia, sino también se utilizaría como aparato de entrenamiento o como una refacción.

Redundancia total.

La redundancia total como una estrategia es demasiado costosa, no sólo porque se requeriría la construcción y mantenimiento de unas instalaciones idénticas a las originales, sino también para la interconexión entre las dos instalaciones. Obviamente, ésta es una opción sólo para las grandes corporaciones y para operaciones selectas del gobierno.

Y hasta, para aquellas organizaciones que pueden pagar tal lujo, la redundancia total es un mito. Llevando a cabo una transición instantánea desde el ambiente de operaciones normal hasta el ambiente de recuperación usando el mismo personal de la compañía requiere algo de tiempo. El personal debe ser cambiado al site de respaldo, que se encontraría localizado remotamente desde el site original para que no se vea afectado por el desastre regional que ha afectado ya al site original. Suponiendo que el personal necesario, no se ha visto afectado por la muerte, traumatismos, etc. en el momento del desastre, los planes para cambiarse del site pueden ser afectados por el clima adverso o por situaciones en la cuales el personal sería alejado de su familia.

La probabilidad de un desastre que afecte de manera total es muy escasa. De todas formas en cualquier desastre, existen algunas prioridades que deben tomarse en cuenta en la restauración. Manejar desastres que afecten sólo algunas partes de la compañía y no a toda la empresa, por medio de una redundancia total o de una estrategia de recuperación organizacional (ambos métodos diseñados para abarcar un desastre total) podría ser un proceso que consumiría más tiempo en vez de restaurar las funciones de las unidades de trabajo afectadas. Las pruebas de éstos aciertos se encuentran en las experiencias de las empresas que se han recuperado exitosamente de desastres severos. Invariablemente, estos casos demuestran que la recuperación funcional puede ser realizada con unas 48 o 72 horas, mientras que la recuperación organizacional o total (la restauración o transición a los modelos normales organizacionales) tomaría muchas semanas.

Estrategias para proporcionar redundancia a equipos y subsistemas.

El objetivo es identificar registros e información que requieran protección, tanto en las áreas de trabajo y en los centros de información. La técnica a llevarse a cabo en cada caso sería obtener la asistencia e involucrar a la unidad de trabajo administrativa (gerencia). Esto se puede llevar a cabo, haciendo que los gerentes tomaran posesión de los registros e información que se produce.

Identificando los requerimientos de almacenamiento (retención) de las unidades de trabajo.

Algo de la información en registros y requerimientos de información, se seleccionará con ayuda de cuestionarios contestados por los gerentes o administradores en alguna parte del proyecto.

Con el cuestionario, los gerentes de las unidades de trabajo se les pedirán que indiquen 5 puntos de información acerca de cada registro que hayan identificado. Primero, la forma (2-1) usa un código "clase" que debe ser usado para reportar estadísticas en almacenamiento de registros de información. Entonces el gerente selecciona un número de la columna A en la parte baja del cuestionario para seleccionar el tipo de dato o registro que ha sido identificado, para mantener el código numérico asociado. Entonces el gerente selecciona el código numérico asociado de la columna B para especificar el tiempo que se requiere para su retención. El tiempo especificado debe estar basado en evaluaciones que indiquen si los datos realmente son necesarios y si se utilizan para aspectos legales o para requerimientos de auditorias. Éste código de "clase" (la combinación de letras con códigos numéricos) se ingresa en la columna "Clase" de la forma a llenar.

Después, el administrador escribirá una breve descripción de los registros y el tipo de medios en los cuales los registros serán almacenados. El almacenamiento debe ser en papel, microfichas, medios electrónicos (cintas, o discos duros removibles), o discos compactos.

La columna marcada como "volumen" es para su uso posterior en la asignación de registros para su almacenamiento en cajas que se guardarán en los dispositivos o medios externos. La columna de "requerimientos especiales" especifica cualquier mantenimiento en específico, preservación, o requerimientos de retención que no se hayan especificado en la parte de las definiciones del código "Clase" en la parte baja de la forma.

Estas hojas proporcionan los medios para mantener los registros de almacenamiento de todas las unidades de trabajo, además de dar una lista para usarse en revisiones periódicas de planes de almacenamiento de unidades de trabajo. Un administrador de unidades de trabajo, podría así rápidamente revisar la lista, quitar cosas que ya no se necesiten, agregar más cosas, etc.

Identificación de los requerimientos de los centros de datos.

Desde luego, una unidad de trabajo en la compañía con requerimientos especiales implica la necesidad de procesar datos. Para que esto sea efectivo, los respaldos en un ambiente de procesamiento de datos, se deben hacer diariamente, especialmente en los datos relacionados con sistemas críticos y redes de trabajo.

En la forma (2-2), se muestra una forma básica, para monitorear respaldos por medio de cintas (que es lo más común para los respaldos, aunque podrían usarse otros medios), en los centros de datos.

Generalmente, los respaldos en los centros de datos son de dos tipos: de "volumen total" o "en incremento". Se puede hacer una copia total del sistema, incluyendo el software, utilerías, aplicaciones y datos, creando lo que a menudo se conoce como respaldo de "volumen total". En algunas empresas, los requerimientos de tiempo para llevar a cabo ésta tarea, provocan que los respaldos de volumen total se hagan semanalmente o con menos frecuencia. El administrador del centro de datos es responsable de indicar en qué intervalos se deben hacer los respaldos de volumen total.

HOJA DE REGISTRO DE RETENCIÓN.

Instrucciones: Complete ésta forma para indicar los requerimientos de retención para los registros producidos o usados por su unidad de trabajo. Indicar la clase de registro, usando las marcas indicadas al pie de la forma. Indicar el formato para el medio del registro usando el código P para papel, E para medios electrónicos, D para discos, o M para microfichas. Especificar el volumen actual en números de cajas de almacenamiento para la Planeación de almacenamiento exterior.

Clase especiales	Descripción	Medio	Volumen	Requerimientos

Códigos de clase: Un código de clase consiste de 2 entradas, una de la columna A y otra de la B (ej: 2B)

COLUMNA A

1—Cuenta/Dato fiscal retención
2—Registros del personal
3—Legalidad/Registros de impuestos retención
4—Ventas/Registros de mercado retención
5—Manufactura/Registros de la planta retención
6—Registros de la empresa
7—Compras/obtención
8—Transporte/envío
9—Seguridad
10—Aspectos médicos
11—Otros

COLUMNA B

X—0-12 meses de retención
A—1-5 años de retención
B—5 a 7 años de retención
C—7 a 10 años de retención
D—10 a 15 años de retención
E—Retención permanente

forma (2-1)

HOJA DE RESPALDOS CON CINTAS.

REQUERIMIENTOS DE ALMACENAMIENTO Y AGENDA PARA LOS RESPALDOS CON CINTAS.

RESPALDOS DE VOLÚMEN TOTAL. Estos respaldos del sistema son realizados en intervalos regulares. La frecuencia de éstos respaldos es:

Semanal
Dos veces por semana
Mensualmente
Dos veces al mes
Trimestral
Otro:_____

REQUERIMIENTOS DE ALMACENAMIENTO. Los respaldos de volumen total actualmente requieren:_____cintas. El número de copias hechas del respaldo de volumen total es:_____

VERIFICACIÓN DE RESTAURACIÓN: Los respaldos de volumen total son probados para su restauración cada:_____ (meses/semanas/días).

RESPALDOS DE INCREMENTO: Estos respaldos del sistema clave y archivos de datos son realizados en intervalos regulares. La frecuencia de éstos respaldos es:

Diario
Cada dos días
Semanalmente
Dos veces a la semana
Dependiendo de la transacción
Volumen
Otro:_____

REQUERIMIENTOS DE ALMACENAMIENTO: Los respaldos de incremento actualmente requieren: _____ cintas. El número de copias hechas con respaldos de incremento es: _____

VERIFICACIÓN DE RESTAURACIÓN: Los respaldos de incremento son probados para su restauración cada: _____ (meses/semanas/días).

MÉTODOS Y SOFTWARE PARA LOS RESPALDOS DE CINTAS

MÉTODOS Y SOFTWARE DE RESPALDO: Los respaldos de incremento y volumen total son realizados usando (imágenes físicas/lógicas). El software usado para crear y restaurar los respaldos es:

Nombre de Producto: _____
Versión/Realización: _____
Fabricante/Contacto: _____

Forma (2-2)

También es importante que la planeación de almacenamiento en medios externos de respuestas a las siguientes preguntas: ¿cuántas cintas (o algún otro tipo de medio de almacenamiento) se usan para los respaldos?, ¿cuántas copias de volumen total de respaldo son producidas?, ¿qué tan frecuentes son probados los respaldos para su restauración?

El número de cintas producidas en un respaldo de volumen total determinarán parcialmente los requerimientos del tamaño físico que se necesitara para llevarlo a un medio de almacenamiento externo. El número de copias hechas (más de un respaldo, por aquello de que los respaldos no se puedan recuperar) afectarán tanto los requerimientos de almacenamiento como a la frecuencia con la cual las cintas deban ser alternadas al centro de datos (externo) para pruebas periódicas y verificaciones de su funcionamiento. Finalmente, el plan hecho para alternar los respaldos, afectará el cuidado de la cinta (o algún otro medio) y a los servicios para su traslado que se utilizarán en una estrategia de almacenamiento externo.

Obviamente, en el período de tiempo en regular los respaldos de volumen total, se agregarán nuevos datos, las aplicaciones cambiarán, y en algunos casos hasta los sistemas serán modificados. Estos cambios se hacen comúnmente en la noche y en medios removibles, y es lo que a menudo se le llama respaldo en incrementos. Dos o más copias de respaldos en incremento frecuentemente se hacen, con una o más copias almacenadas en dispositivos externos.

De ésta manera, en otra parte del documento, se pregunta acerca de la frecuencia con la que se hacen los respaldos, el número de cintas involucradas, número de copias hechas y la frecuencia con la cual su buen funcionamiento es verificado.

En la parte baja de la forma, se registran los detalles del método que se utiliza para hacer los respaldos y el software utilizado. La administración del procesamiento de datos debe indicar si son lógicos o físicos los métodos para hacer las imágenes que son utilizados para hacer los respaldos, encerrando en un círculo la selección.

Con respaldos lógicos, el software de respaldo abre cada conjunto de datos, lee cada grabación de manera individual, y procesa los archivos en algún orden lógico (por ej: por tamaño de archivo). El proceso lógico, es independiente del hardware y reorganizará la información, en el momento en que halla una recuperación de los datos, para mandar los datos a los dispositivos de almacenamiento de la manera más eficiente posible.

Por otro lado, los respaldos de imágenes físicas, operan a nivel de hardware y la información se respalda desde discos de la manera más rápida posible. Los respaldos y las restauraciones de la información respaldada se hacen cuando mucho al doble de la velocidad de los respaldos lógicos, pero no hay una reorganización de los archivos, ni en el proceso de respaldo ni en el de restauración. Además, con los respaldos de imágenes físicas, las restauraciones, generalmente se hacen para almacenar unidades que son del mismo modelo que las unidades de almacenamiento originales, un detalle importante a tomar en cuenta para identificar el mainframe apropiado en la estrategia de recuperación.

Una vez que el administrador ha identificado el tipo de software que se utiliza para los respaldos, es importante tomar nota del nombre, el número, versión y el fabricante del software. Puede existir el caso, de que la recuperación en desastres se retrace por las diferencias del software utilizado para hacer los respaldos y el software que utiliza el mainframe de recuperación que se ha usado para restaurar los respaldos. Hay que asegurarse de que se tiene la información para contactar con el proveedor del software de respaldo, y que esté disponible las 24 horas del día en caso de que los problemas aumenten.

Requerimientos de almacenamiento en sistemas pequeños.

Un gran número de soluciones de software y hardware existen para respaldar sistemas y redes descentralizados.

Antes, en el mundo de los sistemas descentralizados, los respaldos frecuentemente se hacían con disquetes, después, la cinta magnética y los discos duros removibles se volvieron populares. Esto se debe a que la capacidad de los discos duros y otros medios son cada vez mayores y su precio es relativamente accesible.

Otro hecho es que los sistemas operativos de las computadoras más populares incluyen una utilería para hacer respaldos. Los nuevos programas para hacer respaldos ofrecen características básicas para los administradores y usuarios de sistemas pequeños: Son fáciles de usar, con funciones automáticas, compresión de archivos y encriptamiento seguro, además de ser muy flexibles.

Además de éstas características, es importante aprender tres cosas acerca de los requerimientos de los sistemas descentralizados para propósitos de planeación de almacenamiento externo.

Los encargados de la planeación deben identificar la manera en que los sistemas actualmente son respaldados, qué tipo de software y hardware se utiliza, con qué frecuencia se hacen los respaldos, y qué es lo que se necesita para llevar a cabo la restauración. Además, el encargado de la planeación debe aprender cómo es que los respaldos se están almacenando, aún si cualquier actividad de verificación es realizada para asegurar su restauración. Finalmente, el encargado de la planeación necesita investigar cuáles medios son usados para almacenar los respaldos y en qué cantidad.

En la forma (2-3) se muestra una hoja para registrar algunos de éstos puntos de información. También es importante referirse a la información recolectada durante un análisis de riesgo, para identificar cuáles sistemas no son respaldados con regularidad e identificar si se tiene un programa de almacenamiento externo.

Juntando todo, en una lista de requerimientos.

Una vez que la información ha sido juntada con respecto a su tipo y cantidad de registros a ser almacenados en dispositivos exteriores, el encargado de la planeación ahora si está listo para finalizar los requerimientos necesarios para hacer solicitudes a los proveedores de almacenamiento externo (almacenamiento empresarial, off-site storage). Esto, desde luego asumiendo que una estrategia comercial de almacenamiento externo es lo mejor para la compañía.

Por ahora, es importante consolidar la información que ha sido acumulada para así tener una idea más clara de los recursos de almacenamiento, que se necesitarán para la información crítica y registros de la compañía.

La forma (2-4) funcionaría para éste propósito.

Claramente, un requerimiento que debe ser definido es el volumen agregado de registros y medios que deben ser almacenados en los dispositivos externos.

Todas las formas deben ser totalizadas para obtener un resultado estimado del volumen de cintas, discos, etc. y cajas que se utilizarán para almacenar de forma permanente o de período largo, en períodos cortos o frecuentes.

También se deben identificar los requerimientos especiales para el manejo y cuidado de almacenamiento. Para medios, como las cintas, se deben incluir las instrucciones para pruebas periódicas y validación de la integración de los datos, además de los cambios periódicos que se les deben hacer a las cintas. Para papel y registros en microfichas, sus requerimientos deben incluir controles ambientales, inspecciones periódicas, etc.

En la segunda página de la forma, se muestra un calendario o agenda para hacer los cambios preliminares. El calendario debe ser simple o complejo, pero siempre debe contener la información para localizar los puntos de almacenamiento de interés, otros también involucrados, qué tan seguido se deben cambiar, y quién será el responsable en recibir las entregas o preparar los cambios.

También, en la parte baja de la forma, compradores autorizados deben ser designados en caso de hacer una nueva adquisición de emergencia.

Esto se hace por dos razones. Primero, si una emergencia ocurre y los compradores autorizados por la empresa no se encuentran para hacer el pedido, alguien más debe autorizar la compra. La segunda razón para designar a los compradores especiales es para prevenir que individuos sin autorización tengan pretexto de tener acceso a información y registros sensibles que son almacenados en dispositivos externos. Aún en una emergencia, se deben mantener niveles apropiados de seguridad.

HOJA DE ESTRATEGIA DE RESPALDOS PARA SISTEMAS PEQUEÑOS.

LOCACIÓN Y TIPO DE SISTEMA

UNIDAD DE TRABAJO: _____
CONTACTO: _____
TIPO DE SISTEMA: _____

DESCRIPCIÓN_____
_____

ESTRATEGIA DE RESPALDO

¿ES UN PROGRAMA DEL ACTUAL RESPALDO DEL LUGAR? SI/NO
SI LA RESPUESTA ES AFIRMATIVA, DESCRIBIR EL MÉTODO DE RESPALDO:

FRECUENCIA DE RESPALDOS:_____
¿VOLUMEN TOTAL?_____
¿DE INCREMENTO? _____

NÚMERO DE COPIAS HECHAS: _____
¿DATOS COMPRIMIDOS? _____

¿DATOS ENCRIPTADOS? _____

MEDIOS USADOS: _____

CANTIDAD DE MEDIOS: _____

INFORMACIÓN DEL PROVEEDOR DE RESPALDOS DE HARDWARE Y SOFTWARE

HARDWARE DE RESPALDO _____
DESCRIPCIÓN: _____

PROVEEDOR: _____
MODELO: _____
NÚMERO DE SERIE: _____

CONTACTO: _____

SOFTWARE DE RESPALDO
DESCRIPCIÓN: _____

PROVEEDOR: _____
VERSIÓN: _____

NÚMERO DE SERIE: _____

PASSWORD: _____
CONTACTO: _____

Forma (2-3)

HOJA DE REQUERIMIENTOS PARA ALMACENAMIENTO EXTERNO.

ALMACENAMIENTO PERMANENTE.

INSTRUCCIONES. Usar las formas de retención de registros y las de respaldos de cintas para calcular los requerimientos de capacidad de almacenamiento para el almacenamiento externo permanente.

MEDIO DE ALMACENAMIENTO	VOLÚMEN	CANTIDAD
CINTA		
ARCHIVOS DE PAPEL		
MICROFICHAS		
DISCOS		
OTROS _____		

MANEJO ESPECIAL DE CINTAS PARA ALMACENAMIENTO PROLONGADO: Especificar los requerimientos para cintas, incluyendo agenda para validación periódica de la integridad de la cinta.

MANEJO ESPECIAL DE MEDIOS NO MAGNÉTICOS. Especificar los requerimientos especiales en el manejo de almacenamiento de otros medios, incluyendo requerimientos ambientales, accesos periódicos para su inspección, y rotación periódica de regreso al site de trabajo.

Forma (2-4)

ALMACENAMIENTO TEMPORAL/DE TRASLADO.

INSTRUCCIONES: Usar las hojas de retención de registros y las hojas de respaldos de cintas para estimar los requerimientos de la capacidad de almacenamiento de manera temporal o para su traslado continuo al site externo. Usar una unidad de medición estándar.

MEDIO DE ALMACENAMIENTO	VOLUMEN	UNIDAD DE MEDICIÓN
CINTAS		
ARCHIVOS DE PAPEL		
MICROFICHAS		
DISCOS		
OTROS _____		

HORARIO DE TRASLADOS PRELIMINARES.

SE LLEVA DESDE ENTREGAR A	DESCRIPCIÓN	CUÁNDO/QUÉ FRECUENCIA	

ENCARGADOS PARA PEDIR LAS ENTREGAS EN CASOS DE EMERGENCIA:
Lista inicial, objetivo a cambiar, de tres individuos que hallan pedido el transporte o el acceso en emergencias, para almacenar datos y registros. Escribir el nombre, título, licencia de conducir o número de seguro social.

_____

_____

Reverso (2-4)

2.4 Estrategias de respaldos de información.

Habiendo examinado los objetivos básicos en las estrategias de respaldos de sistemas, una revisión de las actividades que tiene la fase del proyecto de la PLRD, se muestra en la tabla (2-5).

Las estrategias a tomar en cuenta son las siguientes:

- Desarrollar una configuración mínima de equipos.- Usando una colección de datos como parte de un análisis de riesgos, es necesario definir cuál es la configuración más adecuada, combinando todas las aplicaciones críticas que el sistema, para la estrategia de respaldos, busca recuperar.
- Identificar los requerimientos en las comunicaciones de datos.- Ya que el proceso de aplicación en el sistema de respaldos será conducido en una locación remota (alternativa al site del servidor), es necesario desarrollar algo para entender cómo es que esto impactará a las comunicaciones normales con el sistema. Los requerimientos para el usuario remoto de alguna terminal y redes periféricas deben ser identificadas tan bien como otras aplicaciones relacionadas con las necesidades de comunicaciones.
- Identificar los requerimientos del usuario.- Dependiendo de la naturaleza del desastre, los usuarios deben permanecer en sus lugares normales de trabajo o ser cambiados a otro lugar para seguir trabajando. La información debe ser recolectada, para definir qué recursos se requerirán en la locación del usuario para reestablecer el proceso y seguir trabajando.
- Evaluar las opciones de respaldo.- Identificando la configuración y otros requerimientos para el sistema de respaldos, el equipo de la PLRD debe buscar una estrategia de respaldos para el mainframe, que cumplirá con todos los requerimientos.
- Evaluar y seleccionar a los proveedores.- El hecho es que más y más compañías están seleccionando proveedores comerciales de recuperación de mainframes, como su solución de respaldos del sistema. En reconocimiento de éste hecho, los encargados de la planeación necesitan saber qué buscar en un vendedor y cómo seleccionar al mejor de acuerdo con sus necesidades.

Respaldo por medio de línea telefónica.

Éste respaldo es muy familiar para los encargados de la PLRD. Como se describe en la figura (2-6), éste método de respaldo describe cómo se enruta la voz y las comunicaciones de información por medio de un interruptor (switch).

Un alcance similar, se ha aplicado exitosamente en el área de repetidores (channel extenders). Éstos habilitan los periféricos del mainframe, para cambiarse a locaciones remotas.

Las comunicaciones entre el canal del mainframe y el dispositivo remoto están realizadas con medios para banda ancha, tales como fibra óptica, enlaces de redes de área amplia, y comunicaciones digitales. Si el centro de datos de alguna compañía se ve interrumpido y si un mainframe de respaldo ha sido instalado, el repetidor debe ser usado para permitir a los usuarios quedarse en su lugar, siempre y cuando se comuniquen con el servidor remoto por medio de un enlace de área amplia.

Enrutar el camino para las comunicaciones entre el servidor y el remoto, por medio del repetidor, los dispositivos deben ser vistos como una variación de la estrategia de respaldo por línea telefónica. Aún así, para una estrategia de éste tipo, los requerimientos para un camino alterno, deben conocerse con anticipación y los planes deben ser puestos en su lugar para establecer la nueva ruta de comunicación cuando sea necesario.

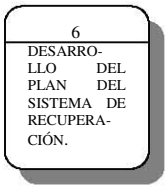
El enrutamiento también es una importante consideración para ver los posibles riesgos en las redes. El acceso a las redes puede ser interrumpido en varios puntos a través de la ruta de acceso, dando como resultado una caída en la red afectando seriamente a la compañía. Por ejemplo, un incendio en la compañía local telefónica puede interrumpir la operación de las redes locales de voz y datos y también afectar el acceso a la WAN.

Una alternativa a éste problema, mostrado en la figura (2-7) es establecer un camino alterno a otra estación de la compañía local telefónica, cercana a la empresa. Ésta redundancia es muy costosa, pero

EL PROYECTO DE RECUPERACIÓN DE DESASTRE.
SISTEMAS DE RESPALDO.

ACTIVIDADES PRINCIPALES

Desarrollar una configuración mínima de equipo
Identificar los requerimientos de las comunicaciones de datos
Identificar los requerimientos de usuarios
Evaluar las opciones de respaldo
Evaluar y seleccionar a los proveedores
Documentar la estrategia



EL PROYECTO DEL PLAN DE RECUPERACIÓN DE DESASTRES

(2-5)

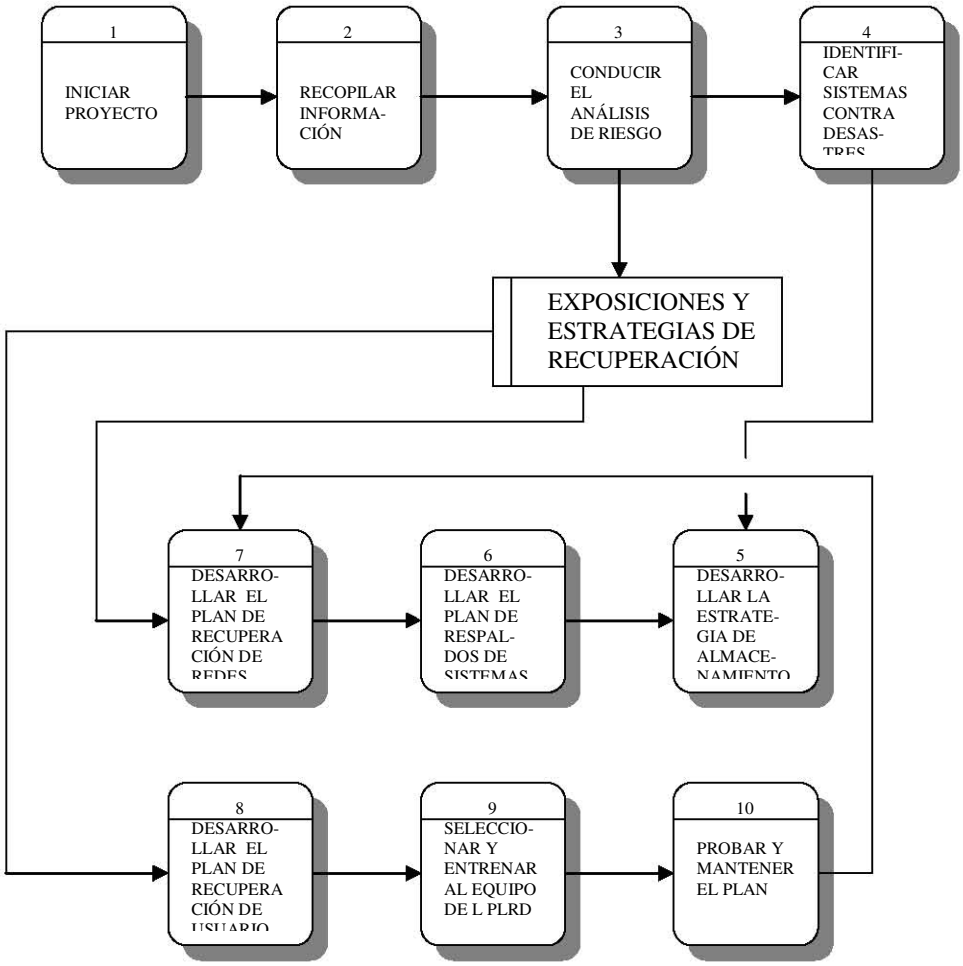
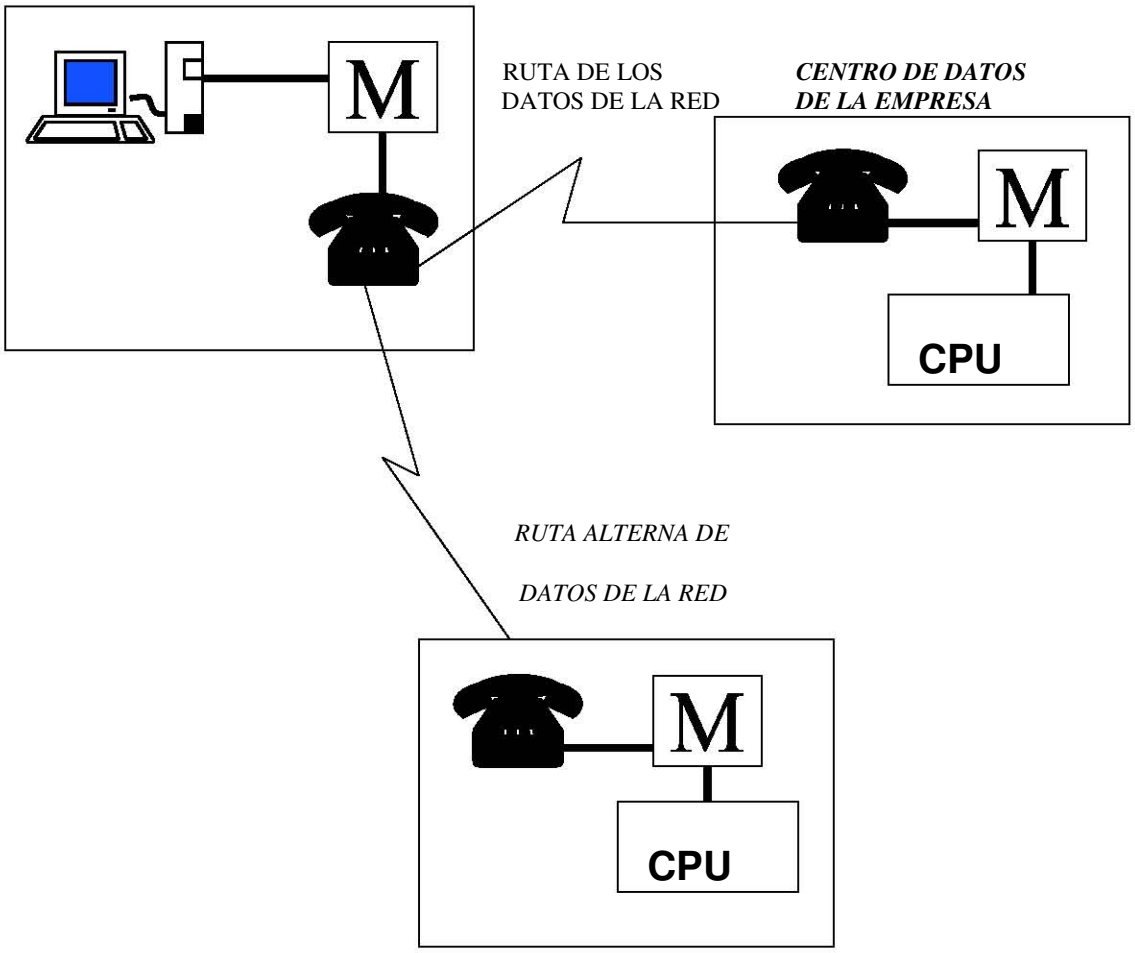


TABLA (2-5)

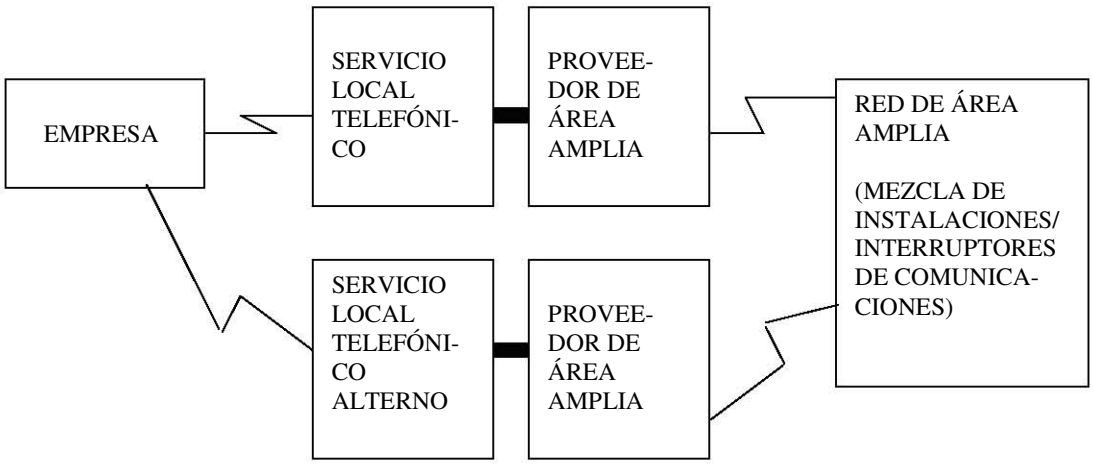
SITE DEL USUARIO *FIG (2-6)*

DE LA EMPRESA



RESPALDO DEL
MAINFRAME DEL SITE

RESPALDO TRADICIONAL POR MEDIO DE LÍNEA TELEFÓNICA.

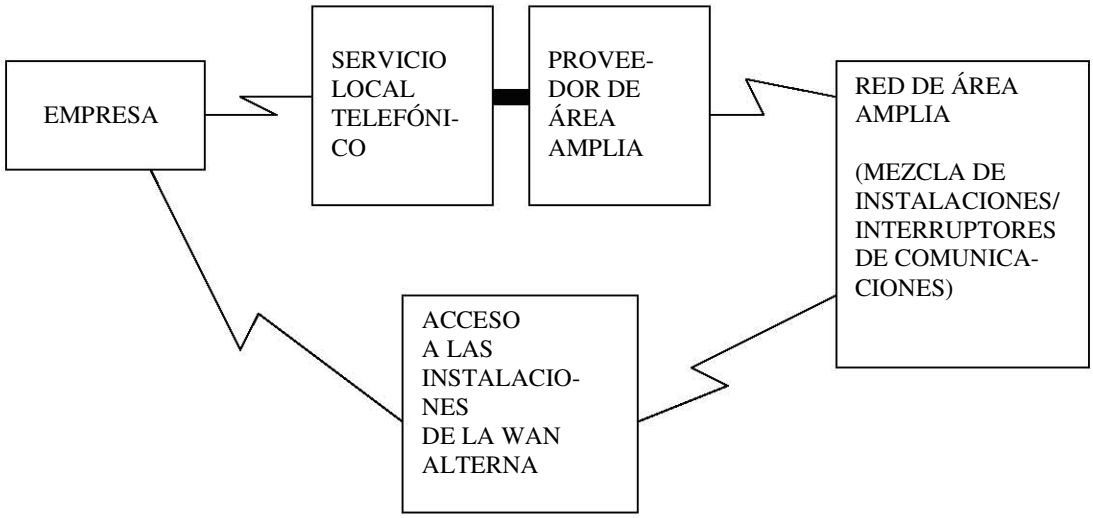


Alternativas de enrutamiento de redes: Acceso a la red a través de una compañía local telefónica.

Fig. (2-7)

Alternativas de enrutamiento de redes: Acceso a través de una instalación alterna.

Fig. (2-8)



puede reducir los riesgos y justificar los costos, sobre todo para una compañía que dependa de las redes de voz y datos.

Una variación en la estrategia de redundancia por medio de enrutamiento se describe en la figura
(2-8).

En algunos casos, a las compañías no les gustaría depender de una sola estación de la compañía telefónica, o intercambiar la portadora de punto de presencia para ganar el acceso a la WAN.

Si el acceso a las instalaciones de una WAN alterna puede ser alcanzado por medio de una ruta alternativa, implementar ésta topología reduciría los riesgos en las redes importantes.

Estas estrategias podrían superar las interrupciones en los accesos que resulten de causas localizadas en el enlace físico o en la estación de la compañía telefónica. Los encargados de la planeación deben ver si es factible tener un camino alterno para las comunicaciones, ya que éste tipo de redundancia es costosa.

Para enfrentarse con la posibilidad de una interrupción en un enlace, se deben considerar otro tipo de medios. Estas alternativas están resumidas a continuación.

Líneas Digitales y Análogas.

Las tradicionales redes telefónicas usan tecnologías analógicas.

Las redes digitales ofrecen un rango mayor de velocidad de transmisión y mucho menos errores que una analógica.

Tecnología Celular.

La comunicación celular usa transmisores en una configuración de panal (honeycomb) para permitir el rehúso de una frecuencia de tiempo múltiple en un área pequeña. -- Útil en casos de fallas de la línea local.

Radio Digital.

Es un medio omni-direccional sin los requerimientos de alineamientos de las microondas terrestres o las comunicaciones satelitales.

Puede haber interferencia debido a obstrucciones por la línea del site, aunque éste problema debe ser vencido por medio del uso de repetidoras (de retención-envío), que reciban los datos o "paquetes" en cortas transmisiones de arranque.

Microondas

Se usa una antena parabólica para enfocar una estrecha onda dirigida para obtener una transmisión de alta velocidad.

Sujeta a retrasos de propagación sobre largas distancias.

Satélites.

Similares a las microondas terrestres, pero se utiliza un satélite como antena de transmisión.

Es una opción de bajo costo pero, la propagación de retrasos presenta algunos retos para las comunicaciones digitales con errores y control de flujo.

Sería un costo menor, usar medios alternos, tales como las microondas, implementar una estrategia de enrutamiento si, alguna falla ocurre en los enlaces o en la compañía telefónica.

Con estrategias de enrutamiento bien documentadas, se tendría un elemento clave para completar la estrategia de los respaldos de las redes de emergencia. Aún así, los requerimientos de ancho de banda de la red de emergencia, no pueden ser determinados sin la referencia de su uso actual.

Respaldos por medio de imágenes.

Desde luego, éstas, son apropiadas sólo para almacenamiento de información en formato electrónico.

Para convertir un documento o microficha en formato electrónico, debe ser escaneado (digitalizado) y convertido en una imagen en blanco y negro (o a color) formada por puntos llamados pixeles. Esta imagen debe ser almacenada electrónicamente y consultada por medio de una base de datos, para revisarse e imprimirse. Como información electrónica, el documento o microficha en imagen, debe ser transmitida vía electrónica y retenida en línea en el almacén exterior de datos (en inglés.-data vault).

Muchas empresas ya usan los sistemas de imágenes y bases de datos por funciones hechas previamente en archivos de papel o microfichas. Complementando con el almacenamiento exterior, de documentos legales originales ahora en formato de imágenes, es una manera efectiva para hacer que estos recursos estén disponibles a aquellos que deban accesarlos para seguir con los procesos de negocios en un caso de emergencia.

Respaldos en redes.

La figura (2-9) describe algunas de las actividades principales en ésta fase de la PLRD.

Como en los respaldos para sistemas, en las redes se busca primero, discernir las configuraciones de la red que dan soporte a las funciones clave de los negocios.
Finalmente, servicios y productos se seleccionan para incluirse en la PLRD.

2.5 *Manejo de garantías y políticas de mantenimiento.*

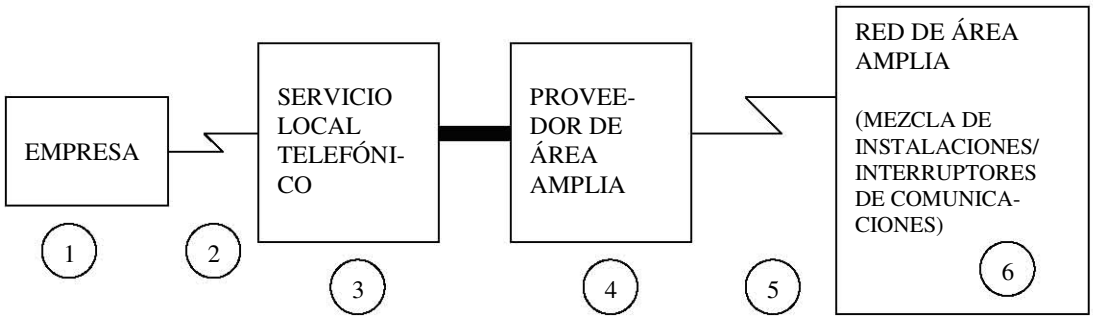
Desde luego, reparar y reemplazar por fallas a los componentes de la red es siempre una opción de recuperación. Los arreglos se pueden hacer con un equipo de respaldo para reemplazar los componentes.

Con los elementos identificados, que compondrán el plan de recuperación de la red, se deben considerar las opciones y sus respectivos costos. Esto implicaría primero a los contactos con el proveedor, y solicitar las cotizaciones de los precios.

Para identificar a los proveedores de servicios y productos para recuperación de redes, los encargados de la planeación deben ir a conferencias de recuperación de desastres, consultar artículos sobre redes, pedir visitas en otras compañías, hablar con los proveedores de telecomunicaciones, y consultar con profesionales de redes. Se deben investigar las características de muchos proveedores de éstos servicios.

Para obtener las cotizaciones de éstos servicios, se debe hacer cita con los proveedores y comentar la estrategia de recuperación, para que se describa en detalle, la función que el producto tendrá. El proveedor debe sugerir otras opciones que el encargado de la planeación no haya tomado en cuenta. Se debe solicitar una descripción del producto o servicio con su respectiva cotización. Agregar todo esto en la estrategia de recuperación de redes para una revisión posterior.

Una vez que se hayan recopilado los precios de diferentes proveedores, se deben documentar y así compararse, y hacer los cálculos de costos, por medio de un proceso de evaluación. Los resultados de estos procesos deben ser presentados al director administrativo, asegurándose de que los criterios de



1. INSTALACIONES DE LA EMPRESA, PBX, FALLA EN LAS INSTALACIONES DE DISTRIBUCIÓN.
2. CORTES DE LÍNEA O FALLAS DE ENLACE DE LA COMPAÑÍA LOCAL TELEFÓNICA.
3. DAÑOS EN LAS INSTALACIONES DE LA COMPAÑÍA LOCAL TELEFÓNICA.
4. DAÑOS A LOS SERVICIOS DEL PROVEEDOR DE LA WAN.
5. INTERRUPCIÓN AL ACCESO DEL GATEWAY.
6. INTERRUPCIÓN DE INSTALACIONES/INTERRUPTORES DE LA WAN.

Accesos típicos a las redes y sus posibles puntos de intersección.

Fig (2-9)

evaluación hayan sido bien definidos y que los beneficios y limitaciones de cada opción sean presentados para que todo quede claro.

También, es muy útil tener referencias de tres clientes de cada proveedor, y así documentar las experiencias que hayan tenido con los proveedores e identificar las similitudes y diferencias entre los requerimientos del cliente y los requerimientos de la empresa para la cual, la estrategia de recuperación ha sido planteada.

Después de esto, hay que asegurarse, que todos los contratos por servicios sean revisados por profesionales competentes y autoridades legales. Se tendrá que buscar si hay algún recargo oculto o cargos extras en instalaciones. Ver si existe una garantía confiable en caso de que el producto o servicio tenga alguna falla. También se debe solicitar una prueba antes de adquirir el producto. Cuando se seleccione un producto, se debe solicitar soporte para todos sus componentes o servicios. Y asegurarse de que el costo del soporte no expire antes de la presentación de la estrategia al director administrativo. Una vez que la mejor estrategia haya sido documentada, se deben identificar las tareas que se requieren para implementar la recuperación de la red. Estas tareas se dividirán en otras subtareas y procedimientos, una vez que la estrategia de recuperación de la red, sea presentada y aprobada por la administración.

Presentar los costos estimados por mantenimiento.

Los costos deben incluir los siguientes puntos:

- Un coordinador de mantenimiento.

Se necesita alguien para coordinar el mantenimiento y así asegurar el plan vigente de recuperación de desastre de la compañía, ya sea de medio o tiempo completo, tomando en cuenta su respectivo salario.

- Renovar el contrato del proveedor.

Las actualizaciones deben ser revisadas para determinar cuánto; los costos de productos y servicios de los proveedores, han subido o bajado, en la última década. Se debe hacer una estimación de costos sobre un período de varios años.

- Contratos de mantenimiento del hardware y software del plan de redundancia.

Los costos de proyecciones de hardware y software son notoriamente inexactos. Aún así, los acuerdos de mantenimiento en el centro de datos se deben referenciar para obtener una estimación del precio del contrato de mantenimiento. Entonces, ésta información puede ser relacionada a los costos de mantenimiento de hardware y software del plan específico de redundancia.

- Tomar en cuenta el entrenamiento en el presupuesto.

Se debe ver si existe la posibilidad de cambiar los requerimientos de entrenamiento a un departamento corporativo de entrenamiento. Si éste es el caso, el departamento de entrenamiento debe proporcionar un costo estimado. Si el entrenamiento va a ser conducido por personal de planeación, el presupuesto debe ser estimado, basado en los salarios y requerimientos de recursos.

- Pruebas en el presupuesto.

Diferentes tipos de pruebas tienen diferentes precios. Se deben calcular por lo menos dos pruebas al año para el hot site, y se debe preguntar al proveedor qué otros clientes están de acuerdo con sus costos. Se debe usar la estimación del proveedor como un punto de partida y añadir los detalles obtenidos en los requerimientos de pruebas de la empresa.

- Primas de seguros.

Determinar si algunos costos de aseguramiento se reducirán, una vez que el plan se establezca y que los sistemas de seguridad se instalen. Incluir los costos reducidos en el presupuesto de mantenimiento.

III. ESTRATEGIAS PARA UNA RECUPERACIÓN EFECTIVA DE SISTEMAS Y REDES.

Los encargados de la PLRD tendrán que confrontar sistemas no integrados, múltiples, o malhechos, a la hora de desarrollar una estrategia de recuperación.

Aún así, las mismas tecnologías que están disponibles para dar soporte a la integración y compatibilidad de aplicaciones para ambientes de producción, deben ser aprovechadas para desarrollar un sistema consolidado de recuperación de desastres. De manera resumida, esto es una configuración mínima de equipo.

El concepto de una configuración mínima de equipo debe ser aplicado en una variedad de diferentes formas, dependiendo de las preferencias y requerimientos del equipo de recuperación de desastres. En ésta situación, una configuración alterna debe consolidar múltiples aplicaciones en una sola plataforma. Por ejemplo, una LAN o un sistema multiusuario debe ser usado para servir a un número de aplicaciones normalmente utilizadas en PCs aisladas. Idealmente, el uso de código compatible (compatibilidad) en software diseñado para sistemas pequeños, facilitará su integración con una operación de una sola plataforma de mainframe en modo de recuperación de desastres.

Al principio, los encargados de la planeación necesitarán desarrollar una estrategia que abarque la recuperación de muchos sistemas. Muchos proveedores de sistemas de recuperación de mainframes hacen que todo lo anterior sea posible, de acuerdo a lo que el cliente requiera para sus sistemas. En todos lados hay servicios para consolidar la plataforma, que los encargados de la planeación deben aprovechar como puntos para reducir los costos y las complicaciones logísticas de la estrategia de recuperación.

Los encargados de la planeación deben alentar el establecimiento de un estándar corporativo, en la adquisición de tecnología y desarrollo de software que, ayudará a que las aplicaciones se cambien de muchos sistemas pequeños a una sola plataforma para propósitos de recuperación. Más aún, el equipo de la PLRD debe hacer disponible toda la información obtenida en sus análisis de riesgos y sus subsecuentes recopilaciones de datos, acerca de sistemas y redes para los encargados de sistemas de la compañía. Y es muy probable, de que no exista una base de datos, que describa todos los sistemas instalados, sus propósitos, y sus aplicaciones, dado el hecho, de que pocos proyectos tienen un enfoque de recuperación de desastres.

La hoja (3-1) nos da un ejemplo de formato de configuración mínima. En éste caso, el formato tiene un enfoque muy simple.

Tanto las aplicaciones como las unidades de red de trabajo que las utilizan están enlistadas en la forma. Entonces, para cada aplicación, se escriben los requerimientos de CPU, memoria y capacidad del disco duro. En la última columna se registran, los requerimientos especiales de la aplicación (pantallas especiales de video, dispositivos de entrada, periféricos, etc.). Basándose en ésta información, así como indicando el uso de la aplicación, se debe desarrollar una nueva configuración de hardware, combinando muchas plataformas en una sola.

El objetivo es consolidar las aplicaciones en pocas plataformas de computadoras. Entonces, los recursos de automatización serían ahora menos costosos y con pocas complicaciones logísticas.

Una vez que las aplicaciones críticas (incluyendo aquellas plataformas micro, mini y mainframes) hayan sido evaluadas, y las oportunidades para una configuración mínima de equipo hayan sido exploradas, se deben preparar los resúmenes de las estrategias ya consolidadas. Estos resúmenes dan los detalles de las configuraciones que serán instaladas en la locación de recuperación de usuario o en el site de respaldo del mainframe. Entonces, la forma incluye, un componente de recuperación de usuario de la estrategia de recuperación de sistemas, mientras que la figura será la base para seleccionar la mejor opción para respaldar el mainframe que se adecue a los requerimientos de la empresa.

HOJA DE CONFIGURACIÓN MÍNIMA DE EQUIPO. Fig (3-1)

INSTRUCCIONES: Use ésta forma para identificar los requerimientos del software para PC´s. Los requerimientos se deben resumir para definir una plataforma alterna y consolidar los requerimientos de la recuperación de hardware.

NOMBRE DE LA APLICACIÓN OTROS	UNIDAD DE TRABAJO	CPU/RAM	REQUERIMIENTO EN DISCO	
	RAM TOTAL			
TOTAL EN DISCO				

3.1Revisar la función de los sistemas.

Con el concepto de una configuración mínima de equipo bien definida fig. (3-2), se debe hacer notar que formular tal configuración de sistemas puede ser un reto técnico. Se requerirá que los expertos de la compañía y los proveedores, desarrollen la combinación más recuperable de plataformas independientes y sistemas combinados.

Éste proceso comienza con una revisión, de todas las funciones específicas de los sistemas identificados en la fase de análisis de riesgo. El encargado de la planeación debe inventariar al mainframe, las estaciones de trabajo y los sistemas de computadoras personales, para determinar si el trabajo que realizan es crítico, y determinar los parámetros de su uso, que permitirán que los sistemas múltiples se consoliden en menor número.

Sistemas basados en Mainframes, estaciones de trabajo, LANs y PCs .

Estos sistemas generalmente, por su naturaleza centralizada, dan un objetivo más simplificado para la recuperación. La mayoría de las PLRD actuales se enfocan en el proceso de recuperación del mainframe. Existen algunas empresas que dan soporte a un rango de estrategias para respaldos de mainframes. Para aprovechar los servicios de éstas compañías, primero, los sistemas del mainframe deben ser inventariados e identificar los componentes críticos de hardware.

También se están incrementando los casos en los que los mainframes son parte de grandes esquemas de proceso distribuido. Por ejemplo, los mainframes a menudo forman parte de LANs corporativas donde ofrecen bases de datos centralizadas o funciones comunes de almacenamiento.

Estas configuraciones de conectividad y sus propósitos deben ser claramente entendidos antes de que puedan ser distinguidas las configuraciones ya consolidadas del mainframe.

Igual que con los mainframes, con las estaciones de trabajo, se deben conocer antes de la instalación, las configuraciones y especificaciones de hardware.

La mayoría de las LANs corporativas proveen servicios básicos como correo electrónico, transferencia de archivos y aplicaciones de grupos de trabajo y de cliente-servidor. Si el análisis de una LAN revela que se está desaprovechando su uso principal, más que por acceder a una base de datos u otros tipos de procesamiento distribuido, entonces, sería posible quitar la LAN completamente del diseño del sistema de recuperación de desastre.

Algunos usuarios requieren PCs muy bien configuradas para realizar trabajos de misión-crítica, mientras que otros las usan para captura de datos, o para tener acceso a aplicaciones otorgadas por el mainframe. Se deben examinar las configuraciones de las PCs para determinar el trabajo que hace cada una y ver si es necesario incluirlas en la PLRD.

3.2 Identificando aplicaciones críticas.

Con las plataformas inventariadas, el siguiente paso para definir una configuración de recuperación total es revisando las aplicaciones críticas. La criticidad se ha determinado como parte de un análisis de riesgo. Los encargados de la planeación necesitan determinar qué aplicaciones deben continuar disponibles lo más pronto posible, y que otras no, después de una interrupción. Esto, determinará qué capacidades de los sistemas, deben estar disponibles inmediatamente y cuáles después, en el período de recuperación.

Identificando los periféricos requeridos.

Los sistemas no sólo constan de servidores, sino también de dispositivos periféricos para la entrada y salida de los datos. Algunos dispositivos, como los mismos servidores, son críticos y deben estar disponibles de inmediato para un caso de recuperación.

Fig (3-2) **CONFIGURACIÓN MÍNIMA DE EQUIPO.**

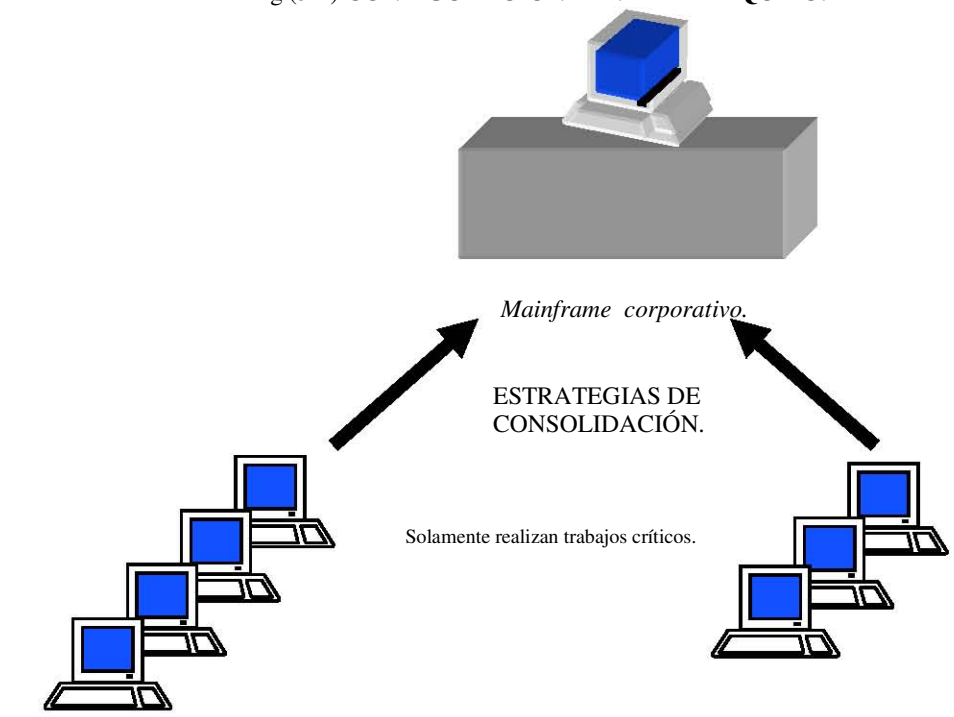
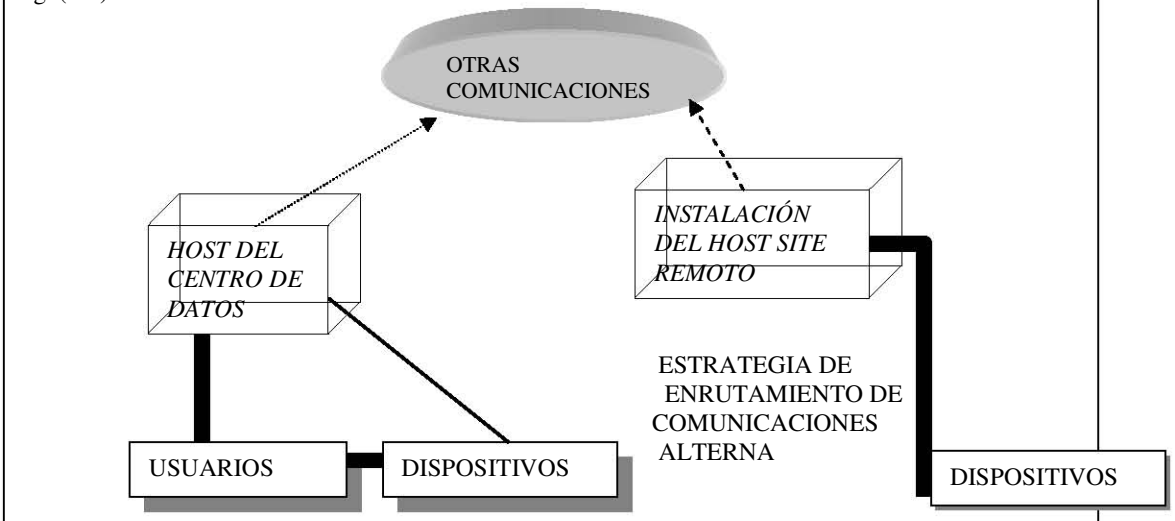


fig. (3-3) **ESTRATEGIA DE RESPALDOS "*HOT SITE*".**



Determinar los parámetros de uso.

El uso es donde la configuración mínima de equipo se pone a prueba. Además de tener un reemplazo físico o virtual para sistemas con los cuales los usuarios estén familiarizados, los

sistemas de recuperación necesitan tomar en cuenta otros factores relacionados a su uso. Estos factores incluyen el número de usuarios que tienen acceso a los sistemas, los requerimientos de acceso de acuerdo a las terminales y comunicaciones, y los requerimientos de disponibilidad para los sistemas.

Estructura principal de usuarios.

En la mayoría de los escenarios de recuperación no se permite un acceso total al sistema de todos los usuarios finales; por lo menos no al inicio del proceso de recuperación**.** Usando el perfil de uso de terminal, los requerimientos de recuperación de negocios y los datos de la inspección en función de negocios (vistos en capítulos anteriores), sería posible determinar el número de personas que servirían como equipo principal para tener las operaciones esenciales usando el sistema de recuperación.

El equipo principal puede ser seleccionado de diversas formas. Los encargados de planeación, podrían identificar números de usuario por aplicación, por plataforma o por área de trabajo. Para la planeación, éste número debe ser muy bien seleccionado, para que los accesos a los recursos estén bien administrados.

3.3 Las terminales mínimas para la red.

Con los usuarios asociados al sistema ya definido de recuperación, es necesario relacionar ésta información a los requerimientos de dispositivos de acceso. En otras palabras, los encargados de la planeación necesitan asegurar que el número de terminales o estaciones de trabajo, sea el necesario para que los usuarios puedan realizar un buen trabajo.

En muchos escenarios, se prefiere a las terminales tontas o a las PCs simples con software emulado desde una terminal por su amplia disponibilidad. Estaciones de trabajo altamente configuradas son más difíciles de usar, o más caras en los períodos de tiempo requeridos para la recuperación.

Requerimientos de comunicaciones de datos.

Las nuevas configuraciones requerirán también de nuevas comunicaciones. De hecho, hasta que se reinicien las labores, los usuarios, en la misma locación en donde se encuentren los sistemas de recuperación provisionales, deberán hacer algo del trabajo vía remota o con acceso dedicado. En algunos proyectos de planeación, los requerimientos para el acceso a las comunicaciones de datos, son registrados en éste punto para una consideración posterior bajo la planeación de recuperación de redes. En otros casos, es preferible documentar todo el hardware de comunicaciones de datos y alinear los requerimientos durante la fase de planeación de recuperación de sistemas, y es ahora cuando se pueden hacer las sugerencias y peticiones a los proveedores de servicios y productos de sistemas de respaldo.

Cambios en la agenda de trabajo.

Determinar el número de integrantes del equipo principal de la empresa, los requerimientos de los dispositivos acceso/terminal, y lo necesario para el acceso en comunicaciones de datos, es sólo una parte en la tarea para describir el uso del sistema de recuperación. Los encargados de la planeación deben considerar el uso de una agenda para los cambios que se den en el trabajo.

Las operaciones subsecuentes del sistema deben consistir en hacer procesos diariamente y realizar las funciones administrativas del sistema tales como los respaldos. En un modo de operaciones de emergencia, los usuarios deben administrar sus horarios para maximizar el uso del sistema mientras se minimizan los accesos a los recursos. La planeación en la agenda ayudará a los responsables de la planeación determinar la óptima configuración mínima de equipo; una configuración que permita realizar el trabajo crítico, y proceso administrativo.

Hot sites comerciales.

Una solución altamente confiable es la estrategia del hot site comercial. Los sistemas comerciales de respaldos, son instalaciones comerciales, donde se instalan los componentes del sistema, listos para usarse por empresas que pagan una suscripción mensual o anual.

Como se describe en las siguientes figuras (3-3) y (3-4), existen dos variedades de hot sites comerciales. En el hot site tradicional, la empresa se subscribe a una instalación designada donde se mantendrá un sistema de configuración específico. Un proveedor de instalaciones mayor, puede ofrecer una o más instalaciones alternas, entonces se puede ocupar la instalación primaria que se le ha asignado al suscriptor o habilitar el servicio hasta que el subscriptor se declare en desastre y el contrato sea invocado.

Como se muestra en la figura (3-4), la estrategia de los MIPS not sites supone la misma relación de subscriptor-proveedor. El suscriptor contrata a un proveedor, algún sistema de respaldo, ofreciendo varios sites de recuperación. La diferencia entre ésta variante y el arreglo del hot site tradicional es que no se especifica alguna locación de recuperación en el contrato de suscripción. Además, se aclara que la locación será propiedad del proveedor y escogida por él mismo.

Las diferencias entre estos dos acuerdos son pequeñas pero potencialmente significativas. La estrategia tradicional del hot site dispone del desarrollo de la afinidad entre el personal de la empresa cliente y los técnicos de la empresa que ofrecen el servicio y que ayudarán en el proceso de recuperación. Las pruebas son conducidas en el site diseñado, y el cliente con el proveedor trabajan juntos de la misma manera como si estuvieran en una situación de emergencia. Éste no sería el caso para los MIPS not sites.

También, en un contrato con un hot site, se puede hacer una auditoria en el site diseñado, para ver si no ha sido alquilado por muchas empresas, y ver si tiene demasiadas suscripciones o sin el equipo necesario para proveer la capacidad suficiente, necesaria para hacer los respaldos. Lo anterior es imposible de hacer en el caso de los MIPS not sites.

Finalmente, para empresas con necesidades especiales de equipamiento, la recuperación por medio de un hot site, tiene la ventaja de proveer un lugar para almacenar hardware de respaldo para redundancia. En los MIPS not sites, el equipo especializado debe ser transportado desde una locación central, con todo lo que el proveedor necesite para dar el servicio de respaldo. Esto puede retrazar la recuperación.

Shell Site (COLD SITE).

El shell site es básicamente una instalación lista para usarse, equipada con controles de energía, controles ambientales, y conexiones de redes, pero no tiene el equipo de cómputo instalado. Algunas empresas eligen ése espacio disponible para convertirlo en una instalación (shell) que puede ser ocupada en caso de que un desastre impacte las instalaciones principales.

Shell Site comercial.

Igual que el shell site de la compañía, un shell site comercial, está equipado con electricidad, controles ambientales y conexiones para redes, pero sin el equipo instalado. El costo para suscribirse a un shell site comercial es generalmente menor al costo de una suscripción de hot site. El equipo instalado en el shell site, puede ser cambiado a la instalación permanente del suscriptor, una vez que la instalación se halla preparado para ocuparse.

Los shell sites son frecuentemente ofrecidos por proveedores de hot sites y por compañías de renta de computadoras. Para los proveedores de hot sites, el cold site sirve como un amortiguamiento para compañías que se han retrasado en sus requerimientos de recuperación. El proveedor de hot sites requerirá que la empresa cambie de hot site a shell site después de un período de tiempo de arreglos.

fig. (3-.4) **ESTRATEGIA DE RESPALDOS "*HOT SITE*" (MIPS, not sites).**

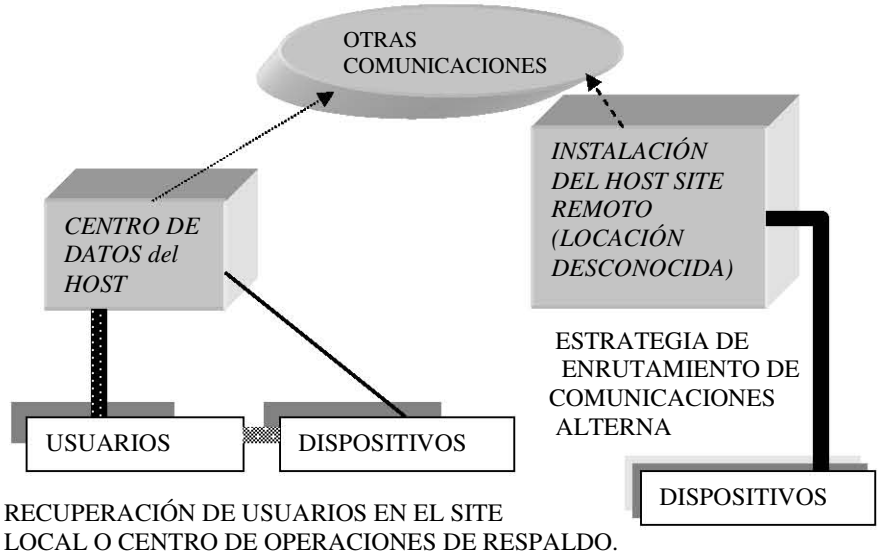
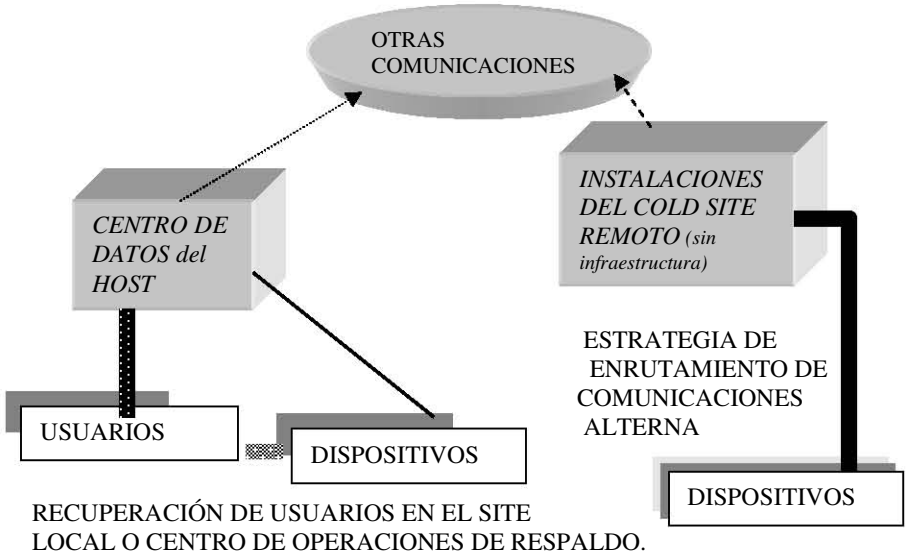


fig. (3-.5) **ESTRATEGIA DE RESPALDOS "COLD *O SHELL SITE*").**



Las compañías de rentas ofrecen un espacio con aire acondicionado y piso elevado para recuperación de desastres como un medio para rentar o revender equipo a sus clientes. Ellos prometen equipar la instalación con el hardware requerido en un período específico de tiempo, cuando el cliente experimente una emergencia.

Si se selecciona un shell site privado o comercial como una estrategia principal de sistema de respaldo, los encargados de la planeación deben tener cuidado de las limitaciones de su elección. Usando un shell site, excluye la posibilidad de probar previamente la implementación actual del sistema de recuperación. Más aún, el marco de tiempo de recuperación, está atenido a qué tan rápido el nuevo equipo puede ser ordenado e instalado en el momento del desastre.

3.4 *Hardware, ubicación y características geográficas de las instalaciones de la empresa.*

Una vez que una configuración mínima de equipo se ha documentado y definido, es necesario definir una estrategia para implementar una configuración en un site alterno.

Instalaciones alternas.

A la estrategia para el respaldo de la red, que ofrece una máxima confiabilidad para una recuperación completa en las operaciones críticas del sistema en un caso de interrupción; se le denomina redundancia. Como se describe en la siguiente figura (3-10), una estrategia de redundancia, plantea un segundo centro de datos para la compañía, que esté bien equipado para manejar las cargas de trabajo del sistema (aún en niveles de producción total o en niveles de emergencia), cuando el primer centro de datos se vuelva inoperable.

En la práctica, después de una interrupción, cambiarse a éste centro de datos alterno, implicaría horas o tal vez minutos. Todas las redes son duplicadas y cada site provee las instalaciones para que los usuarios finales puedan operar. La principal desventaja de ésta opción es su alto costo. De todas formas, no tendrán otra opción, aquellas compañías que sus aplicaciones críticas sean sensibles en extremo al tiempo. Por eso, hay que solicitar que los administradores revisen las diferentes ofertas de diversos proveedores de sistemas de seguridad, y alentarlos a que lo hagan lo más pronto posible para reducir los riesgos inmediatos de incendios, inundaciones, daños al equipo por contaminación ambiental, vandalismo o robo; que a veces las operaciones normales de negocios deben confrontar.

El caso más claro en la PLRD reside en una evaluación de riesgo del desastre y los correspondientes potenciales de pérdidas para la compañía. Se debe hacer notar que es difícil o imposible establecer una estadística confiable para saber la probabilidad de que exista un desastre que afecte a una empresa.

Para empresas establecidas en regiones propensas a huracanes o temblores, las estadísticas favorecerán aún más un desastre, en comparación con otras compañías localizadas en otras zonas geográficas relativamente aisladas de alguna amenaza natural.

La fuente de información en potenciales de riesgo debe incluir datos de protección civil, compañías de seguridad, las oficinas del proveedor telefónico, y sobre todo algún perito de construcción del edificio.

Entonces sería útil comprender, cómo es que la energía eléctrica y el servicio telefónico, son proporcionados al edificio de la empresa. Quiénes son los vecinos y si sus actividades también presentan algún riesgo, y cómo trabaja protección civil en la zona; todo lo anterior serviría para identificar otros potenciales de riesgo y así ayudar en encontrar un porcentaje más exacto y calcular la posibilidad de una interrupción más prolongada.

La culminación de ésta investigación no necesita ser sintetizada en una estadística. Sería suficiente dar un informe, con un porcentaje de riesgo más informal, para identificar a cada uno de los riesgos y poner pocos comentarios. De ésta forma avisar a la gerencia de la posibilidad de un desastre y de la necesidad de planear sin tratar el punto de qué probabilidades existen de que ocurra un desastre.

fig. (3-10) **ESTRATEGIA DE REDUNDANCIA COMPLETA.**

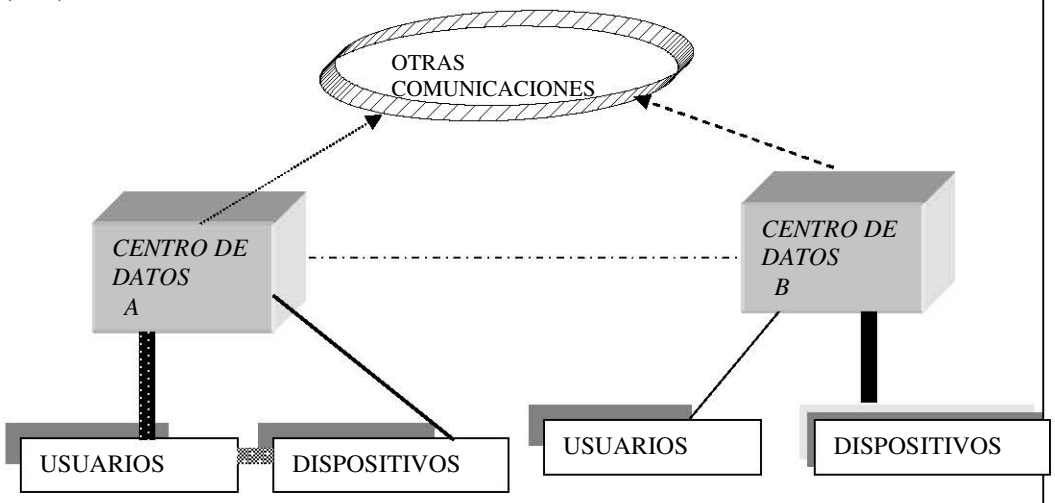
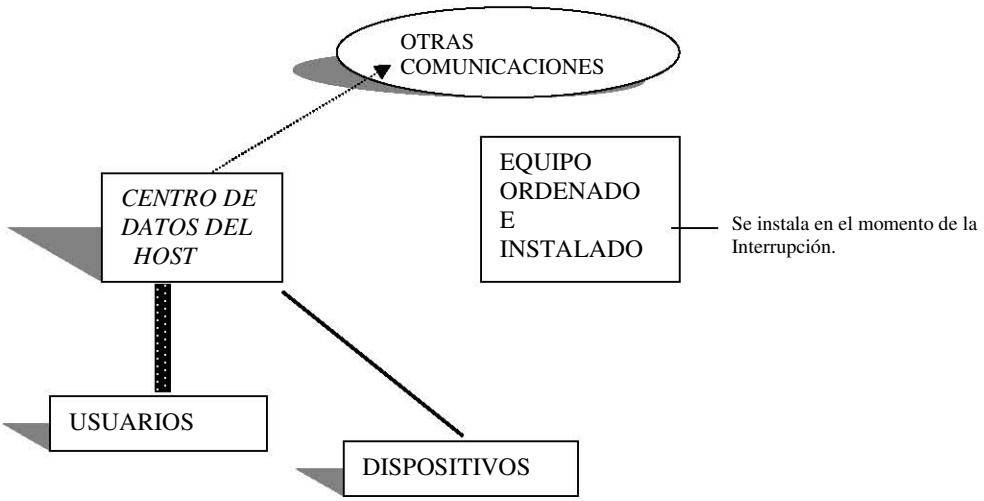


fig. (3-11) **ESTRATEGIA DE NO INTERVENCIÓN.**



Otro tipo de información que debe ser solicitada a los representantes del gobierno concierne a los riesgos naturales o hechos por el hombre que se puedan presentar por la cercanía de las instalaciones de la compañía. Si plantas de procesamiento químico o edificios nucleares se encuentran cerca de la compañía, los encargados de la PLRD deberán considerar un método obligatorio de evacuación. Por ejemplo, si una fábrica de químicos tiene un incendio y se

empieza a contaminar el aire, los oficiales encargados de mantener la seguridad deben evacuar áreas de empresas y hogares, por un período de tiempo hasta que el fuego quede controlado y comprobar que el riesgo ha terminado, si a una empresa, por el perímetro de evacuación, se impide el acceso a las instalaciones por varios días, se necesitaría aplicar la PLRD y temporalmente reinstalar sus operaciones a un centro de datos de respaldo. Este potencial de riesgo, que viene con la ubicación donde esté instalada la empresa, necesitará ser considerado en la PLRD, inspectores locales son generalmente la mejor opción para identificar tales potenciales de amenaza en el vecindario.

A algunos potenciales de desastres se les debe poner más atención en el proyecto de planeación debido a cuestiones ambientales. Por ejemplo, ciertas áreas geográficas son más susceptibles a huracanes o temblores que otras. Además de potenciales de desastre provocados por la naturaleza, la proximidad de la compañía con algunas fábricas que elaboren, procesen o almacenen cosas de peligro, como plantas de energía nuclear, pinturas y procesos químicos, etc., son detalles que deben ser considerados por los responsables de la planeación. Estos potenciales pueden ser mejor identificados con la ayuda de alguna institución de protección civil. Estas organizaciones por lo regular tienen información acerca de los peligros locales que pueden ser de gran ayuda.

Los encargados de protección civil deben ser consultados para poder realizar de manera correcta una evacuación en caso de que se requiera. Ya que éstos planes son típicamente desarrollados por estas organizaciones, en eventos como huracanes, temblores o desorden civil.

Los encargados de la planeación deben saber bajo qué condiciones se encuentran las instalaciones que deberán ser evacuadas y que procedimientos existen para volver a reinstalarse después del siniestro. Todos estos procedimientos deben ser tomados en cuenta para realizar el plan.

3.5 *Selección de proveedores y servicio de equipo*.

Con el hardware y prioridades de aplicaciones establecidas, el siguiente paso es contratar al proveedor especialista para identificar las oportunidades de integrar y consolidar los recursos en menos plataformas. En éste contexto, la integración se refiere a usar un simple servidor para operar varios sistemas. La consolidación se refiere a la combinación de múltiples aplicaciones corriendo en un ambiente de un solo servidor.

La integración es posible con un procesador poderoso, varias particiones y ambientes operativos. En muchos mainframes, se puede instalar UNIX en una partición, Windows 2000 en una segunda, un sistema operativo más simple en otra, etc. De ésta forma, las aplicaciones que normalmente operan en una variedad de sistemas pueden ser integradas en un solo servidor. Serían como varias máquinas virtuales operando en una sola unidad física. Esto ayudaría a minimizar el número de estaciones de trabajo o de PCs, que se necesitarían a corto plazo en la recuperación.

Por lo tanto, la consolidación ocurre cuando múltiples aplicaciones son llevadas a un sólo servidor, donde sus funciones se realicen aceptablemente por un período de tiempo. Por ejemplo, puede ser posible consolidar las aplicaciones, en múltiples sistemas pequeños, (como aquellos conectados a una LAN) estableciendo un sistema multiusuario en una sola estación de trabajo altamente configurada, teniendo como clientes varias estaciones de trabajo.

Desde luego, las opciones de integración y consolidación deben ser evaluadas en base a su facilidad de uso y economía de operación. De todas formas, los encargados de la planeación deben considerar la facilidad y familiaridad de uso de estas alternativas. Las nuevas configuraciones, aún económicas, no contribuirán a la recuperación si se requiere de una adaptación y aprendizaje significativo para los usuarios finales. En general, entre más familiar y similar se vea al sistema que reemplace, más fácil será realizar el trabajo que se requiera.

Documentando una configuración mínima de equipo.

Una vez que el análisis descrito anteriormente se halla realizado, la configuración mínima de equipo debe ser documentada. Hacer esto nos provee de un registro para las auditorias y pruebas igual que una "lista de compras", todo esto para negociar con los proveedores de servicios de recuperación de desastres.

Requerimientos de hardware.

Una descripción de los requerimientos de hardware, (parecido al inventario de hardware del centro de datos), se debe hacer para el sistema de recuperación. Eso, debe describir a los procesadores, dispositivos de almacenamiento, controladores y otros equipos requeridos para la configuración. Entre más específica sea la descripción, más fácil será equipar una instalación de respaldo, anticipando un desastre, o localizar un proveedor para suplir la configuración requerida en caso de una interrupción.

Requerimientos de software.

De manera similar al inventario del software del centro de datos, hay que enlistar todo el software que se requiera para la instalación de los sistemas. Es muy útil ver si los archivos del software son parte de datos incluidos en respaldos de sistemas rutinarios o si estarán contenidos en medios separados. También es importante indicar si una versión separada del software ha sido preparada para usarse con el sistema de recuperación.

Además de hacer una lista del software, será importante recalcar las referencias del software para los recursos del sistema y determinar si los requerimientos de todas las plataformas para la aplicación se han incluido en la configuración del sistema de recuperación. Una vez que el software de recuperación se ha definido, será esencial instalarlo como parte de una prueba para asegurar que no se hayan pasado por alto los requerimientos de la configuración.

Hay que hacer notar todos los requerimientos de software para los dispositivos de comunicaciones. Incluyendo el sistema operativo, la lista de nodos para los ruteadores, configuraciones para los repetidores, software PBX, software para módems, paquetes de emulación de terminales, etc.

Además hay que hacer notar cualquier cambio que se requerirá para la aplicación del software y facilitar la comunicación con entidades externas o nodos de otras compañías en el momento de un "reenruteamineto de redes", cambio de medios, u otra desviación de operaciones normales. Algunas aplicaciones, por ejemplo, pueden ser sensibles a retrasos de tiempo que se pueden acumular por el uso de satélites o transmisiones de tierra.

Estas aplicaciones necesitan afinarse para trabajar bien con las características de la red de recuperación.

3.6 *Requerimientos en las comunicaciones de datos*.

Se debe hacer una lista de los requerimientos de hardware para conectar los dispositivos de entrada y salida a los sistemas de recuperación. Dispositivos emuladores de terminales, equipos terminales (DSU/CSUs), repetidores, módems, equipo de interruptores, ruteadores, puentes, gateways, y otros dispositivos que deben ser incluidos.

También se deben calcular los requerimientos de ancho de banda para el acceso previsto, por medio de las comunicaciones de datos. Esto no sería posible hasta que una estrategia de recuperación a usuarios se haya formalizado. Los requerimientos de ancho de banda darán al proceso de planeación en la estrategia de recuperación de la red, qué tipo de líneas o instalaciones se requieren para recuperar las conexiones entre la locación de sistemas de respaldo y las otras unidades corporativas.

Requerimientos de usuario.

Éstos deben ser articulados en dos partes. Primero se debe hacer una contabilidad completa para los dispositivos de entrada/salida que serán utilizados por los usuarios del sistema. Esto debe ser bien definido por la unidad de trabajo, aplicación o servidor asociado al sistema. El método usado para conectar los dispositivos al servidor también debe ser mencionado.

Con la contabilidad de los dispositivos, los responsables de la planeación pueden articular los sistemas utilizando alguna agenda. La agenda debe indicar cuándo, la aplicación es utilizada, por quién y en qué base. La agenda debe ser lo suficientemente detallada para que los administradores del sistema puedan usarla para hacer un manual, identificando cómo los recursos serán destinados a un proceso en línea, y funciones administrativas con un proceso diario.

Las opciones de estrategias para recuperación de redes son pocas en número. Los paquetes de soluciones son raros y generalmente costosos. Típicamente, la estrategia de recuperación de redes incluye una mezcla de servicios de proveedores y preparaciones internas.

Opciones.

Las opciones en la estrategia de recuperación de redes son las mismas que se aplicarían a una recuperación de sistemas. Una estrategia de redundancia total, es la opción más cara y dispone de la máxima seguridad de éxito. Una estrategia de no intervención (sin tomar medidas de preparación), es lo menos costoso con la mínima seguridad de éxito.

Redundancia.

Claramente, cualquier estrategia de recuperación implica alguna redundancia. Ya sea que se identifiquen los caminos de enrutamiento alterno de las comunicaciones o el reemplazo del hardware. Desde luego que no todos los aspectos de la estrategia de redundancia, deben ser comprados por la empresa en el momento del desastre. Algunos proveedores de servicios están disponibles para proveer capacidades de redundancia después de la notificación de una interrupción.

Servicios alternos de redes.

De manera simple, la redundancia sugiere que una red alterna debe ser usada si una red primaria falla. En la práctica, éste escenario involucraría el cambio de la WAN privada de la empresa, a una red pública o una híbrida de algún proveedor, en caso de alguna interrupción. La mayoría de las áreas metropolitanas, están servidas por un número de proveedores de redes con un valor agregado, es decir, un servicio extra.

Se debe investigar con la compañía telefónica local o revisar periódicamente con otras compañías de la industria de las telecomunicaciones para identificar mejores proveedores. Hay que pedir una consulta para determinar el costo de ésta opción.

Enrutamiento bajo demanda

La mayoría de las compañías telefónicas locales, ofrecen un servicio de enrutamiento bajo demanda, es decir, de acuerdo a las necesidades. Éste servicio, se hace disponible en base a una suscripción y es facturado como parte de una cuenta mensual de una compañía de telecomunicaciones. Se debe contactar a algunos proveedores de éstos servicios.

Notificación de enrutamiento.

Además del enrutamiento bajo demanda, algunas centrales telefónicas y proveedores de redes con valor agregado, ofrecen servicios de enrutamiento en base a una membresía. En otras

palabras, sin cargos de suscripción. Para obtener el servicio, la empresa debe contactar con el proveedor cuando el servicio se requiera, y esperará por un intervalo estándar, para que sean implementados los nuevos enlaces de redes. Puede ser difícil de obtener el enrutamiento, sobre todo en situaciones de desastres regionales. En estas instancias, muchas compañías contactarían con el mismo proveedor al mismo tiempo, lo que implicaría hacer cola para obtener el servicio. Contactar con el proveedor o compañía telefónica local para más información.

Dependiendo de los requerimientos de la empresa cualquier propuesta debe ser factible. Aún así, las empresas deben ser cautelosas a la hora de firmar cualquier acuerdo, que prometa la capacidad de respaldo que no pueda ser demostrada por su disponibilidad o capacidad.

Arreglos recíprocos.

Los arreglos recíprocos son acuerdos establecidos entre dos compañías, en las cuales una promete dar respaldo a la otra en una emergencia. Estos acuerdos son difíciles de probar y generalmente se consideran inadecuados en la tarea de respaldar sistemas complejos y redes.

Reemplazos (Baja confiabilidad).

Los reemplazos, a menudo son llamados estrategia de no intervención (sin ninguna preparación), debido a que son una estrategia de baja confiabilidad para respaldar los sistemas. Como se describe en la siguiente figura (3-11) éste alcance supone el reemplazo de hardware, software, y de instalaciones en el momento de la interrupción.

Ésta opción de estrategia no solamente es imposible de probar, también falla en las auditorias, lo cual casi equivale a no poder hacer nada en el momento del desastre.

Asignando costos a las opciones.

En general, entre mayor sea el nivel de confiabilidad asociado con la estrategia, la estrategia costará más. La redundancia total es la estrategia más cara y proporciona la más alta confiabilidad para el éxito en una situación de recuperación de desastre. En contraste, una estrategia de no intervención es lo menos costoso, pero otorga la menor probabilidad de éxito.

Como se ha comentado, el encargado de la planeación de desastres deberá balancear los costos de la estrategia, confrontando con los costos extras que se puedan presentar en el momento del desastre. Los gastos de dinero no deben excederse y poner en riesgo a la empresa.

Por ésta razón, se ha incrementado el número de compañías que han adoptado la estrategia del hot site comercial de respaldo. Los hot sites, aunque son caros, casi siempre son tolerables, y estos costos pueden ser legitimados bajo la mayoría de los análisis de costo-beneficio. Para seleccionar una estrategia con hot site apropiada, se deben tomar en cuenta los siguientes pasos:

Contacto con los proveedores.

Se puede obtener una lista de proveedores, en algunas publicaciones de tecnología y telecomunicaciones. Éstas empresas y sus historias exitosas de recuperación, se publican en éste tipo de revistas y se requiere de un mínimo esfuerzo para identificar varios candidatos calificados. Además, los proveedores de hardware y software pueden sugerir algún proveedor de hot site si se les pregunta.

Los primeros contactos con el proveedor, se llevan a cabo con visitas al site, de algún representante de éstos servicios. Existe mucha competencia entre los proveedores de hot sites, entonces los representantes intentarán dar una muy buena impresión con el cliente.

Cotizaciones.

Después de haber contactado con los proveedores y sus propuestas, se les debe dar en resumen los requerimientos para una configuración mínima, y pedirles el precio estimado para una solución de hot site.

Documentar los costos.

Cuando se reciben los precios de varios proveedores, se debe hacer una hoja de comparaciones, resumiendo las ofertas y precios de cada vendedor. Documentando los costos, el encargado de la planeación puede comparar las diferentes ofertas. Esto puede servir como medio para estimar los costos adicionales asociados con la estrategia de aplicación de un hot site en el caso específico de la empresa.

Visitas a sites calificados.

Se deben visitar los sites de los proveedores considerados en la vuelta final del proceso de evaluación. Las visitas al site del proveedor, confirmarán los hechos de las ofertas del proveedor, y darán a los encargados de la planeación una mejor apreciación de cómo la locación del hot site deberá accesarse en el momento de la emergencia.

Revisar referencias.

Los proveedores están preparados para dar referencias a sus clientes. Suponiendo que éstas referencias son los mejores informes del proveedor, también es importante solicitarles información acerca de la calidad de servicio, la frecuencia y tipos de pruebas que llevan a cabo, la participación del proveedor en las pruebas y otros hechos del rendimiento de la solución.

Por lo menos, se deben entrevistar tres referencias. Los encargados de la planeación deben pedir más referencias con la competencia, compañías similares o con configuraciones de respaldo parecidas. Se deben documentar todas éstas referencias cuidadosamente para una revisión posterior.

Revisar contratos.

Revisar los acuerdos de los términos con el proveedor del hot site, muchas políticas deben ser discutidas específicamente en el acuerdo, y adelantarse en las siguientes secciones. Si éstas políticas no se discuten, averiguar porqué no se puede y obtener un documento escrito de ésta política como un adelanto del acuerdo.

Muchos puntos deben ser resueltos por adelantado en la negociación del contrato del hot site.

Esto incluye lo siguiente:

- Identificar cuál es la posición del proveedor en el contrato de servicio de suscripción.
- Determinar si un site específico está diseñado para pruebas y respaldos.
- Determinar si el site es reservado sólo para suscriptores o si a otros clientes se les a otorgado el acceso en una emergencia.
- Identificar cada cuando se hacen pruebas, si se dan cada año y a qué costo, y qué tipo de soporte se espera de parte del personal técnico del proveedor.

Las respuestas a estas preguntas proporcionan diferencias tangibles que facilitarán una decisión más clara para elegir entre los proveedores con ofertas de servicio comparables.

3.7 *Políticas en las instalaciones*.

Como un servicio de suscripción, los hot sites son comúnmente contratados por muchas compañías al mismo tiempo. Esto se hace para reducir los costos de los servicios a todos los suscriptores, para obtener del proveedor el máximo beneficio y tener ganancias por los servicios de actualizaciones y mantenerse con la última tecnología.

El encargado de la planeación debe obtener un estado de cuenta claro del proveedor, debido al número de empresas registradas en la plataforma de recuperación que se ha ofrecido. Observar si hay alguna indicación, de que el proveedor busque compartir las particiones con la misma plataforma con otras empresas o con su propio sistema. Se debe buscar obligatoriamente la solución de un sistema dedicado, exclusivo para la empresa.

También se le debe preguntar al proveedor, cuántas compañías se encuentran registradas al mismo sistema contratado por el encargado de la planeación y en la misma zona geográfica. Éste es un detalle a tomar muy en cuenta si un desastre regional afectara a muchas empresas en la misma zona.

Otra lista de servicios comúnmente otorgados por proveedores de recuperación comercial.

Los encargados de la planeación deben preguntar a los proveedores acerca de otros servicios otorgados por la compañía.

Los servicios de interés deben incluir:

- Soporte para recuperación de sistemas sin mainframes.
- Servicios de Shell site (cold sites).
- Pruebas del plan y servicios de mantenimiento.
- Servicios de recuperación de redes y telecomunicaciones.
- Servicios de centro de operaciones de respaldo para recuperación de usuarios.

Solicitar ofertas.

Una vez que el campo de selecciones ha sido investigado, se deben solicitar ofertas formales a cada proveedor. Esto es para que los proveedores den sus mejores precios de ofertas. De ésta forma, se pueden evitar, los injustos procesos de última hora, de ajustes de precios.

Documentar la estrategia preferida.

Si se ha preferido a un hot site u otra estrategia de respaldo de sistemas, la opción seleccionada y las razones de su selección (incluyendo el análisis de ofertas del proveedor) se debe documentar escrupulosamente. Esto permitirá que el encargado de la planeación se defienda en contra de cualquier reto administrativo subsiguiente debido a la estrategia seleccionada y a los procedimientos de evaluación de ofertas.

Una vez que la estrategia se ha identificado, se puede presentar a la gerencia para su aprobación. Cuando se apruebe, el encargado de la planeación se pondrá a identificar las primeras tareas que deban hacerse, que deben ser llevadas a cabo para realizar los puntos de la estrategia en una emergencia. Éstas tareas y sus procedimientos relacionados se incluirán en una sección del documento de planeación.

Conclusiones.

Las estrategias de recuperación de sistemas vienen en todas las variedades de gastos y complejidad. La estrategia apropiada para cualquier empresa, es la estrategia que dará la restauración de las funciones mínimas aceptables, periodos de tiempo, y costos.

Se debe tener en cuenta que las estrategias de recuperación de sistemas no son como recetas de cocina. Están inexorablemente relacionadas al usuario final, y a estrategias de recuperación de redes que deben ser revisadas siempre que ésta u otras estrategias, sean completamente articuladas.

3.8 *Seleccionando a un proveedor de almacenamiento externo (off-site)*.

Algunas de las consideraciones básicas para seleccionar un proveedor para almacenamiento externo se muestran en la siguiente lista, más adelante se explicarán con mayor detalle:

MEDIOS.

¿El proveedor puede manejar el volumen y los tipos de medios que la compañía debe almacenar?

INSTALACIONES.

¿Las instalaciones del proveedor cuentan con estándares de diseño y protección?

TRANSPORTE.

¿Los medios serán transportados al site del proveedor de manera segura?

PERSONAL.

¿El personal del proveedor cuenta con entrenamiento y experiencia en técnicas propias de manejo de medios de almacenamiento?¿ El personal está sujeto a revisiones de seguridad periódicas?

SEGURIDAD.

¿Están instalados de manera adecuada los controles de acceso físicos y cuentan con acceso restringido al personal del proveedor?

ACCESO.

¿Se proporciona un acceso las 24 horas?¿Qué se necesita para asegurar los datos cuando se requieran?

SOPORTE LOGÍSTICO.

¿El proveedor ofrece soporte en la implementación o desarrollo del plan?

Son siete las áreas a evaluar con cualquier oferta de proveedores de almacenamiento externo:

1. Medios- A veces el problema son cintas que no se pueden usar y pueden ser la causa principal de fallas en las pruebas en el PLRD y son una fuente de retrasos en la recuperación en situaciones de desastre.

Los proveedores de almacenamiento externo deben ser evaluados en sus habilidades para proporcionar un ambiente requerido para el almacenamiento prolongado de cintas y para

mantener los medios apropiadamente mientras se almacenan. Para evaluar los controles ambientales de las instalaciones de almacenamiento es conveniente ver si los proveedores cumplen con algunos requisitos, y a menudo ofrecen certificados en los que se corrobora el cumplimiento de algunas normas y reglas de almacenamiento.

Los encargados de la planeación deben asegurarse de que los dispositivos de almacenamiento sean regresados periódicamente al centro de datos y que las pruebas de restauraciones sean conducidas usando ésos medios.

2. Instalaciones- Los estándares formales para el almacenamiento de cintas implican o enumeran pautas específicas para el diseño de las instalaciones de almacenamiento. También existen estándares para la construcción de las instalaciones. Tales estándares incluyen estructura de paredes contra fuego, tipos de alarmas para desastres y sistemas de supresión que deben ser empleados, niveles de temperatura y humedad que deben ser mantenidos, y consideraciones locales como la altitud, proximidad a aeropuertos, etc. Los encargados de la planeación deben evaluar varias instalaciones de almacenamiento en base a los estándares y reglas de construcción impuestas por reglas locales.

3. Transporte- Los medios de almacenamiento son en su mayoría vulnerables al ser transferidos de la compañía a la instalación de almacenamiento. La mayoría de los proveedores ofrecen su propio servicio de transporte. Entonces hay que asegurarse de que los vehículos de transporte estén equipados para mantener las condiciones ambientales apropiadas para los medios que se transporten, y que tengan sistemas contra fuego.

4. Personal- El personal que transporta, maneja y mantiene el almacenamiento, requiere entrenamiento especial en el manejo de medios, y debe estar sujeta a revisiones de seguridad. Los proveedores deben comprobar que han tomado medidas para asegurar que las grabaciones almacenadas y otros medios no estén abiertos, vendidos u alguna actividad relacionada con el personal del proveedor de haber otorgado los medios o grabaciones a la competencia o a personas sin autorización. También deben asegurar que el personal del proveedor tiene los conocimientos y habilidades para prevenir algún daño a las grabaciones almacenadas y otros medios.

5. Seguridad- Los controles de acceso físico y medidas de seguridad electrónicas (en el caso de cajas de seguridad con información en medios electrónicos), deben ser bien escudriñados por el equipo de la PLRD. El proveedor debe demostrar que los medios y grabaciones estén seguros cuando se almacenen y durante su transporte. Los encargados de la planeación, deben tener cuidado de no contratar a proveedores que permitan el acceso sin supervisión a las áreas de almacenamiento a personal externo u otros clientes. Muy importante también, es que el proveedor se comprometa legalmente por medio del contrato, de compensar al cliente por pérdida, daño, o divulgación de las grabaciones e información.

6. Acceso- Así como se debe restringir el acceso de datos y grabaciones sólo a personal autorizado y acompañados por un supervisor de los proveedores, también el acceso debe ser lo suficientemente flexible para permitir el acceso a las grabaciones y medios en una emergencia. Los proveedores deben permitir la designación de solicitantes autorizados que pidan la entrega (o la obtengan en persona) de las grabaciones y medios requeridos en una situación de recuperación. Ese acceso debe estar disponible las 24 horas. Debido a eso, los bancos y negocios con cajas de seguridad con horas normales de servicio son a menudo excluidos para considerarse como proveedores de almacenamiento externo.

7. Soporte logístico.- Muchos proveedores están empezando a ofrecer sus servicios con la intención de ofrecer sus servicios de almacenamiento a los requerimientos específicos del plan de recuperación del cliente. Por ejemplo, algunos proveedores ofrecen desarrollar y mantener una parte del plan de recuperación relacionada con los programas de almacenamiento externo, usando su propio sistema de computadoras y llevar los cambios de los

medios almacenados con información de acuerdo a su agenda para mantener de manera apropiada la lista de peticiones del cliente. Otros facilitarán el transporte de los medios a los mainframes remotos o la instalación de respaldo del usuario, manteniendo las cajas de almacenamiento en el site, que serán rápidamente bajadas y entregadas por el proveedor al aeropuerto local para su envío. Estos servicios por lo general tienen un costo adicional, así que los encargados de la planeación deben evaluar ésos servicios adecuadamente para asegurar que sean comprados los servicios apropiados para dar soporte a los requerimientos de la PLRD.

Tipos de proveedores de almacenamiento externo.

Existen muchos tipos de instalaciones para el almacenamiento externo. Compañías de servicios de almacenamiento y transporte, instalaciones de almacenamiento comerciales, instituciones financieras, compañías especializadas en almacenamiento de información y grabaciones, bunkers a prueba de bombas que se utilizan como locaciones de almacenamiento.

Generalmente, las empresas en la mayoría de las ciudades tienen una variedad de proveedores de almacenamiento externo de dónde escoger. Las empresas localizadas en pequeñas ciudades que carecen de instalaciones comerciales con éstos servicios, deben hacer acuerdos cooperativos con otras empresas.

Se debe asumir que, las grabaciones e información almacenada de manera externa, no se vea afectada en un desastre local, como un incendio que consuma a la empresa. Aún así, los desastres regionales pueden hacer que la información, las grabaciones locales y lo almacenado de manera externa estén propensos a perderse.

Solicitando ofertas y evaluando opciones.

Un proceso formal de especificación y evaluación de ofertas es una buena regla para seleccionar al proveedor. Siguiendo la definición de los requerimientos de almacenamiento y la identificación de muchos proveedores potenciales, el equipo de la PLRD debe solicitar sus ofertas.

Los proveedores deben responder con: propósitos de sus servicios, un contrato, y los nombres de muchos clientes para usarlos como referencias y contactarlos para obtener información adicional acerca del rendimiento del proveedor. El proveedor debe proporcionar lo siguiente:

1. Certificaciones de sus servicios de acuerdo con los estándares para los medios de almacenamiento y normas de construcción apropiadas.

2. Certificaciones de garantías y/o aseguramiento.

3. Descripciones de entrenamiento de empleados y medidas de seguridad del personal.

4. Una agenda provisional para el transporte de medios y mantenimiento, con todos sus costos claramente indicados.

Una vez que la documentación se haya recibido, el equipo de la planeación debe seguir las certificaciones con las respectivas autoridades y buscar en la historia de la organización, sus prácticas pasadas en los negocios.

Otro paso obvio es consultar con otros clientes para obtener referencias del proveedor. Preguntar por, cómo se lleva el contrato, qué volumen de almacenamiento se tiene para el cliente, qué desventajas tiene el proveedor, etc. Los encargados de la planeación deben esforzarse para obtener una imagen completa de cuáles son los requerimientos de los otros clientes y así, compararlos con los propios, y ver cómo el proveedor otorga ésos servicios.

Finalmente, el equipo de la planeación debe organizar visitas a cada una de las instalaciones del proveedor. En las visitas se debe incluir inspección en los vehículos de

transporte, en las instalaciones y en mantenimiento de equipo, también los arreglos con gerentes y equipo.

Documentando las ofertas.

Para propósitos de auditorias, es muy benéfico documentar las decisiones del equipo de planeación acerca de los proveedores. Cada miembro del equipo involucrado en la selección del proveedor, puede escribir un texto breve, resumiendo sus observaciones acerca de los proveedores competentes y recomendando a un proveedor en específico.

A final de cuentas, la decisión acerca de cuál proveedor contratar no debe estar basado estrictamente en el precio. La calidad de las instalaciones del proveedor, servicios, personal, etc. se deben discutir en favor de contratar a un proveedor más confiable, aunque casi siempre éstos son los más caros.

El líder del proyecto será requerido para dar la decisión final del proveedor a contratar, tomando en cuenta las recomendaciones de los miembros del equipo, sus observaciones y las limitaciones del presupuesto en el proyecto de planeación. El líder del proyecto también debe negociar los precios en el contrato.

Finalmente, se debe conservar una provisión para el almacenamiento externo inicial, y para las auditorias regulares que lleve a cabo el proveedor. Los pasos iniciales incluyen, llevar a cabo algunas citas con los usuarios de los diferentes departamentos para avisarles de los horarios y fechas en las que se llevarán a cabo los procedimientos para recoger los medios con la información, además de su entrega y demás tareas de emergencia, y para asignar responsabilidades a personas específicas en cada una de sus unidades de trabajo. Al principio, se debe monitorear el momento en el que se realizan los traslados de la información hacia los sites externos, para asegurarse de que las partes responsables estén participando, y que todos entiendan lo que se tenga que hacer.

Los planes también deben ser realizados para probar el programa de almacenamiento externo en una base diaria. El contrato con el proveedor debe ser revisado en intervalos regulares, para asegurarse de que se hayan cumplido los horarios de la agenda, que se hayan usado los vehículos apropiados, y que las instalaciones donde se almacena la información, no se hayan deteriorado. El plan de almacenamiento externo debe ser probado, avisando o no, al proveedor. Se debe asegurar que las pruebas del PLRD incluyan la adquisición de respaldos, refacciones y otros materiales almacenados de manera externa con el proveedor. Se debe simular una emergencia y observar cómo el proveedor se desempeña al entregar sus servicios de emergencia.

Existen muchas variaciones para representar la manera en que se hacen los respaldos por medio de un almacenamiento externo. En algunos casos, las empresas eligen almacenar sus respaldos permanentemente en su site del mainframe de respaldo. Un proveedor de servicios de mainframe de respaldo, recomienda que los respaldos del sistema operativo, que hayan sido hechos en el transcurso de una prueba formal de la PLRD, deben ser guardados en las instalaciones de respaldo y actualizados solamente cuando se realice otra prueba. Asumiendo que las pruebas se llevan a cabo muy frecuentemente, o cuando se haga un cambio al software del sistema, ésta estrategia tiene un mérito considerable.

Otra de las variaciones involucra los requerimientos de almacenamiento externo de las unidades de trabajo, cuando las unidades de trabajo están distantes entre si. Es muy posible que se necesiten varios proveedores y que los gerentes de las unidades de trabajo necesiten evaluar y seleccionar sus propios proveedores y análisis de requerimientos. Cuando éste es el caso, el equipo de planeación necesitará documentar los avisos, para que los administradores de las unidades de trabajo participen en la evaluación y selección del mejor posible proveedor para el trabajo. Entonces, deberán obtener copias de los contratos y de las listas de almacenamiento de cada unidad de trabajo y asegurarse de que los gerentes estén revisando constantemente sus estrategias de almacenamiento.

El almacenamiento externo y la instalación de las capacidades de prevención de desastre son claves para reducir las probabilidades de un desastre sin una recuperación posible. Si el

equipo de planeación se encarga de llevar a cabo estas dos fases de la PLRD, será una contribución substancial a la integridad de los negocios de la empresa.
Los respaldos efectivos y los programas de almacenamiento externo son críticos en cuanto al tiempo de restauración de las funciones de los negocios, en el momento de un desastre. Estos programas se acoplan individualmente con las estrategias para los sistemas, redes, y recuperación para el usuario final, y deben ser revisados en el contexto de los requerimientos de recuperación asociados con estas estrategias, una vez que se hayan formalizado.

Preguntas para seleccionar a un buen proveedor.

1. ¿Cuánto tiempo ha trabajado el proveedor en ésta área?

2. ¿Cuántos clientes tiene el proveedor?

3. ¿El proveedor ha realizado cotizaciones de trabajo o a proporcionado productos a otras compañías de la misma área?

4. ¿Tiene el proveedor licencia y garantía?

5. ¿Qué certificaciones tiene el proveedor (asociaciones técnicas o profesionales, aprobaciones del gobierno, etc.)?

6. ¿El personal del proveedor tiene entrenamiento especial, certificado o con licencia?

7. ¿Tiene el proveedor garantía de trabajo y cuáles son sus condiciones?

8. ¿El proveedor tiene los manuales o libros de todos sus productos que se usarán?
Ver si ésos productos cumplen con los estándares de la industria.

9. ¿El cliente otorga información de referencia de otros de sus clientes?

10. ¿Los vendedores y representantes técnicos del proveedor tienen los conocimientos necesarios?

11. ¿Los representantes se ven comprometidos con los requerimientos operativos de los negocios y si seguirán al pie de la letra los horarios determinados por éstos requerimientos?

12. ¿Qué es lo que ofrece el proveedor? ¿También se incluye en el contrato el mantenimiento en el site?

13. ¿Tiene el proveedor entrenamiento para el personal del cliente?

14. ¿El proveedor ofrece soporte en forma de mantenimiento preventivo periódico o inspecciones al site después de haber contratado sus servicios?

Resumen.

3.9 *Recomendaciones importantes.*

Instalar sistemas para evitar desastres.

Es recomendable adelantar un plan para instalar un sistema de seguridad y así minimizar alguna interrupción posible. Incluyendo subtareas como el entrenamiento clave del personal que utilizará éste sistema.

Contratar un servicio de almacenamiento exterior.

Hay que enfatizar que la implementación de un servicio de almacenamiento exterior, representa una excelente reducción de costos-riesgos. Subrayando también que los sistemas y las redes se pueden reconstruir fácilmente, pero la información crítica de la empresa se puede perder para siempre si no se respalda y almacena en algún lugar externo.

Formalizar y articular una agenda para almacenamiento externo.

Con un proveedor de almacenamiento externo seleccionado, explicar cómo, el soporte administrativo se requerirá para asegurar el mejor uso posible del programa. Enfatizar que los administradores y empleados requerirán de una orden de parte de la gerencia en algunos casos para cambiar sus prácticas habituales y trabajar en un nuevo programa. Explicar cómo la agenda propuesta no interferirá con la productividad.

Desarrollar procedimientos para recuperar sistemas críticos.

Tener una estrategia, que proporcione el mejor servicio en sistemas de recuperación al costo más bajo no significa que también se halla desarrollado la implementación del sistema cuando se necesite. Se requerirá de tiempo para formalizar los procedimientos y probarlos.

Contratar un servicio de recuperación de sistemas.

Asumiendo que un site de respaldo en frío o en caliente es la estrategia óptima para la compañía, se debe presentar el contrato a los gerentes para que lo revisen y firmen. Indicar que una junta o una visita al site puede ser presentada con el proveedor si los gerentes lo desean. Indicar el período de tiempo de compra del servicio al precio establecido.

En un sistema de cómputo:

En primer lugar, los datos generales (como los inventarios de hardware y software, diagramas de configuración, especificaciones de aplicaciones) deben ser recopiladas para el personal del proyecto de la PLRD. Muy importante también es la información del propio centro de datos, incluyendo subsistemas de soporte, instalaciones de disponibilidad y diseño, locaciones del equipo e interconexiones, controles de acceso físico y sistemas de prevención de desastre instalados.

Se debe mantener el cableado de terminales de redes de trabajo y también las conexiones que utilizan los usuarios vía remota. También son de interés los recursos de cómputo descentralizado y las redes de área local.

Esto significa que hay demasiada información, pero ésta debe ser útil solamente en el contexto de planeación de recuperación en función de negocios, que debe ser reorganizada de acuerdo a los requerimientos de recursos que se necesiten.

Una PLRD no tiene como objetivo recuperar todo en su forma original, en vez de eso, se busca mantener una organización eficiente y temporal diseñada para mantener los requerimientos necesarios hasta que la crisis termine. El objetivo principal es recuperar las configuraciones mínimas tanto de redes como de sistemas que darán soporte a los requerimientos específicos para funciones de negocios que han sido identificados como críticos y vitales.

Para facilitar esto, el equipo encargado de la planeación necesitará saber qué aplicaciones y su respectivo hardware, están directamente relacionados a las funciones específicas de los negocios, con lo cual se ahorrará tiempo y dinero.

Para identificar cuáles aplicaciones son las más necesarias se deben consultar muchas fuentes de información. Pero con los sistemas de administración de bases de datos (DBMS) debe ser relativamente fácil distinguir la información necesaria, en el caso de una restauración total del sistema, debe ser eficiente en tiempo y recursos para separar lo innecesario de la información vital, de los recursos críticos. Dado en casos en que los sistemas sean muy antiguos, seria muy difícil separar la información, entonces se tendría que restaurar el sistema en su totalidad. En áreas donde existan sistemas descentralizados es más difícil la recuperación. Todo se dificulta debido a que se tienen varios sistemas pequeños, cada uno corriendo su propio sistema operativo, diferentes programas y aplicaciones administrativas. Caso contrario a las áreas centralizadas donde la recuperación es muy sencilla.

Por lo tanto, los recursos de computadoras descentralizadas deben ser reunidos, revisados y cuidadosamente probados para ver si son necesarios para los propósitos de la empresa. Una vez hecho todo esto, es decir, que los sistemas descentralizados se hayan identificado, sus operaciones hayan sido validadas, y la documentación arreglada, los encargados de la planeación deben ver si existe la posibilidad de hacer compatibles las aplicaciones descentralizadas asociadas con las funciones críticas y vitales a un sistema centralizado. La razón es simple: entre mayor sea el número de aplicaciones descentralizadas, que se puedan hacer compatibles y así centralizarse; en un caso de emergencia, será menor el número de PCs que se necesiten al realizar la PLRD, y así reducir tiempo y costos.

Las aplicaciones del software deben ser legibles independientemente de las diferentes plataformas que se tengan para facilitar la comunicación entre las aplicaciones, nuevos dispositivos y diferentes tipos de terminales.

Los archivos de información deben estar en un formato compatible con el sistema de operación de destino.

Aunque esto es más complejo de lo que parece, todo esto debe ser examinado meticulosamente y es una tarea más en el esfuerzo para reunir la información.

En una red:

Todo lo anterior también se puede aplicar a transmisión de voz y redes de comunicación de datos. A los cuales se les ha incrementado su uso en soporte. Las configuraciones y descripciones de operación de redes deben ser obtenidas. Se requiere de igual forma, la configuración en redes de datos que comuniquen la oficina principal con otros centros de operaciones dispersos, o enlacen a la compañía con sus clientes, consumidores, y también se necesita proveer los medios para intercambiar datos entre la compañía e instituciones financieras, y agencias regulatorias.

El objetivo de ésta investigación es saber qué servicios de redes de comunicaciones son los que se necesitan y, qué instalaciones han sido establecidas para dar soporte a éstos servicios. Además, los investigadores deben adquirir datos acerca de los recursos que proveen otras empresas a la compañía que facilitan lo necesario para las comunicaciones, incluyendo:

- Las oficinas de servicio local de telecomunicaciones (COs) y la Central telefónica que proporciona los puntos de presencia (POPs) de larga distancia que controlan la conmutación en el tráfico de las llamadas entrantes de la compañía y proveen los *gateways* a redes de área amplia en llamadas de salida, (ambos servidores y posibles alternativas para éstas instalaciones, que deben ser utilizadas en caso de que ocurra una interrupción de algún servidor).

- Instalaciones especiales, enlazadas desde servidores públicos, tales como las T-1, satélites, redes de conmutación de paquetes, y respaldos para estos servicios en el momento de la interrupción.
- Servicios en línea, tales como, llamadas en espera, etc., que son rentados de los servicios de compañías telefónicas, además de los servicios de disponibilidad para enrutar éstos servicios a un centro de operaciones alterno, como por ejemplo, un centro de operaciones de respaldo de información, en el momento de un desastre.
- Acceso a las instalaciones de comunicaciones mantenidos por un centro de administración ubicado en un lugar alterno a la empresa.

Una vez que la infraestructura para comunicaciones de voz y datos ha sido investigada y documentada, la siguiente tarea es buscar las instalaciones y servicios asociados a las funciones específicas de los negocios económico/administrativos. Como en el caso de los sistemas, las respuestas documentadas dadas por el usuario final con respecto a los negocios, nos revelan cuáles recursos de la red son accesados y cómo son utilizados.

La documentación de las redes debe proveer algo de la información "oculta" de éstas transacciones. Otras pistas deben ser obtenidas desde sistemas de documentación o revisando las salidas de los sistemas registradores de llamadas, las conexiones de llamadas telefónicas, copias de mensajes o reportes de la compañía telefónica.

Afortunadamente, la mayoría de las compañías de redes se recuperan intactas en el momento de una interrupción. Lo que podría fallar en éstos casos sería la compañía telefónica que proporciona el servicio a la empresa.

3.10 *La calidad-grado de servicio para los clientes o usuarios de una red.*

En muchas compañías, el procesamiento de información es proporcionado al usuario en base a un contrato llamado *Calidad-Grado de Servicio*. Éste establece las reglas de interacción entre la compañía que procesa la información y los usuarios finales. Los acuerdos a menudo incluyen descripciones de los procedimientos de los servicios de procesamiento de la información, devolución, etc. que serán empleados para reponer la información.

Tales acuerdos son considerados un elemento importante en la cultura de compañías que buscan emprender e innovar en su trabajo.

El procesamiento de datos, se espera que proporcione el servicio lo mejor posible a un costo que sea competitivo con otras empresas que ofrezcan los mismos servicios. Los acuerdos de C*alidad-Grado de Servicio*, formalizan éstos valores y los promueven.

Muchos acuerdos de C*alidad-Grado de Servicio* también dan una garantía de disponibilidad de servicio, esto significa que prometen al usuario que los sistemas siempre estarán disponibles a un valor cercano al 100%, ó dicho de otra forma, sin caídas de servicios.

Tales promesas ayudan a justificar el gasto de los recursos presupuestados para una compañía de servicios de procesamiento de información, que no se podría hacer sin la previsión de una PLRD.

En muchas empresas, auditores internos sirven como "ojos y oídos" para el director administrativo, alertándolo de los puntos legales confiables, riesgos financieros y eficiencia en función de negocios. Algunas empresas otorgan éstos trabajos extras para los auditores externos y con sus visitas periódicas proveen más ideas para saber lo que está bien o mal.

IV. PROCEDIMIENTOS DEL PLAN DE RECUPERACIÓN

4.1 *Asignación y entrenamiento del personal técnico y de operaciones*.

Juntar al equipo del proyecto.

La PLRD es un esfuerzo de equipo. Aún si el encargado de la planeación es el único individuo responsable de tiempo completo para hacer el esfuerzo, otros (incluyendo los técnicos, personal administrativo) estarán involucrados. Aún en casos donde un consultor sea llamado para realizar la PLRD, la compañía asigna normalmente a un coordinador para que trabaje en el plan, revise y/o aprenda del consultor.

Consideraciones para seleccionar al equipo del proyecto.

El equipo del proyecto consistirá del encargado de la planeación, un representante de cada función corporativa o departamento (incluyendo auditores internos) y técnicos expertos, son requeridos para el uso de la tecnología de redes y computadoras de la empresa. También personal de oficina, tal vez una secretaria para el proyecto, personas para grabar las juntas, coordinarlas, etc.

El equipo de planeación debe ser pequeño, para que sea efectivo y para que mantenga los costos del proyecto al mínimo. También, los miembros del equipo, deben ser confiables, puntuales y si están sirviendo en otras áreas o tareas en la misma empresa, deben tener el tiempo suficiente en sus horarios, para realizar las tareas que se les demande.

Administración.

Para éste ejemplo, el administrador del proyecto (encargado de la planeación, coordinador) es un empleado de la empresa y no un consultor externo. Los consultores deben ser vistos como miembros potenciales del equipo de planeación, y como técnicos expertos de acuerdo a su experiencia con el desarrollo de éstos planes. De todas formas, aún cuando se emplea a un consultor externo, el consultor opera (y/o trabaja en conjunto) bajo la dirección del encargado de la planeación de la misma empresa.

La pregunta: ¿quién debe desarrollar el plan; el propio personal o un consultor externo?, se está volviendo irrelevante, desde que la información de planeación de recuperación de desastres se ha vuelto más accesible a cualquier interesado. La nueva pregunta es: ¿si un consultor externo es definitivamente necesario, o si esto es sólo un gasto superfluo?

A veces el gasto de un consultor externo puede servir de influencia para superar la poca participación de algunos gerentes, o para cultivar la confianza administrativa en la realización del plan. Trabajar sin consultor externo es conveniente cuando el gasto por el mismo, es demasiado, cuando las capacidades técnicas del encargado de la planeación de la propia empresa compensen la complejidad técnica que se tenga, o cuando se esté esperando la respuesta por parte del gerente general. Desde luego, el coordinador de la empresa, también debe tener las habilidades que se requieren para desarrollar el plan, o para que tenga acceso a los recursos que se necesitan para desarrollar aquellas habilidades y así, permitirle trabajar en el plan de tiempo completo.

Cualquier empleado con habilidades en comunicaciones, conocimientos básicos en los objetivos de la PLRD y administración de proyectos, puede desarrollar un plan que debe ser probado y bien revisado para así, dar la capacidad de recuperación a su empresa. Desde ésta perspectiva, los consultores externos son vistos como un útil y potencial recurso técnico para la PLRD, pero no son sustitutos para un plan interno efectivo.

Ahora se debe examinar el papel del encargado de la planeación en mayor detalle. En el contexto de la iniciación del proyecto, lo primero que se debe hacer es probar las capacidades administrativas del encargado de la planeación.

Negociación en el liderazgo.

Se entiende por administración efectiva, a las negociaciones en el liderazgo.

¿Qué son las negociaciones en el liderazgo? Es un respeto por la experiencia, conocimiento, habilidades de los individuos, todo esto expresado en sus opiniones. El equipo de la PLRD tendrá individuos con diferentes experiencias y mentalidades. Un negociador maneja la interacción de éstos individuos para mejorar la cooperación y disminuir los conflictos.

Los miembros del equipo técnico tendrán la tarea de desarrollar soluciones técnicas de recuperación de sistemas y redes. De todas formas, estas soluciones técnicas no suplantarán las necesidades e intereses de los administradores de negocios que formen parte del equipo. Los gerentes entienden el trabajo que se hace en los departamentos para la compañía y seguramente tienen una mejor apreciación de las interrelaciones entre las funciones de negocios, los costos de operaciones y del mundo mercantil. Este respaldo es igualmente vital para establecer un plan de recuperación de los negocios.

Sin una apreciación de estas interrelaciones, el encargado de la planeación (dependiendo de su propia experiencia) favorecerá a alguno de los dos grupos previamente mencionados. Si existe algún truismo, esto es, que los miembros del equipo con mentalidad de negocios, serán de enorme ayuda para identificar las prioridades de recuperación y los que tengan mentalidad técnica ayudarán las prioridades de los negocios con soluciones técnicas. El encargado de la planeación deberá dar a ambos grupos sus deberes, y así mediar para negociar los desacuerdos.

Funciones administrativas y presupuesto.

El encargado de la planeación, como gerente del proyecto de recuperación de desastre, es el responsable de la administración y el presupuesto. Ésta responsabilidad incluye:

1 Formular un presupuesto; aprobando los gastos; coordinando con la nómina de la empresa, contabilidad, y documentar los gastos.

2 Hacer contacto con el director general, para presentar, justificar y revisar los planes del proyecto para presentar progresos y solicitar soporte en actividades de planeación y gastos.

3 Hacer contacto con los gerentes de departamento y administradores de sistemas para obtener su cooperación y asistencia en la obtención de datos, implementación de políticas de respaldos y refuerzos, pruebas del plan e instalación de las capacidades de prevención de desastre, trabajar con los gerentes y administradores para resolver conflictos.

4 Seleccionar y contratar a los miembros del equipo del proyecto, trabajar con recursos humanos de la empresa y gerentes de departamento para coordinar los horarios de trabajo, y otros puntos personales.

5 Monitorear el rendimiento del equipo, asignar tareas y responsabilidades, evaluar la calidad del trabajo, entrenamiento y disciplina.

6 Negociar disputas, construir solidaridad en el equipo, servir como abogado y mediador para el equipo.

Habilidades en la administración del proyecto.

El encargado de la planeación como administrador del proyecto, tiene responsabilidades adicionales que lo relacionan con el mismo proyecto, específicamente, el encargado de la planeación debe:

A Establecer el enfoque del plan, articular los objetivos, definir tareas de planeación.
B Establecer estándares para el rendimiento del trabajo y las herramientas del proyecto.
C Definir los componentes de trabajo, recursos requeridos e identificar un camino de tareas críticas.
D Hacer un horario de trabajo, monitorear el horario, identificar y superar los obstáculos del horario de trabajo.
E Mantener registros exactos de trabajo, incluyendo un modelo de proyecto e información actual, identificar variaciones y sus causas, hacer reportes periódicos para el director general o a su representante designado.
F Validar o verificar el trabajo completado.
G Establecer un criterio aceptable y manejar el proceso de aprobación.

El encargado de la planeación debe tener experiencia en las técnicas de administración del proyecto como se plantea en las tareas anteriormente citadas. Además, el o ella debe tener las habilidades necesarias para utilizar software de administración de proyectos que sean utilizados por la empresa (en caso de que se tengan). El uso de estas herramientas, ayuda al encargado de la planeación para participar directamente en la recolección de información y formulación de la estrategia.

Técnicos expertos.

Una PLRD efectiva requiere de la coordinación de talentos y habilidades de diferentes expertos. Como se ha mencionado previamente, se debe contratar a alguien que tenga experiencia en el desarrollo de planes para otras empresas y un gran conocimiento de la industria de recuperación de desastres. El personal de la empresa que esté bien preparado en tecnología de redes y sistemas, además de quienes han participado en el diseño de aplicaciones para la empresa, deben ser empleados para ayudar en el desarrollo de estrategias para recuperar los servicios y capacidades en el evento de una interrupción prolongada. Los gerentes administrativos o los usuarios de sistemas deben ser consultados para agregar otra perspectiva muy necesaria en las funciones críticas de negocios, estándares y operaciones empresariales. Deben ser invitados los auditores de la empresa para participar y contribuir con su experiencia en la justificación del plan, calidad segura y pruebas.

Consultores Externos.

Como se mencionó anteriormente, el consultor de recuperación de desastres puede ofrecer útiles ideas en el proyecto de planeación basándose en la experiencia de desarrollo de planes para otras empresas y conocimiento de los productos y servicios de la industria de recuperación de desastres. Lo malo es que los consultores son siempre costosos. Debido a eso, su uso debe ser cuidadosamente considerado y maximizado.

Lista para evaluar los servicios de consultoría.

1. Verificar que los servicios del consultor hallan sido adquiridos en la experiencia y desarrollo de planes para otras empresas de la misma categoría y área de negocio de la empresa que lo contrate.

2. Investigar referencias y discutir su desempeño pasado. Averiguar qué servicios el consultor otorgó. Preguntar opiniones personales de rendimiento:

¿El servicio fue efectivo?
¿El consultor cumplió con la agenda?
¿El consultor recomendó otros productos y servicios de recuperación de desastre? ¿Cuáles?
¿El servicio justificó el costo?
¿El consultor mantuvo el plan?
¿Participó en las pruebas del plan?
¿Otorgó entrenamiento a los participantes del plan o al coordinador del plan de la empresa?
¿Cuál fue la mayor contribución con su cliente anterior?
¿Podría volverlo a contratar su cliente anterior?

3. Identificar las áreas en la cuales el consultor podría ser más útil.

¿Evaluando los cuestionarios en la recolección de información?
¿Ayudando en el análisis de riesgo?
¿Revisando los resultados del análisis de riesgo?
¿Formulando estrategias de recuperación?
¿Desarrollando el documento del plan de recuperación de desastre?
¿Evaluando el documento del plan?
¿Desarrollando programas de entrenamiento para los participantes del plan?
¿Desarrollando pruebas de estrategia?
¿Analizando resultados de pruebas?
¿Manteniendo el plan?

4. ¿Cuál es la metodología del consultor? ¿Es consistente con un proyecto de método administrativo? ¿Utiliza alguna herramienta de planeación de recuperación de desastre?

5. Pedir una guía para el proyecto de planeación de recuperación, representando el método del consultor.

6. ¿El consultor se relaciona con los proveedores de productos y servicios de recuperación de desastres?

Además del precio del consultor, el encargado de la planeación debe investigar las relaciones del consultor con los proveedores de productores de servicios y productos de recuperación de desastres. Si el consultor será llamado para participar sobre la formulación de la estrategia de recuperación, será de utilidad saber con cuales proveedores el consultor ha hecho negocios (para saber si puede haber un conflicto de interés, y para identificar abusos en los precios que pueden ser resultado y para uso particular del mismo consultor).

Muchos consultores de recuperación de desastres ofrecen soporte de servicio completo para PLRD, incluyendo alguna herramienta para PLRD, metodología y hasta un plan. Éste debe ser revisado para ver si es consistente con el método administrativo del proyecto de la empresa. Si el encargado de la planeación, sólo quiere usar al consultor en ciertas áreas del desarrollo del plan, éstas deben ser identificadas y se deben estimar los requerimientos de tiempo. Entonces se debe hacer una propuesta al consultor, para su cargo de trabajo.

Los consultores pueden ser una ventaja para la PLRD, si se usan propiamente. La experiencia es la mejor contribución del consultor, que es mejor utilizada en el análisis de riesgo, en el diseño del documento del plan y en la formulación de pruebas de estrategia. De todas formas, aún estas actividades deben ser realizadas de manera adecuada por el personal de la empresa, dadas las limitaciones del presupuesto.

Especialistas de redes y sistemas.

La PLRD, consiste en gran parte, en implantar sistemas y redes de emergencia, para dar servicios críticos, que hallan sido interrumpidos en sus plataformas normales. Aquellos que diseñan, implementan y mantienen los sistemas y redes de la compañía, son casi siempre las mejores fuentes de información, en cómo restaurar aquellos sistemas y redes en situaciones de desastres. Por ésta razón, la mayoría de los expertos técnicos requeridos para la PLRD deben ser buscados en el personal técnico de la empresa.

Las tareas a las cuales se deben confrontar los miembros de éste equipo incluyen lo siguiente:

- El desarrollo de una configuración mínima de equipo aceptable, para dar los servicios de procesamiento de información crítica para un período de tiempo establecido.
- El desarrollo de una mínima configuración de red aceptable, para manejar los requerimientos de comunicaciones de voz y datos críticas, para un período de tiempo establecido.
- La formulación de estándares de diseño de software, para facilitar la compatibilidad de la aplicación, desde los servidores hasta la configuración mínima de equipo aceptable.
- Recolección y análisis de uso de estadísticas, documentación de aplicaciones en-línea y por lotes, documentación de las características de seguridad de la aplicación y soluciones, la identificación de los requerimientos de logística para las operaciones del site remoto.
- El desarrollo y la implementación de una gran estrategia de respaldo de sistemas de información.
- El desarrollo de una guía y programas para respaldos y seguridad de PCs.
- Mantenimiento y pruebas de la estrategia de recuperación.

Se requerirán expertos técnicos de la empresa para dar soluciones en el proceso de la información y requerimientos de redes en una situación de desastre. Usarán el diseño de estándares y técnicas de desarrollo (comúnmente empleadas para el desarrollo de sistemas actuales), para crear un sistema, que cumpla con las necesidades y objetivos de la empresa, como se definió en el PLRD.

Expertos en función de negocios.

Si los expertos técnicos de la empresa trabajarán para desarrollar sistemas de recuperación y redes, los expertos en función de negocios (gerentes administrativos o representantes de equipo de los departamentos clave de la empresa, que han sido seleccionados para el equipo de recuperación de desastre), identificarán los requerimientos que los sistemas y redes de emergencia necesiten. Un experto en función de negocios, examinará a cada departamento de la empresa, identificando los típicos procesos de trabajo. Ellos le pedirán al personal de algún departamento, sus opiniones acerca de algún posible desastre, y de la capacidad que tendría el departamento, sin redes o sistemas.

Habiendo recopilado la información: de terminales, retención de grabaciones, y otros requerimientos de trabajo (FAX, equipo para fotocopias, lectores de microfichas, formas, etc.), el experto en función de negocios intentará aplicar un esquema de clasificación crítico a las funciones de cada departamento. Las funciones que sean identificadas como críticas, junto con el personal, sistema, red, instalación y logísticas, serán objetivos de recuperación para el Plan de Recuperación de Desastre.

Auditores.

El trabajo del auditor tiene que ver con lo legal o lo regulatorio, con la integración de la información, seguridad, y el aseguramiento de la calidad. No sólo va a ayudar en los asuntos legales de la PLRD, el o ella también pueden aportar en otros asuntos como:

- Identificando las funciones de los negocios que sean críticas, no por su contribución a la continuidad de las operaciones de los negocios, sino por su ayuda en los aspectos legales y regulatorios.
- Ayudando en la formulación del plan de estrategias para pruebas usando herramientas empleadas en auditorias.

Supervisando el proceso de evaluación de las pruebas y asegurando el mantenimiento del plan.

Adicionalmente, los auditores quienes sirven como "los ojos y oídos del administrador general", pueden mantener un canal excelente para mantener a la administración informada de los progresos y obstáculos del plan, recomendando los costos para la estrategia, y para justificar los propósitos del plan.

También son de ayuda para evaluar las coberturas de seguros e identificando las áreas en las cuales los costos se pueden reducir, basándose en las provisiones de recuperación de desastres.

Empleados de oficina y personal de soporte.

La PLRD es una tarea compleja con mucha recopilación de información, procesamiento y distribución de componentes. Las juntas deben ser documentadas, las agendas de entrevistas para recopilar información con los principales del proyecto, se deben generar reportes del estado actual del proyecto, se deben solicitar ofertas al proveedor, recibir respuestas y documentar las propuestas.

Algunos gerentes de proyectos de recuperación de desastre utilizan los servicios de un secretario(a) de proyecto para complementar éstas tareas. En algunas empresas, los capturistas se deben llamar para ayudar en algunos trabajos de preparación de entregas de datos. Para el beneficio del presupuesto, el administrador del proyecto debe esforzarse para mantener los costos al mínimo, posiblemente requiriendo miembros del equipo para realizar sus capturas de información, y asignando actividades secretariales a los miembros del equipo de manera rotativa. Por lo menos a un individuo se le debe pedir que maneje de tiempo completo, la enorme cantidad de información generada en el proyecto de recuperación de desastre.

4.2 *Entrenamiento del personal.*

El precio por una auditoria es excesivo, pero es el mismo precio no tener un plan exitosamente completado a tiempo para la siguiente auditoria; una posibilidad real si los expertos de la compañía auditora no escriben el plan usando su conocimiento previo de los sistemas de la empresa, redes y las vulnerabilidades existentes. Se puede reducir el precio, diría un vendedor en tono de conspiración, si las fases de entrenamiento y pruebas se omiten.

Pero el plan de pruebas es absolutamente vital para asegurar su viabilidad. La planeación es un proceso interactivo con pruebas periódicas, y precisamente da los medios necesarios para identificar lo que se debe omitir.

El entrenamiento es igualmente vital. El PLRD es más que un papeleo o una barrera si nadie sabe implementar sus procedimientos en caso de una interrupción.

El entrenamiento imparte un conocimiento del plan para aquellos que deban actuar en él en una emergencia. Y también puede ser benéfico para crear conciencia en el personal. Los empleados entrenados para reconocer potenciales de desastre, son la primera línea de defensa para la supervivencia de la empresa. Pueden reportar riesgos, y entonces tomar medidas para eliminarlos. Se abarcarán tanto las formas tradicionales de entrenamiento corporativo y, las empresas externas que ofrezcan el servicio.

Objetivos del entrenamiento.

El objetivo es crear la capacidad de recuperación de desastre de una empresa, creando una cultura de conciencia y seguridad. En términos más prácticos, el entrenamiento comprende lo siguiente:

- Se debe familiarizar al personal que se involucrará en la implementación del plan y sus respectivas complejidades de los procedimientos y estrategias.
- Incrementar la conciencia de la existencia de potenciales de desastre y seguridad en riesgos en el personal, de tal forma que puedan participar y prevenir en desastres que se puedan evitar.

Hacer programas de entrenamiento para llevar a cabo estos objetivos es una parte para hacer el equipo y una fase de entrenamiento del proyecto de PLRD como se describe en la tabla (4-2).

Las otras actividades de ésta fase, (las cuales debieron haberse realizado en el momento en el que los programas de entrenamiento hallan sido formulados y conducidos) incluyen la identificación de los equipos de recuperación a los que se les asignarán las tareas en la crisis que se presente, seleccionando a los integrantes de éstos equipos, desarrollando una estrategia para notificar a los miembros del equipo a la hora de enfrentar una interrupción de las actividades críticas de negocios, y desarrollando un organigrama de administración de emergencia para coordinar las actividades de los equipos.

El entrenamiento es un componente importante en la preparación para desastres. Personal que fue involucrado directamente en la preparación de las estrategias de recuperación, y el resto que trabaja en la empresa, debe ser entrenado para reconocer y responder a potenciales y situaciones de desastre.

Los programas formales deben ser articulados para aplicar estos requerimientos de entrenamiento. Deben ser desarrollados de acuerdo a una estructura y métodos de diseño. Deben ser presentados, de tal forma que mejoren la eficacia de los aprendices.

Una vez que los equipos hallan sido identificados y seleccionados, (una actividad que podría tomar diferentes formas de acuerdo a la empresa) los líderes de equipo y/o los miembros deben tomar parte en el entrenamiento o en el procedimiento del plan.

Desarrollando el programa de entrenamiento.

La retroalimentación del aprendiz y la observación del rendimiento se usan para evaluar la efectividad, para revisar y mejorar los programas de entrenamiento.

La tarea del programa de entrenamiento será presentar procedimientos, de tal forma que los objetivos del procedimiento se correlacionen con los objetivos del entrenamiento.

La tabla (4-3) nos da una herramienta muy útil para correlacionar los objetivos del PLRD con los objetivos del entrenamiento. Para cada objetivo del entrenamiento (OBJ#) y descripción se tiene una columna asociada para registrar el número de tarea del PLRD. El balance de la forma es usado para registrar el método de enseñanza que se usará para comunicar los contenidos, procedimientos para la tarea y el método que se usará para validar que el aprendizaje se halla realizado.

Desde luego, el entrenamiento en los procedimientos se debe hacer después de que los aprendices hallan hecho una revisión de las estrategias del plan y que hallan sido familiarizados con el contenido y diseño del documento del PLRD. Éstas lecciones preliminares darán un contexto para entender los elementos más raros de los procedimientos del entrenamiento y facilitarán a los aprendices el uso de la guía de entrenamiento (el documento del PLRD) de una manera más efectiva.

EL PROYECTO DE RECUPERACIÓN DE DESASTRE.
SELECCIÓN Y ENTRENAMIENTO.

ACTIVIDADES PRINCIPALES

Identificar los equipos de recuperación
Seleccionar a los miembros del equipo
Desarrollar un árbol de notificación
Hacer un diagrama administrativo de emergencia
Entrenar a los integrantes del equipo
Implementar un programa de conciencia corporativa

EL PROYECTO DEL PLAN DE RECUPERACIÓN DE DESASTRES

(2-5)

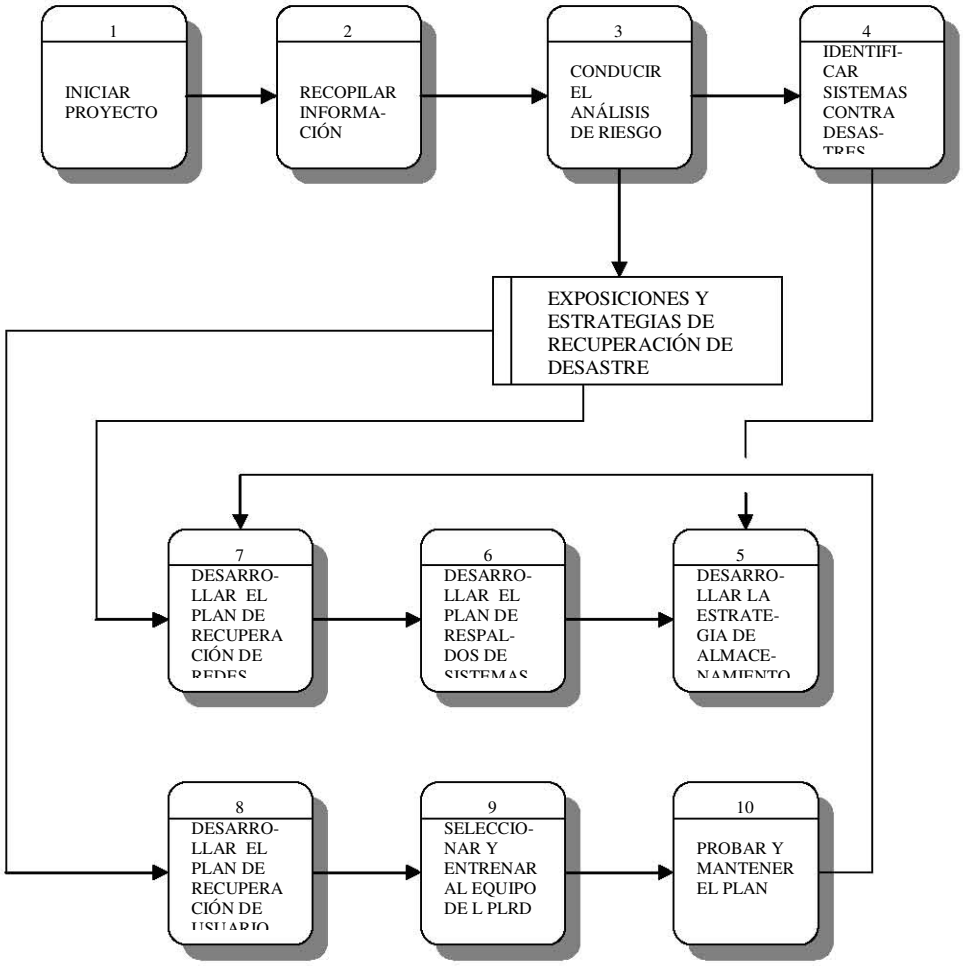


TABLA (4-2)

HOJA DE DESARROLLO DE OBJETIVOS.

# OBJ VALIDA-CIÓN	OBJETIVO	# TAREA	RESUMEN DE TAREA	MÉTODO DE ENTRENAMIENTO/ TIEMPO REQUERIDO	

FIG (4-3)

FIG (4-3)

Salón de clases.

Una guía general para conducir un salón para un programa de entrenamiento de manera exitosa, incluye lo siguiente:

- Desarrollar un plan por lección. La FIG (4-4) nos da un ejemplo. Los planes por lección nos permiten organizar los métodos de entrenamiento, lectura del material, los requerimientos del aprendiz y los requerimientos de tiempo para la enseñanza en un solo lugar para facilitar su uso. Las lecciones deben correlacionarse a las tareas del actual PLRD y deben ser relevantes para una audiencia específica.
- Hacer una agenda. Una agenda es una muestra de respeto para los aprendices identificando lo que se debe llevar a cabo en un marco de tiempo dado. La agenda de entrenamiento debe incluir las fechas de inicio y fin, hora de descanso, y lecciones clave que se deban aprender. También debe tener la hora de preguntas y respuestas, tomando en cuenta que las preguntas entretengan en la presentación para asegurar un buen ambiente.
- Coordinar el entrenamiento con los gerentes. Se debe asegurar que los gerentes de los aprendices sepan que el horario de entrenamiento no tolerará interrupciones. Para tener éxito, el entrenamiento en el salón debe ser conducido con un mínimo de interrupciones.
- Ser cuidadoso de la experiencia y conocimientos del aprendiz. Los aprendices adultos requieren respeto por sus conocimientos y experiencia actuales. Observaciones, sus anécdotas, preguntas, serán entretenidas siempre que tengan que ver con el contexto y no quiten el tiempo para seguir comunicando los puntos clave del entrenamiento. El entrenamiento ayuda a los aprendices a comprender la criticidad de sus tareas asignadas y de las relaciones entre sus tareas y el trabajo de otros equipos en el momento de una crisis.
- Dar variedad a los métodos de entrenamiento empleados. El salón de entrenamiento no es una clase de lectura. Cuando sea posible, se debe alentar la interacción para mejorar el entendimiento. También se deben utilizar otros métodos de enseñanza (visuales, con sonido) tanto como sea posible. Los estudios muestran que el aprendizaje es más fácil y la información se retiene por más tiempo si se utilizan varios sentidos.

El entretenimiento también es clave. Anécdotas acerca de experiencias de otras empresas en situaciones de recuperación de desastre ayuda a relajar a los aprendices, entonces el aprendizaje es más sencillo.

- Solicitar retroalimentación de parte de los aprendices. Una hoja de evaluación se muestra en la tabla (4-5) que debe ser adaptada para solicitar comentarios. Las evaluaciones de los aprendices pueden ser una herramienta muy útil para ver cuáles enseñanzas alcanzan lo esperado y cuales no. Esta entrada puede ser usada para mejorar las siguientes lecciones de entrenamiento.

Desde luego, estos son solo unos cuántos ingredientes para tener un aula exitosa. En algunas empresas, una organización formal para entrenamiento corporativo puede estar disponible y debe ser usada para desarrollar y conducir el entrenamiento del equipo de recuperación de desastres. Como mínimo, los profesionales de entrenamiento de la empresa deben estar disponibles para ofrecer consejos en la construcción de un programa de entrenamiento bien desarrollado.

En algunas empresas, el entrenamiento en un aula no es disponible debido a falta de tiempo, instalaciones o recursos. El entrenamiento basado en texto nos da una alternativa.

Las lecciones basadas en texto, son desarrolladas de la misma manera como las lecciones en salones, a excepción de que la enseñanza se realiza con la lectura de documentos, típicamente partes del PLRD. Siguiendo la lectura, el aprendiz debe ser cuestionado para responder muchas preguntas de manera escrita, acerca de lo que él o ella ha leído, o por lo menos, firmar una forma para confirmar que ha tomado el entrenamiento.

Claramente, la instrucción basada en texto será validada, sobre la marcha del entrenamiento, a través de la participación del aprendiz en la prueba del PLRD. Los aprendices que entiendan lo que se espera de ellos en un escenario de prueba, y que puedan encontrar y usar los procedimientos establecidos en el documento del plan, ya han realizado los puntos del entrenamiento.

FIG(4-4) PLAN DE LECCIONES.

NÚMERO DE LECCIÓN: _____
TITULO DE LECCIÓN: _____
NÚMERO DE TAREA: _____
OBJETIVOS DE TAREA: _____
_____

# OBJ	PROCEDIMIENTO / OBJETIVO	MÉTODO DE ENSEÑANZA	MATERIAL

REFERENCIAS DEL PLAN: _____
MÉTODOS DE VALIDACIÓN: _____
_____
_____

LECCIÓN PREPARADA POR: FECHA:

FIG(4-4)

HOJA DE EVALUACIÓN DE ENTRENAMIENTO.

NÚMERO DE LECCIÓN: _____
TÍTULO DE LECCIÓN: _____
INSTRUCTOR: _____
FECHA: _____

INSTRUCCIONES: Por favor, completar la siguiente evaluación para ayudarnos a mejorar el entrenamiento a los integrantes del equipo en el plan de recuperación y tú función en él. Tus comentarios son importantes.

1. El entrenamiento que recibiste ¿fue relevante para tu función en el plan?
   Seleccionar con un círculo.

   SI NO

   Si tu respuesta fue NO, por favor explica tu respuesta:

_____

_____

_____

2. ¿El entrenamiento fue realizado profesionalmente? ¿el instructor estuvo preparado?
   ¿se tomaron en cuenta los horarios ?

   SI NO

   Si tu respuesta fue NO, por favor explica tu respuesta:

_____

_____

_____

3. ¿Cambiarías algo en el entrenamiento si tuvieras oportunidad?

   SI NO

   Si tu respuesta fue SI por favor explica tu respuesta: (escribe al reverso si es necesario)

_____

_____

_____

Gracias por tu participación.

OPCIONAL: Por favor firma y fecha. Puedes ser contactado para otra encuesta.

PARTICIPANTE: FECHA:

TABLA (4-5)

Incentivar la concientización responsable en los empleados.

Además de la administración del entrenamiento, también es importante el entrenamiento en todo el personal, para los líderes de equipo, y así activar el plan e implementarlo en una emergencia. La seguridad y bienestar de los empleados es un objetivo principal del PLRD. Debido a esto, deben estar familiarizados con los puntos de los planes que la compañía tiene para responder a una emergencia.

Como mínimo, los empleados deben saber qué hacer en una situación riesgosa, cómo reaccionar ante una evacuación de emergencia, y saber con quién contactar en el momento en el que un desastre impacte la oficina donde trabajen. En algunas empresas, éstas tareas importantes de entrenamiento son otorgadas a personal de recursos humanos. Se debe familiarizar a los empleados, con los procedimientos de emergencia como parte de su agenda. En otros casos, los gerentes de negocios contratan y entrenan a sus propios empleados y la tarea de crear conciencia en los empleados, es de ellos.

Cualquiera que sea el método que se utilice, el equipo del proyecto del PLRD debe buscar la cooperación de la alta dirección para fomentar la conciencia. Buzones de sugerencias, direcciones de correo electrónico para comentarios anónimos y otros medios para facilitar las comunicaciones, debido a los potenciales de desastre, pueden ser establecidos y presentados a todos los empleados. Los directores ejecutivos pueden cooperar, estableciendo reglas, escribiendo reconocimientos aplaudiendo el trabajo de los encargados de la planeación, y estableciendo un programa de conciencia en la empresa.

Todas éstas preparaciones, incluyendo entrenamiento en aulas o basados en texto, ayudan a preparar al personal de la empresa a cooperar de manera racional en la gran irracionalidad que provoca un desastre. Esto debe ser el filo de lo que se necesita para responder de manera efectiva a una emergencia y mantener el negocio en lo alto y trabajando después del desastre.

Además las compañías más grandes de proveedores externos, ofrecen un interés especial en algunos grupos de usuarios para sus clientes y consumidores. El resultado debe ser una mezcla informativa por los expertos internos y la organización del proveedor.

Los encargados de la planeación deben comenzar a circular información acerca del PLRD, seleccionada de algunas fuentes como revistas, periódicos, libros, etc. a los gerentes y a los líderes de los equipos de recuperación de manera rutinaria. Tales actividades tienden a reforzar el entrenamiento, concientización y puede estimular mejorando las funciones del sistema administrativo cambiante de recuperación de desastres.

Juntas de los equipos.

Se les debe aclarar a los miembros del equipo que atender a las juntas de planeación, es una función de negocios. Los horarios de las juntas deben ser anunciados, observados y se debe hacer una agenda más formal. La atención a las juntas de los equipos es muy importante. Se debe establecer un procedimiento para notificar en el evento, de que un miembro estará ausente.

Los administradores de los integrantes del equipo, también deben notificar de las actividades y juntas del equipo. Si un administrador no puede hacer, que algún miembro del equipo esté disponible, en el tiempo requerido que se necesita para asistir a las juntas y así, realizar sus tareas de PLRD, se debe notificar, para buscar a algún sustituto.

Las juntas de los equipos, proporcionan solamente al encargado de la planeación; métodos para monitorear la realización completa de las diferentes tareas. Estas deben realizarse profesionalmente en foros para la evaluación del trabajo y para la organización de nuevas tareas. También son una oportunidad para los miembros del equipo, el expresar sus opiniones y discutir las opciones. También nos dan métodos para que el coordinador del plan de sus consejos.

Otras consideraciones.

Los gerentes de negocios rebeldes deben ser alentados para que cooperen y participen en la recopilación de la información. Lo básico para obtener esta respuesta, incluye lo siguiente:

- Miembros del equipo-Explicar a los administradores o gerentes de las unidades de trabajo que su participación se necesita para que el plan proporcione la recuperación para toda la empresa: como miembros del equipo administrativo de la empresa, sus responsabilidades incluyen ayudar en la misión de una gran empresa. De otra forma, explicar que la ausencia en la participación del gerente, puede tener un impacto negativo en el plan, para recuperar las otras funciones claves de los negocios de la empresa, en caso de que ocurra un desastre. Si es posible, se deben identificar otros gerentes, que estén dando su total cooperación para persuadir al gerente apático a participar.
- Administración proactiva-Se les debe explicar a los gerentes de las unidades de trabajo que su participación (o falta de participación), en el proyecto de recuperación de desastre, refleja la habilidad que tienen como administradores. Un buen gerente ve más allá de las tareas diarias, para planear el desarrollo y salvaguardar la operación de su departamento. Anticipar las interrupciones potenciales y planear de manera proactiva para prevenir los desastres o para mantener bajo control algún posible daño, son cosas básicas para tener una buena administración.
- Cultivar el interés propio-Algunos gerentes también pueden ser persuadidos a participar en base a su propio interés. Si se puede demostrar que la no-cooperación o el retrazo en la participación pueden dar como resultado una falta de prevención de desastre y de recursos de recuperación para las unidades de trabajo con participantes más cooperativos, el propio interés del gerente debe ser enlistado para ayudar en un caso de cooperación. De igual forma, si se puede decir que el gerente general ha sido avisado de la participación de los otros gerentes, y que éste reconocimiento tiene algunos puntos positivos, otra vez el resultado puede ser más motivante para el gerente.

Se le debe avisar al gerente general de la falla del gerente apático. Esto puede dar como resultado una orden directa del gerente general, o de plano una censura, algo no deseable para la mayoría de los gerentes.

Desde luego, ésta medida es un caso extremo, y se debe hacer al momento de haber agotado todas las maneras posibles para hacer que el gerente cooperara. Si la información puede ser extraída por otros medios, tales como manuales de procedimientos e información regular financiera, el equipo de recuperación de desastre debe buscar éstas soluciones y realizar su trabajo. No existe un punto para cultivar la hostilidad en le plan.

Más aún, los miembros del equipo de recuperación, incluyendo al director del proyecto, deben mantener en mente la dificultad del esfuerzo que están pidiendo a los gerentes. Llenando algunos cuestionarios y documentos relacionados, es una tarea que consume tiempo. Algunas entrevistas consumen aún más tiempo del gerente. Viendo de cerca el problema de no cooperación, desde ésta perspectiva, dará al encuestador un punto de vista más positivo. Lo que se necesita es comprensión, investigadores bien intencionados, no misioneros forzados o sin compromiso.

Conclusión.

El entrenamiento es un componente importante para la preparación en caso de que exista algún desastre. El personal que estará involucrado directamente en la implementación de las estrategias de recuperación, y el resto que trabaja en la empresa, debe ser entrenado para reconocer y responder a las situaciones y potenciales de desastre.

Los programas formales deben ser articulados para enfatizar este requerimiento de entrenamiento. Deben estar presentados de forma que mejoren su eficacia para los aprendices

adultos. Solo entonces los desastres que se puedan evitar serán evadidos y el impacto de los desastres inevitables serán mitigados.

4.3 *Selección del personal.*

La fig. (4-6) sugiere que el proceso de recuperación de desastre involucrará al mismo tiempo, tareas realizadas por equipos o de manera individual. Casi todos los planes de recuperación emplean algún equipo para llevar a cabo las tareas críticas. La asignación de estos equipos varía de un plan a otro, dependiendo de los requerimientos exclusivos de recuperación.

En general, habrá un responsable que mande, controle y comunique los detalles de la recuperación a los equipos en una emergencia. Los miembros del equipo deben incluir a un coordinador de recuperación designado, gerentes representativos, un ejecutivo financiero y si es necesario, un corresponsal de relaciones de prensa de la empresa.

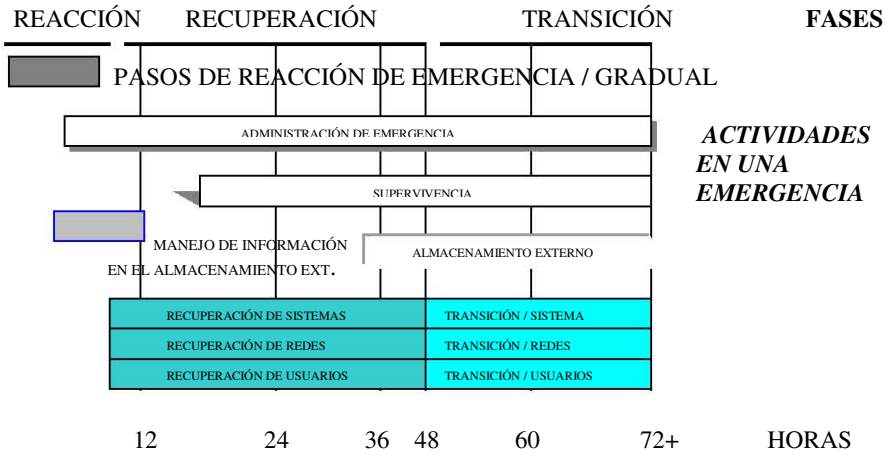


Fig. (4-6) Fases de las actividades en una emergencia.

El equipo de administración de emergencia establecerá un centro de administración de emergencia que será responsable para recibir los reportes de campo y coordinará las tareas de los equipos, proveedores, compañías de seguros, etc. Éste esfuerzo administrativo es guiado por medio de un diagrama de flujo.

Generalmente, la administración del equipo de emergencia, también establecerá un centro de comunicaciones de emergencia. Éste será el punto central para la administración de medios y para aterrizar las tareas de los investigadores, consumidores y clientes clave.

En adición de la administración de emergencia, otros equipos deben incluir un grupo de restauración de redes WAN, uno para mainframes, otro para LANs, otro para preparación del centro de usuarios, equipo de salvamento, para el site externo, etc. Cada equipo es definido por las tareas que deban realizar. Se tiene una misión, un marco de tiempo para completar el trabajo y números entre los miembros del personal con habilidades y conocimientos para realizar correctamente las tareas asignadas. Todos los equipos deben tener a un líder y su respectivo suplente. Estas personas son responsables para participar en todas las pruebas del plan y para hacer una apreciación de todas las tareas asignadas al equipo y sus interrelaciones con las tareas asignadas a otros equipos.

En una emergencia, el líder del equipo o su suplente serán responsables para contactar con los miembros de los otros equipos o para iniciar el trabajo lo más pronto en el momento en que la gerencia conceda la orden. Como parte del mantenimiento del plan, los líderes de equipo se asegurarán de que los procedimientos y las posiciones de los miembros del equipo se mantengan al corriente con los negocios cambiantes y los intercambios de personal.

La figura (4-7) nos ejemplifica una forma para registrar a los miembros de equipo. Ésta forma debe ser parte de la sección administrativa de emergencia del plan y debe ser revisada para actualizarla.

Criterio de selección.

La designación de los líderes de equipo, suplentes e integrantes no es arbitraria. La mayoría de las tareas de recuperación requieren personal con un gran conocimiento de las tecnologías o procedimientos de negocios que deban ser restaurados. Para formar parte del equipo, generalmente se decide en base a si se presentan ciertos pre-requisitos, habilidades y conocimientos.

Los líderes de equipo deben ser tanto hombres como mujeres, casados o solteros; éstos factores no afectarán o mejorarán sus capacidades en una crisis.

Si un miembro prospecto vive con cierta proximidad a las instalaciones principales de la compañía, éste candidato será preferible, que aquél que viva más lejos, o el que tenga que cruzar puentes, etc. para llegar al site de recuperación. Aquellos candidatos que tengan miedo para viajar en avión no serán una buena opción para volar, por ejemplo, a un hot site en una emergencia. Se deben tomar en cuenta muchas cosas para la selección del equipo. La consideración fundamental, de todas formas, es si el candidato tiene los conocimientos y habilidades (y tal vez la creatividad) para realizar las tareas identificadas para el equipo.

El papel de recursos humanos.

La función de recursos serviría para mantener actualizada la lista de integrantes del equipo. Cuando un empleado renuncia o es despedido, deben realizar una entrevista o mantener el archivo del personal que identificará si el empleado fue un miembro del equipo de recuperación de la empresa. Ésta notificación debe ser dirigida al coordinador de recuperación de desastre para asegurase de que el equipo esté completo y de que el nuevo integrante este siendo preparado.

Notificaciones.

Como se ha indicado, las formas de definiciones del equipo deben ser incluidas en la sección administrativa de emergencia del documento del plan. Esto facilitará la notificación de los líderes del equipo o los suplentes en una emergencia. Estas personas serán entonces, las responsables para notificar a todos los miembros del equipo. La sección administrativa, también debe contener otros directorios de notificaciones. Estos deben incluir un directorio de notificación administrativa fig(4-8), un directorio de notificación de departamentos fig(4-9), y uno de notificación de proveedores fig (4-10).

Responsabilidades específicas se deben asignar en el plan para contactar a varias personas de las listas, de tal forma que se active al personal que se requiera para recuperar las operaciones de los negocios. Éstas listas deben ser revisadas y mantenidas de manera rutinaria como parte de procedimientos administrativos de cambios.

En algunos planes, se hace una gráfica de responsabilidades de notificación. La persona A notifica a la persona B, C, y D que a su vez notificarán a las personas E, G y F. El resultado es una gráfica de árbol representando una cascada de notificaciones. El problema con esto, es que una falla en la comunicación puede ocurrir si un contacto malinterpreta o se confunde con el árbol.

Para evitar éste problema, puede ser útil establecer un procedimiento de contacto simple que notifique a cada persona, que existe una emergencia. Entonces llamarán a una línea designada (muchos proveedores de recuperación de desastre la ofrecen) para obtener

información o hacer comentarios y sugerencias. Éste único número también ofrecerá la ventaja de involucrar a la gente rápidamente, aún cuando no estén disponibles al principio.

FIG(4-7) **HOJA DE REGISTRO DEL EQUIPO.**

ESTRATEGIA: ______________________
TAREAS: ______________________
NOMBRE DEL EQUIPO: ______________________
PROPÓSITO DEL EQUIPO: ______________________
CONOCIMIENTOS / HABILIDADES: ______________________

LÍDER DE EQUIPO

NOMBRE: ______________________
TEL. OFICINA: ______________________
TEL. DOMICILIO: ______________________
OTROS: ______________________

SUPLENTE

NOMBRE: ______________________
TEL. OFICINA: ______________________
TEL. DOMICILIO: ______________________
OTROS: ______________________

INTEGRANTES

NOMBRE: ______________________
TEL. OFICINA: ______________________
TEL. DOMICILIO: ______________________
OTROS:
NOMBRE: ______________________
TEL. OFICINA: ______________________
TEL. DOMICILIO: ______________________
OTROS:
NOMBRE: ______________________
TEL. OFICINA: ______________________
TEL. DOMICILIO: ______________________
OTROS:
NOMBRE: ______________________
TEL. OFICINA: ______________________
TEL. DOMICILIO: ______________________
OTROS:
NOMBRE: ______________________
TEL. OFICINA: ______________________
TEL. DOMICILIO: ______________________
OTROS:
NOMBRE: ______________________
TEL. OFICINA: ______________________
TEL. DOMICILIO: ______________________
OTROS:
NOMBRE: ______________________
TEL. OFICINA: ______________________
TEL. DOMICILIO: ______________________
OTROS:
NOMBRE: ______________________
TEL. OFICINA: ______________________
TEL. DOMICILIO: ______________________
OTROS: (agregar páginas adicionales si es necesario)

FIG(4-8) **DIRECTORIO DE NOTIFICACIÓN ADMINISTRATIVA DE EMERGENCIA .**

GERENTE PRINCIPAL

NOMBRE: _____
TEL. OFICINA: _____
TEL. DOMICILIO: _____
OTROS: _____

SUPLENTE

NOMBRE: _____
TEL. OFICINA: _____
TEL. DOMICILIO: _____
OTROS: _____

GERENTE TÉCNICO DE OPERACIONES

NOMBRE: _____
TEL. OFICINA: _____
TEL. DOMICILIO: _____
OTROS: _____

GERENTE DE TELECOMUNICACIONES

NOMBRE: _____
TEL. OFICINA: _____
TEL. DOMICILIO: _____
OTROS: _____

COORDINADOR FINANCIERO DE RECUPERACIÓN

NOMBRE: _____
TEL. OFICINA: _____
TEL. DOMICILIO: _____
OTROS: _____

INTEGRANTES

NOMBRE: _____
TEL. OFICINA: _____
TEL. DOMICILIO: _____
OTROS: _____
NOMBRE: _____
TEL. OFICINA: _____
TEL. DOMICILIO: _____
OTROS: _____
NOMBRE: _____
TEL. OFICINA: _____
TEL. DOMICILIO: _____
OTROS: _____
NOMBRE: _____
TEL. OFICINA: _____
TEL. DOMICILIO: _____
OTROS: _____
NOMBRE: _____
TEL. OFICINA: _____
TEL. DOMICILIO: _____
OTROS: _____

FIG(4-9) **DIRECTORIO DE NOTIFICACIÓN DEPARTAMENTAL.**

AREA DE TRABAJO: _____
NÚMERO DE PERSONAL: _____
NÚMERO DE PERSONAL DE RECUPERACIÓN: _____

CONTACTO PRIMARIO: _____
CONTACTO SECUNDARIO: _____
NOTIFICADO POR: _____
POR EL PROCEDIMIENTO DEL PLAN: _____

NOMBRE Y TÍTULO	TEL. Y EXTENSIÓN

FIG(4-10) **DIRECTORIO DE NOTIFICACIÓN DE PROVEEDORES .**

PROVEEDOR DE HOT SITE

PROVEEDOR: _____ TEL. EXT
CONTACTO PRIMARIO: _____ _____
CONTACTO SECUNDARIO: _____ _____
POR EL PROCEDIMIENTO
DEL PLAN: _____

CENTRO DE RESPALDO

PROVEEDOR: _____ TEL. EXT
CONTACTO PRIMARIO: _____ _____
CONTACTO SECUNDARIO: _____ _____
POR EL PROCEDIMIENTO
DEL PLAN: _____

SERVICIOS DE REDES

PROVEEDOR: _____ TEL. EXT
CONTACTO PRIMARIO: _____ _____
CONTACTO SECUNDARIO: _____ _____
POR EL PROCEDIMIENTO
DEL PLAN: _____

ALMACENAMIENTO EXTERNO

PROVEEDOR: _____ TEL. EXT
CONTACTO PRIMARIO: _____ _____
CONTACTO SECUNDARIO: _____ _____
POR EL PROCEDIMIENTO
DEL PLAN: _____

PROVEEDOR DE HARDWARE

PROVEEDOR: _____ TEL. EXT
CONTACTO PRIMARIO: _____ _____
CONTACTO SECUNDARIO: _____ _____
POR EL PROCEDIMIENTO
DEL PLAN: _____

OTROS

PROVEEDOR: _____ TEL. EXT
CONTACTO PRIMARIO: _____ _____
CONTACTO SECUNDARIO: _____ _____
POR EL PROCEDIMIENTO
DEL PLAN: _____

PROVEEDOR: _____ TEL. EXT
CONTACTO PRIMARIO: _____ _____
CONTACTO SECUNDARIO: _____ _____
POR EL PROCEDIMIENTO
DEL PLAN: _____

(agregar págs. adicionales si es necesario)

4.4 ***Planeación de simulacros*****.**

Los simulacros y simulaciones de situaciones de urgencia, son una herramienta de gran utilidad para evaluar nuestra capacidad de respuesta ante un evento catastrófico, ya que colocan a la población en riesgo en condiciones lo más parecidas posibles a las calculadas en el evento al que se es vulnerable. Es conveniente recordar que el simulacro pretende un aprendizaje, y de la misma manera que lo que mal se planea, mal se aprende; de la calidad del simulacro dependerá el buen o mal aprendizaje de los involucrados. Debido a esto es recomendable que si se pretende desarrollar un simulacro, se consulte con expertos en la materia. Recuerde: Ni el sentido común ni la buena voluntad son suficientes para salvar vidas. De igual manera, subrayamos que desarrollar una cultura de protección civil, no es una tarea que se pueda cumplir en una semana o un año. El proceso para llegar a desarrollar un simulacro ideal, es el que sin previo aviso se haga participar de manera eficiente a todos los actores vulnerables, puede tardar décadas; lo importante es iniciar el proceso; cada día que se pase participando, será menos susceptible, cada día que se pase sin él, el riesgo que se presente aumenta. Se espera que se produzca un condicionamiento psicológico y operativo que permita enfrentar con un alto grado de éxito cualquier catástrofe, desvirtuando la creencia común de que todos los desastres provocan de manera inevitable el caos.

De manera general, para desarrollar las etapas de un buen programa de preparativos para casos de desastre, incluyen:

1. Integración del equipo de trabajo.
2. Motivación y sensibilización.
3. Diagnóstico de vulnerabilidad.
4. Planeación con base en el diagnóstico.
5. Capacitación de brigadas internas de protección civil.
6. Organización.
7. Puesta a prueba (simulaciones y simulacros).
8. Evaluación de ejercicio de simulaciones y simulacro.

Una vez realizado el diagnóstico de vulnerabilidad de un inmueble, capacitando a sus habitantes y adquirido los recursos materiales correspondientes, es prudente proyectar un plan de evacuación que será utilizado en aquellas ocasiones en que el evento obligue a sus ocupantes al desalojo del mismo.

A su vez, los simulacros se desarrollan en:

1. Etapa de Planificación
2. Etapa de Organización
3. Etapa de Ejecución
4. Etapa de Evaluación y Ajuste

1 Etapa de Planificación

Durante la etapa de planificación se deberá obtener el consentimiento y apoyo de la institución o instituciones que tengan como sede dicho inmueble, así como planear a plazos bien especificados, los simulacros a desarrollar.

Ejemplo

CPA = con previo aviso

Año 1996

Febrero Simulación de gabinete
Mayo Simulación de evacuación por piso o área CPA
Julio Simulacro de evacuación de todo el inmueble CPA
Sep. Simulacro de evacuación simultánea de varios inmuebles CPA
Año 1997
Febrero Simulacro de evacuación simultánea CPA
Mayo Simulacro de evacuación con evento asociado (ejemplo: incendio)
Julio Simulacro de evacuación con atención de víctimas
Sep. Simulacro de evacuación con incendios, colapsos y víctimas (sismo)
Año 1998
Febrero Simulacro global sin previo aviso (matutino)

Sep. Simulacro global sin previo aviso (nocturno)

Se recomienda que se tenga al menos dos simulacros anuales. Por supuesto, lo anterior debe ajustarse a las necesidades de la población específica y los tiempos pueden disminuirse o aumentarse.

Reiteramos la necesidad de consultar a un experto en la materia, quien con base en el diagnóstico de vulnerabilidad específico, pueda proponer un plan de trabajo a corto, mediano o largo plazo.

2 Etapa de organización

- Formación de un comité de organización
- Determinación del tipo y magnitud del simulacro, con base en el diagnóstico de vulnerabilidad
- Realización de un banco de datos conteniendo recursos humanos y materiales
- Elaboración del plan de evacuación del inmueble
- Difusión del plan de evacuación al universo susceptible
- Coordinación interinstitucional para la ejecución
- Capacitación del personal interno y formación de brigadas
- Señalización adecuada del inmueble
- Elaboración de guiones y determinación de necesidades
- Reuniones de preparación
- Información a los medios de comunicación
- Previsión de eventualidades (víctimas reales durante el simulacro)
- Identificaciones de los participantes
- Selección y entrenamiento de observaciones
- Sistemas de información
- Verificación final de preparativos

3 Etapa de ejecución

- Reunión previa con los coordinadores
- Reunión previa con profesionales
- Reunión previa con brigadistas
- Reunión previa con simuladores
- Reunión previa con observadores
- Preparación del escenario
- Inicio del operativo de seguridad
- Sincronización de relojes y cronómetros
- Posicionamiento de todo el personal

- Orden de inicio del ejercicio
- Comunicación del evento (alerta)
- Alarma y evacuación
- Desarrollo del plan de acción por los brigadistas
- Reunión de los evacuados en las áreas de seguridad
- Orden de finalización del ejercicio
- Retorno de los participantes a sus actividades regulares
- Finalización del operativo de seguridad
- Convocatoria a todos los participantes para la reunión de evaluación especificando fecha, hora y lugar

Difusión de la información condensada del simulacro a los participantes

V ORGANIZACIÓN PARA DESARROLLAR EL PLAN

5.1 *Estructura del documento del plan*.

Existen muchas formas para hacer el documento del plan, en éste caso, el inicio del documento empieza con un índice para después poner los diagramas y procedimientos. Esto es para facilitar el mantenimiento del plan y su uso para auditores. Si ocurre un desastre, sería cosa de retomar la sección de administración de emergencia del plan y seguir con la estrategia documentada hasta éste punto. La tabla (5-1) nos da la estructura para el documento del plan.

Estructura para el Plan de Recuperación de Desastres.

INDICE DEL PLAN
PROCEDIMIENTOS DE RESPUESTA DE EMERGENCIA-DIRECTORIO DE NOTIFICACIÓN Y DIAGRAMA DE DESICIÓN DE EMERGENCIA
PROCEDIMIENTOS DE RECUPERACIÓN DE SISTEMAS
PROCEDIMIENTOS DE RECUPERACIÓN DE REDES
PROCEDIMIENTOS DE RECUPERACIÓN DE USUARIOS
APÉNDICE A RESUMEN DEL ANÁLISIS DE RIESGO Y UNA REVISIÓN DE ESTRATEGIAS DE PREVENCIÓN Y RECUPERACIÓN
APÉNDICE B PLAN Y AGENDA DE ALMACENAMIENTO EXTERNO
APÉNDICE C PRUEBAS, ENTRENAMIENTO E HISTORIA DE MANTENIMIENTO DEL PLAN

Tabla (5-1)

Consideraciones para facilidad en el mantenimiento.

Éstas son muy importantes en el desarrollo del PLRD. El plan documentado sirve para regular y actualizar los cambios. En general, mucha información debe ser agrupada. Nombres, contactos con proveedores, teléfonos y direcciones, y otros datos deben ser colocados en un solo lugar del documento, en el cual se puedan actualizar fácilmente.

Consideraciones para facilidad de uso.

En la estructura del plan, el documento es dividido de manera lógica en procedimientos para recuperación de sistemas, redes y usuarios.

Como parte de la formulación de cada estrategia, un conjunto de tareas debe ser identificado. Cada tarea, en cambio, incorpora un objetivo, procedimiento y prueba. La figura (5-2) describe una especificación estructural de estrategias de recuperación.

Para propósitos organizacionales, se debe usar una técnica de numeración para identificar las tareas y sus procedimientos asociados. Esto ayudará con la descripción de las interrelaciones de tareas en un diagrama de flujo de emergencia. A la estrategia de recuperación

de sistemas, por ejemplo, se le debe asignar el valor numérico de 1.0. Como parte de ésta estrategia, debe haber una tarea en la cual, el proveedor de hot site, será avisado, de que la compañía se encuentra en una emergencia. Si ésta es la primera tarea, se le pondrá 1.1. a los pasos de los procesos asociados con la tarea de declaración de desastre y deben recibir los valores de 1.1 A, 1.1 B, 1.1 C, y así sucesivamente.

ESTRUCTURA DE ESTRATEGIAS DE RECUPERACIÓN DE DESASTRE.

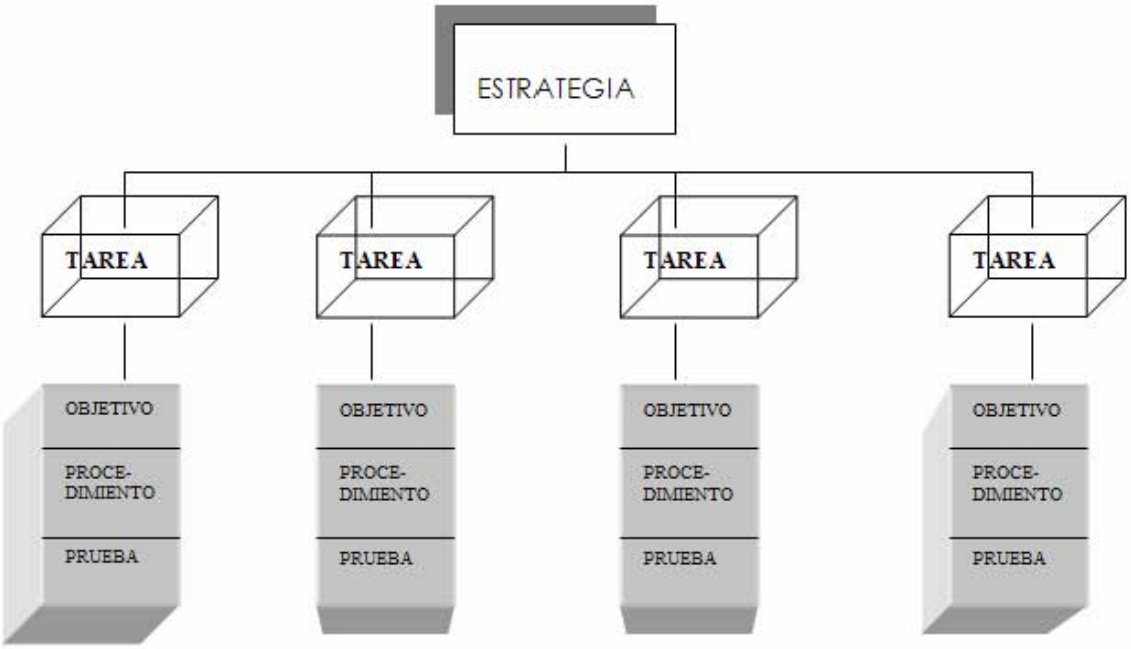


TABLA (5-2)

Cada sección de la estrategia, debe dar un resumen breve de los objetivos de la estrategia y una lista de todas las tareas asociadas con sus objetivos. Esto debe ser fácil de hacer con el análisis que se hace al formular la estrategia.

Todo eso nos recuerda que completar una sección de la estrategia es para completar los procedimientos de la tarea. La figura (5-3) nos da una hoja para documentar los procedimientos asociados con cada tarea. Estas hojas deben ser agregadas en secuencia, después de una revisión de estrategia y una lista de tareas.

Dependiendo de la complejidad del plan, se requerirán otros conjuntos lógicos de tareas. Por ejemplo, se requerirá una subsección para recuperación de sistemas, o para restaurar un sistema complejo en particular. El punto importante es, agrupar las tareas de manera lógica, de tal manera que se puedan usar de manera productiva, en una emergencia, para pruebas y entrenamiento.

Otras partes del plan deben incluir, apéndices, resumiendo el análisis de riesgo realizado por el equipo del proyecto, los detalles del plan de almacenamiento externo, y notas con la historia de pruebas del plan, entrenamiento y mantenimiento. El último apéndice es particularmente útil en auditorias.

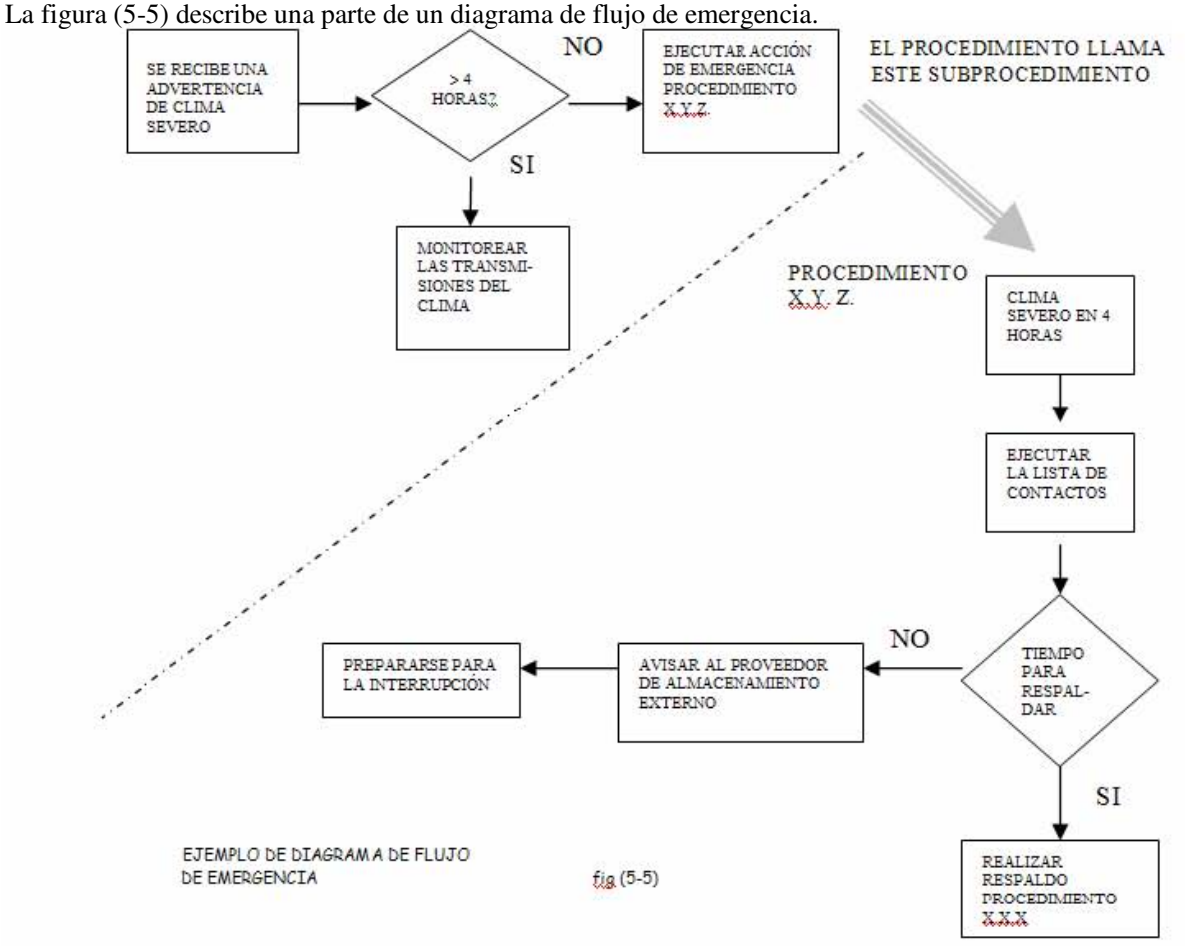
Diagrama de flujo de emergencia.

Se debe notar en la figura (5-3) que la forma tiene un espacio para anotar las dependencias o prerrequisitos para la tarea en uso. En una recuperación real, múltiples equipos trabajan con múltiples tareas al mismo tiempo. Para que una tarea, se complete, otra tarea

(posiblemente en otra área de estrategia), deberá ser completada primero. Estas tareas prerrequisito, serán anotadas en la forma de tareas.

Las interdependencias serán identificadas usando una gráfica, para describir las tareas de recuperación. Un encargado de planeación puede hacer el esfuerzo para realizar una. Éstas gráficas deben ser incluidas en cada sección de la estrategia del plan. Combinando todas las gráficas en una, dará como resultado, un diagrama de flujo de emergencia. Ésta gráfica debe ser simplificada para su uso no técnico, o debe ser construida en su nivel más fino de detalle para proveer a los gerentes técnicos una contabilidad exacta de las secuencias e interrelaciones de todas las tareas.

La figura (5-5) describe una parte de un diagrama de flujo de emergencia.



EJEMPLO DE DIAGRAMA DE FLUJO DE EMERGENCIA

fig (5-5)

OBJETIVOS DE TAREA/PROCEDIMIENTOS.

ESTRATEGIA: _____
TAREA: _____
OBJETIVO: _____
PRE-REQUISITOS/ INTERDEPENDENCIAS: _____
_____

PASO DEPENDENCIAS	DESCRIPCIÓN	REQUERIMIENTOS	

¿TAREA COMPLETA?: (encerrar en círculo) **SI** **NO**

si la respuesta fue no, por favor agregar páginas adicionales para completar el procedimiento de la tarea

PÁGINA _____ DE____

FIG (5-3)

Fase de reacción.

En ésta; la misma empresa nos da una respuesta al ataque de un desastre. Las tareas deben incluir, la notificación del hot site, la del equipo administrativo de emergencia, las estimaciones de los daños e interrupciones del site, los procesos de almacenamiento externo, etc.

Se hace una distinción entre la fase de reacción y una reacción de emergencia. La fase de reacción de tareas, son una serie de pasos tomados metódicamente en el avance de un desastre. Por ejemplo; para confrontar un huracán, en la empresa se deben tener varias horas para realizar los respaldos de último minuto, para quitar la electricidad, cubrir el hardware, y realizar otros procedimientos para reducir las consecuencias desastrosas de una tormenta.

Otras emergencias, tales como incendios repentinos, ocurrirán sin una previa advertencia. Los pasos tomados en respuesta a ésta emergencia, son menos preactivos.

Fase de recuperación.

Ésta incluye todos los procedimientos para recuperar los sistemas de misión-crítica, redes y operaciones de usuario con el marco de tiempo especificado en el plan. Las compañías pueden operar desde los hot sites, redes alternas, y centros de operaciones de respaldo por un período de tiempo considerable, mientras las operaciones de salvamento se realicen, o hasta que las nuevas locaciones queden listas.

Fase de transición.

Ésta es raramente documentada en los planes de recuperación, y sus parámetros no son conocidos hasta que ocurre un desastre. En algunos casos, las empresas utilizando los hot sites, requerirán cambiarse a un cold site del mismo proveedor, después de un período de tiempo específico. Esto incluirá a un conjunto de tareas (por ej. órdenes para reemplazar hardware, instalación, redireccionamiento de redes), que pueden ser documentadas en el plan.

Hasta el punto en que las actividades de transición se conozcan, deben ser documentadas para reducir las confrontaciones administrativas desconocidas, después de un desastre.

5.2 *Probando el Plan de Recuperación de Desastre*.

Para que el PLRD nos dé la capacidad de recuperar a una empresa, éste debe ser probado. Las pruebas validan la integridad de las estrategias, procedimientos de recuperación documentada y familiariza a los participantes de las pruebas con sus funciones en el momento de un desastre.

El propósito de las pruebas.

Es proporcionar una retroalimentación acerca de las estrategias y procedimientos que constituyen la ¨ estructura ¨ de la capacidad de recuperación documentada. A veces esto es malinterpretado, se cree que las pruebas buscan identificar faltas y errores en el plan. Esto solo tiene un poco de cierto. Las pruebas son cuidadosamente construidas para reforzar las estrategias apropiadas y para demostrar los defectos que puedan existir.

Las pruebas son un medio para adquirir información acerca del plan, los resultados de las pruebas son usados invariablemente para mejorar la capacidad de recuperación. Desde ésta perspectiva, uno puede ayudar al argumento de que no hay fallas en las pruebas.

Los propósitos de las pruebas incluyen:

- Validar (e identificar defectos) las estrategias y procedimientos del plan.

- Obtener información acerca de los tiempos de implementación de la estrategia de recuperación (para demostrar qué tan rápido una estrategia de recuperación de redes, por ejemplo, puede ser implementada y usarse).
- Para demostrar el rendimiento de salida de los sistemas y redes operando en modo de recuperación o para comparar el rendimiento de los sistemas de respaldo y redes con sistemas de producción y redes.
- Para demostrar la efectividad a examinadores, auditores y gerentes.
- Para adaptar los planes existentes y encontrar los nuevos requerimientos resultando de negocios, sistemas, redes o cambios de personal.
- Para familiarizar a los integrantes de equipos con sus funciones en el PLRD.

A ésta lista se le debe agregar algo más importante. Las pruebas les dan a los participantes (con un conjunto básico de habilidades) la facilidad de enfrentar un desastre, pero también se les enseña cómo manejarse racionalmente con la irracionalidad de un desastre. Como los desastres contienen una cantidad impredecible de elementos, entonces en las pruebas se ponen retos impredecibles, de manera que los participantes deban superar con un tiempo efectivo. Poniendo retos que requieran innovar en la solución del problema bajo un tiempo limitado, las pruebas equipan a los participantes con una habilidad que sería difícil de obtener de otra forma, que será extremadamente útil en el momento de una emergencia.

Mitos de las pruebas.

Dada la importancia de las pruebas, es interesante ver que hay muy poca información para saber hacer las pruebas. La ausencia de ésta información, en cambio, contribuye a que se den mitos de que las pruebas necesitan ser realizadas antes de que se inicien las discusiones de las técnicas de prueba.

Uno de los mitos mencionados anteriormente es: que con las pruebas se intenta hacer que el plan de verdad funciona. Aquellos que adoptan ése punto de vista, llegan a la conclusión inevitable, de que las pruebas que demuestren errores o fallas en el procedimiento del plan son ¨ fallas de pruebas ¨.

Un segundo mito se comenta por los expertos de la industria como un ¨ mito de realismo ¨. Específicamente, los que tienen éste punto de vista insisten en que para que una prueba sea útil, se deben simular las mismas condiciones de un desastre real – al punto de interrumpir las operaciones normales de los sistemas. Es interesante ver cómo, algunos profesionales de redes y sistemas, siguen temerosos hacia aquellas pruebas porque tienen la idea de que las pruebas requieren un corte de los sistemas operacionales y redes, para simular las condiciones de un desastre. Esto va en contra de minimizar las caídas de sistemas.

De hecho, los sistemas operacionales y redes, no se deben interrumpir en las pruebas. Generalmente, las pruebas se llevan a cabo al mismo tiempo con los procesos normales, pero de manera independiente o en paralelo para producir datos comparativos acerca de las operaciones del servidor y los respaldos. Aún en los llamados ¨ desastres falsos ¨, la interrupción de los procesos normales no es necesaria, y da como resultado problemas en las pruebas.

Tal vez, en algunos casos si será necesaria un interrupción real, obviamente el equipo que se requiera para participar en las pruebas, no podrá estar haciendo su trabajo normal. Debido a esto, es válido para algunos encargados de la planeación, preguntar, qué tan disponibles estarán para mantener un proceso normal y llevar a cabo una prueba, dado los requerimientos de equipo que se necesitan para cada actividad. La solución sería llevar a cabo pruebas en períodos cortos en, temporadas en las que no sea necesario mucho procesamiento, en cambios alternos o en fines de semana.

Además de estos dos mitos, existe el que es derivado del ¨ mito de insuficiencia ¨. Muchas empresas posponen las pruebas hasta que el plan de recuperación pueda ser probado en su totalidad. La razón a ésta postura, es que la capacidad constituye una red compleja de interdependencias entre el sistema, red, y las estrategias de recuperación de usuario y que probar solamente una subsección del plan, da como resultado solo un poco de información útil. Los promulgadores del mito, discuten que las estrategias del plan no pueden ser validadas por

pruebas aisladas de los procedimientos específicos del plan, y que los participantes de dichas pruebas no tendrán éxito en la obtención de una visión global de la capacidad de recuperación (un propósito establecido de pruebas).

De hecho, como se ha venido mencionando, los planes de recuperación se construyen mejor por módulos, organizados alrededor de las funciones discretas de negocios y sus recursos de automatización asociada. De ésta forma, los resultados de una prueba generalizada no serán complicados por los errores de los procedimientos.

Uno de los últimos mitos es el de ¨ preparación ¨. Asumir que las pruebas, preparan a la empresa para un desastre real. Si la preparación es interpretada como ¨ estar armado en base a un conjunto de estrategias probadas para amortiguar una interrupción no planeada ¨, entonces es lo correcto. De todas formas muchos responsables de la planeación, que buscan una prueba generalizada o una prueba más ¨ real ¨ del plan, a menudo lo hacen, porque ellos creen que eso prepara a los participantes a la ¨ realidad ¨. Pero esto no es verdad.

El hecho de que el plan, se halla probado el mes pasado, no significa que la empresa está totalmente preparada para éste mes. Las pruebas familiarizan al personal de recuperación con sus funciones, y dan un repertorio de procedimientos de recuperación, que han sido probados para trabajar bajo circunstancias controladas. Pero, así como las recuperaciones de varias empresas lo atestiguan, la recuperación exitosa en una crisis actual, es comúnmente el resultado de una combinación de factores, incluyendo la estrategia de recuperación probada, un equipo ingenioso y leal, buena administración, la participación efectiva de los proveedores, y muchísima suerte. Es imposible predecir, todas las consecuencias de un desastre. Debido a esto, ninguna prueba puede equipar completamente a una empresa para recuperarse de por sí misma en una emergencia.

Frecuencia de pruebas.

Una de las preguntas más frecuentes en las juntas y conferencias de PLRD es: cuándo debemos probar nuestro plan, debido a la velocidad con la que ocurren los cambios en la mayoría de las redes y sistemas de las empresas, es importante identificar la frecuencia apropiada para probar el plan, tomando en cuenta:

1. Si es consistente con las limitaciones del presupuesto
2. Si da la información necesaria para mantener el plan actualizado con los cambios en los negocios que se deban proteger.

Probando con el proyecto del plan.

La iniciativa del plan, es mejor manejada como un proyecto, controlado y administrado usando técnicas familiares de administración de proyectos. Las tareas del proyecto del PLRD, se derivan de los objetivos del proyecto, ordenadas de acuerdo a prioridades, y recursos asignados, presupuestos y marcos de tiempo para terminarse.

* La terminación de todo el proyecto (y cada uno de los subproyectos orientados a tareas) ocurre en tres situaciones universales: análisis, implementación y evaluación. En la etapa de análisis, el problema o tarea se define y se identifican soluciones alternas. Cuando se selecciona una solución específica, ésta se implementa. Entonces, para confirmar que la solución implementada satisface los objetivos de la tarea o proyecto, está sujeta a una prueba de validación como parte de una etapa de evaluación.

En el contexto del proyecto de PLRD, la etapa de evaluación es muy importante. Las salidas de las tareas (formadas por procedimientos, objetivos) son escudriñadas para asegurarse de que las tareas se hallan completado totalmente. Éste paso de evaluación/validación, se requiere para asegurarse de que todos los subcomponentes del proyecto trabajarán juntos al final para satisfacer los objetivos principales del proyecto de PLRD.

El punto es, que las pruebas son un componente natural del alcance del proyecto administrativo. Las pruebas validan las salidas o resultados específicos de las tareas del proyecto y verifica que los resultados combinados encuentren los objetivos del proyecto en

general. Como una parte integral del PLRD, las pruebas deben ser de acuerdo al estado de las tareas y al presupuesto asignado, recursos y tiempo. Las pruebas deben abarcar cualquier combinación de los módulos y objetivos del plan, y deben ser conducidos tan frecuentemente como el equipo de planeación lo desee.

Por ejemplo, para la prueba de una estrategia, a la que se le ha probado su efectividad en numerosos esfuerzos de recuperación de manera exitosa en los últimos años, nos propone una fórmula de siete pruebas en tres años, que debe ser emulada. De acuerdo con la fórmula, las estrategias desarrolladas por la empresa para recuperar el sistema de operaciones del mainframe, aplicaciones críticas, y telecomunicaciones de redes, deben ser probadas de manera separada en tres pruebas el primer año al terminar el plan. Tales pruebas orientadas a estrategias nos dan los medios para refinar a las mismas estrategias antes de hacer cualquier prueba generalizada.

En el segundo año, los encargados de la planeación son alentados a realizar por lo menos dos pruebas. Una debe ser otra prueba a cualquiera de las hechas del primer año (sistema operativo, aplicaciones, o redes) en las cuales se halla encontrado cualquier problema. La segunda prueba debe ser una de procesamiento, en la cual un ciclo de procesamiento de aplicación completa, se haga en las instalaciones de respaldo. Ésta nos puede dar una referencia de información útil que ayudará a los encargados de la planeación en predecir los requerimientos de tiempo y marcos de producción para una situación de procesamiento de emergencia actual.

Las pruebas del proyecto concluyen en el tercer año, con otras dos pruebas. Una debe consistir en probar de manera paralela las aplicaciones críticas o de procesamiento de un cambio en particular o de una temporada pico (por ejemplo: el procesamiento de fin de mes) para obtener información de control adicional. Para la última prueba, se recomienda simular un desastre, en el cual el sistema operativo, aplicaciones y redes sean llevadas al site de respaldo.

En resumen, bajo el alcance administrativo del proyecto, al menos se llevan a cabo siete pruebas en los primeros tres años después de que el plan se halla desarrollado. El resultado de todo esto es formativo; con lo que se logrará lo siguiente:

- Ayuda al equipo de planeación en afinar las estrategias de recuperación de manera individual.
- Provee en base a los datos, sobre el rendimiento del sistema, que es lo que se requiere para construir un plan administrativo de emergencia confiable.
- Al final, se prueba qué tan bien los diferentes componentes de estrategias trabajan juntas para dar un soporte completo de recuperación de los sistemas críticos y redes en el centro de respaldo del mainframe.

Estas pruebas deben ser organizadas en una agenda y se les debe asignar un presupuesto en el mapa del proyecto de PLRD. Éstas constituyen la fase de evaluación del proyecto y dan la retroalimentación que se requiere para completar la misión del proyecto: el desarrollo de la capacidad demostrada de recuperación de desastre.

Las pruebas como un cambio en la función administrativa.

¿Qué sucede después del tercer año? Como todos los proyectos que resultan en sistemas complejos, existe el detalle, del mantenimiento y el cambio administrativo a considerarse en el plan. Las redes y los sistemas cambian igual que los negocios al paso del tiempo. Los procedimientos del cambio administrativo son una parte importante del PLRD y trabaja para asegurarse de que las estrategias documentadas, procedimientos, relaciones con los proveedores, etc. se mantengan actualizados.

La predisposición del cambio administrativo, es manejada más que nada por los eventos que por los horarios del proyecto. La necesidad de volver a probar la capacidad del plan desde el punto de vista del cambio administrativo se originará de diversas fuentes:

- Actualizaciones principales del sistema operativo.– Siempre que exista una actualización importante para el sistema operativo o para alguna utilería que afecte a los núcleos del sistema del mainframe, se debe organizar una prueba.
- Cambios del software de las aplicaciones críticas.- el PLRD utiliza las funciones de negocios para clasificar el software de aplicaciones como crítico o no crítico. Cuando se agregan las nuevas aplicaciones, cuando se actualiza el software existente, o cuando se aplica el cambio del software de un proveedor a otro, éstos eventos originarán la necesidad de hacer otra prueba en el cambio administrativo.
- Cambios importantes de hardware.- cuando el CPU o algún otro componente de hardware se cambie, tanto del hot site o en las instalaciones de respaldo del mainframe, los encargados de la planeación necesitarán volver a probar los planes de respaldo. Los encargados de planeación que utilicen un sistema de respaldos del mainframe comercial, se deben asegurar consultar los contratos del servicio, para determinar cuánto avance notorio recibirán debido a los cambios del equipo en el site del proveedor. Algunos proveedores darán cuando mucho 60 días de avance para asegurarse de que sus clientes tengan el tiempo necesario para evaluar el impacto del cambio y para organizar una prueba.

También se deben monitorear los cambios en el hardware y configuraciones de la red. Los cambios de la red algunas veces se pasan por alto, y eso provoca que la recuperación de la red sea lo que más tiempo consuma para la recuperación. Cuando se hagan los cambios sustanciales para las existentes redes de negocios, se deberá hacer otra prueba a la red.

- Cambios de personal. – el porcentaje de tiempo en el que un individuo se mantiene en su trabajo es por lo menos de tres años aproximadamente. Para el personal de sistemas de información, el promedio para que alguien baje de puesto es más alto. Los siguientes cambios clave del personal, cambios de puesto y otras actividades significativas de personal, es por lo general, una buena idea hacer una prueba con propósitos de entrenamiento.

Desde luego, no todos los cambios se harán automáticamente para probarse el PLRD. La mayoría de veces, muchas señales se van acumulando antes de que la opción de una prueba sea retomada.

En algunas empresas, el encargado de la planeación atiende todo tipo de juntas de procesamiento de información de la empresa, o del departamento de sistemas de información. El encargado de planeación ahorra algo de tiempo de la agenda para cada junta para discutir las ramificaciones de recuperación de las nuevas aplicaciones, cambios en los equipos, y reconfiguraciones de redes.

5.3 *Tipos de pruebas*.

- Pruebas por módulos – como su nombre lo indica, éstas nos sirven para probar uno o un conjunto de procedimientos que conforman una parte de la documentación del plan de recuperación. Los propósitos de tales pruebas son mejorar los procedimientos, identificar descuidos o errores, o recopilar estadísticas de tiempo, útiles para coordinar los objetivos de los procedimientos con otros.
- Pruebas por estrategia – éstas son para validar estrategias enteras o para determinar los tiempos de implementación de las estrategias del

plan. En éstas pruebas, los procedimientos, que han sido sujetos previamente a pruebas modulares, son implementados como si estuvieran en un desastre actual. La información debe estar recopilada de acuerdo a las relaciones entre las tareas de procedimiento, que aparentemente no fueron fáciles o claras de las pruebas por módulos o en descripciones escritas.

- Pruebas paralelas – son hechas como parte de una prueba de estrategia. En éstas pruebas, las redes y sistemas son operadas al mismo tiempo con las operaciones normales del servidor. Las cargas de producción son aplicadas a los sistemas de respaldos y las redes simulan la operación de los recursos de respaldo

Los resultados de la prueba son:

1. la validación de la capacidad de la estrategia de recuperación para manejar la carga de trabajo anticipada de la restauración de las funciones de negocios.
2. información útil de los marcos de tiempo de producción en modo de respaldo, que puede ser de ayuda en establecer los cambios en la agenda para un ambiente de producción de operaciones de recuperación.

Las pruebas paralelas son mejor estructuradas como modelos comparativos, en otras palabras, las pruebas deben aplicarse a un objetivo específico, como por ejemplo una aplicación completa de ciclo de producción, un cambio de horario de producción especifico, o a una función específica de negocios. Múltiples pruebas paralelas deben ser realizadas en horas extras para emular la actividad de procesamiento diaria, de fin de mes, primer y segundo cambio, de producción, etc. Para relacionar una prueba paralela a un modelo de objetivo específico, se debe obtener la información comparativa más útil.

- Simulación de desastres – estas son pruebas del plan administrativo de emergencia. Generalmente, una simulación de éste tipo se hace después de haber hecho las pruebas antes mencionadas. En este caso, se hace un escenario de desastre y los equipos de recuperación usan los procedimientos para implementar ésas partes del plan de recuperación que se requieren para enfrentarse a la interrupción. Desde luego, los sistemas y redes en la simulación no se desactivan. La prueba simularía un problema y se evaluaría la reacción del personal de recuperación.

Todas estas pruebas se hacen en dos formas:

Conferencia
La prueba se hace en una junta, con los participantes indicando lo que harán y cuando. Esto es como parte de una preplantación para cualquier prueba (excepto en simulación de desastres sorpresa).

Simulaciones.
En una simulación, la prueba se hace con el equipo actual.- a los proveedores apropiados se les avisa y se implementa una parte del plan. Esto nos ofrece una gran retroalimentación en procedimientos e implementación de marcos de tiempo.

Cómo hacer las pruebas.

Las pruebas y el desarrollo de un sistema de cambio administrativo, son componentes críticos del proyecto y deben ser tratados como un evento del proyecto. La tabla (5-6) resume la mayoría de las actividades de las pruebas y mantenimiento del plan.

5.4 *Desarrollando estrategias para hacer pruebas*.

Para hacer una prueba, primero se debe hacer una estrategia. La figura (5-7), nos da una forma para usarse en el desarrollo de los objetivos generales de una prueba. Ésta se debe usar en conjunto, con cualquiera de las opciones de prueba previamente articuladas.

En la parte superior de la forma, se da un espacio para ingresar los cinco objetivos generales de la prueba. Los objetivos deben establecer lo que se hará y qué criterios se usarán para medir los resultados. Un ejemplo para esto, puede ser: ¨ para restaurar las comunicaciones entre las oficinas principales de la empresa y las instalaciones de respaldo del mainframe en tres horas y para probar las comunicaciones a través de simulación de cargas de trabajo. ¨

Desde luego, una prueba también debe tener un objetivo de recopilación de información. fig(5-8) Puede quedar de la siguiente manera: ¨ para determinar el tiempo de respuesta, en la reincorporación del usuario (ubicado en una terminal del departamento de contabilidad), en las instalaciones, tomando en cuenta la restauración de los enlaces de sistemas y comunicaciones entre las instalaciones de respaldo del mainframe y las de reincorporación del usuario. ¨

Los objetivos adicionales deben ser registrados en hojas de estrategia adicionales, con el número total de hojas indicadas en la parte baja de la forma. Dependiendo de que tan específicos se hayan establecido los objetivos de las pruebas, un número significativo de objetivos deben ser expuestos para cada prueba.

La parte baja de la forma (5-7) se usa para registrar la agenda de la prueba, el o los lugares elegidos para la prueba, y para enlistar la unidad de trabajo administrativa y proveedores que deberán ser contratados para

EL PROYECTO DE RECUPERACIÓN DE DESASTRE.
PLAN DE PRUEBAS Y MANTENIMIENTO.

ACTIVIDADES PRINCIPALES

Desarrollar una estrategia de pruebas
Desarrollar una agenda de pruebas
Implementar pruebas y documentar resultados
Diseñar e implementar cambios del sistema administrativo
Desarrollar una agenda de mantenimiento del plan

EL PROYECTO DEL PLAN DE RECUPERACIÓN DE DESASTRES

(2-5)

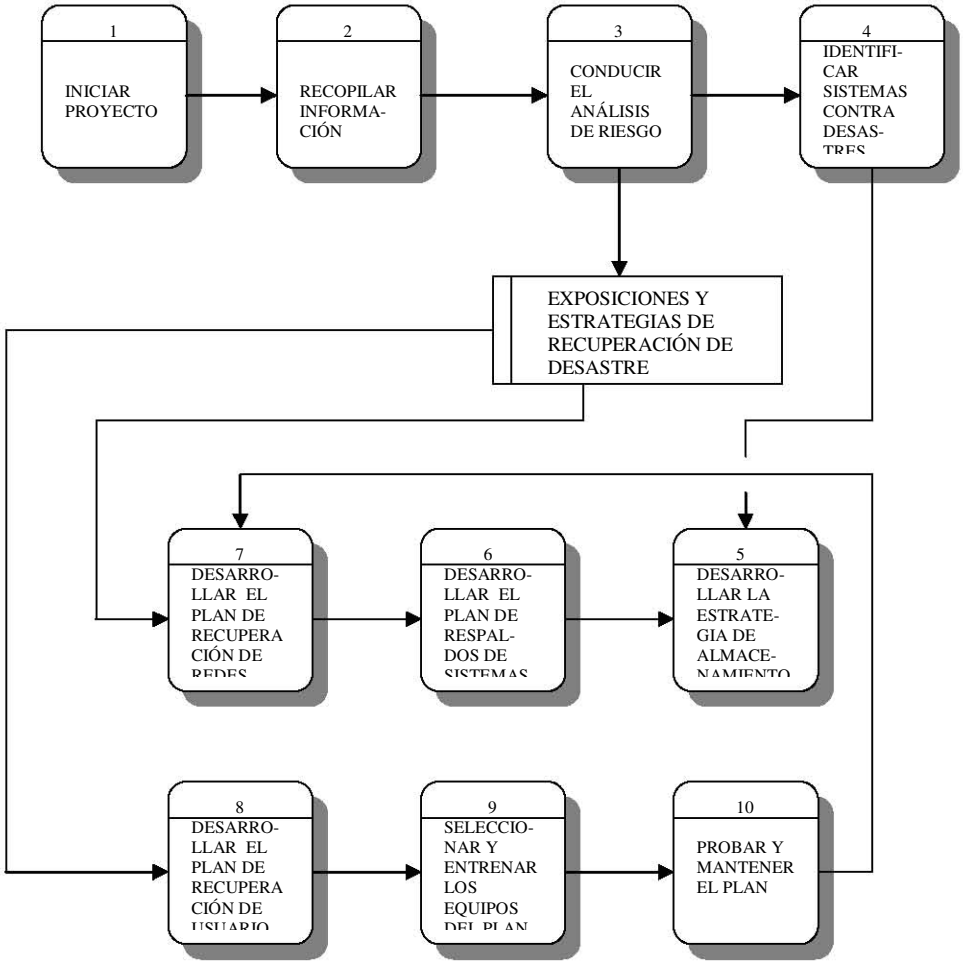


TABLA (5-6)

FIG(5-7) HOJA DE ESTRATEGIAS (para Pruebas).

Objetivos de la prueba.
Instrucciones: enlistar los objetivos generales de la próxima prueba. Incluir los criterios para evaluar los resultados de la prueba o los objetivos específicos de recopilación de información. Agregar más páginas si es necesario.

1 _____
_____
2 _____
_____
3 _____
_____
4 _____
_____
_____
5 _____
_____
_____

Agenda de la prueba

Fecha y duración de la prueba: _____
Locación (es): _____
_____
_____
_____

Unidades de trabajo involucradas: _____
(incluir contacto de información) _____
_____
_____
_____
_____

Proveedores involucrados: _____
(incluir contacto de información) _____
_____
_____
_____
_____
_____
_____
_____

página 1 de ____

coordinar las actividades de prueba. Ésta agenda de prueba será mejorada al igual que la estrategia de prueba que será desarrollada más detalladamente.

Para ayudar en el desarrollo de la estrategia para pruebas, una segunda hoja debe ser utilizada para poner los detalles de cada objetivo establecido de prueba. Como se muestra en la figura (5-8) una hoja con los detalles de los objetivos de las pruebas es completada para cada objetivo formado en la hoja de *Estrategia para Pruebas.*

En la parte superior de la forma, el encargado de la planeación indica el objetivo *(ubicado en la Hoja de Estrategias para Pruebas 5-7)* general de la prueba a la cual la *Hoja de Objetivos para Pruebas* pertenece. Los equipos que estarán involucrados en las tareas descritas por los objetivos son identificados igual que los procedimientos involucrados más relevantes del plan. Finalmente, se ponen en una lista los resultados anticipados de las pruebas.

FIG(5-8) HOJA DE OBJETIVOS (para Pruebas).

Instrucciones: Completar esta hoja para cada objetivo de prueba general indicado en la hoja (5-7) de estrategias de prueba.

Enlistar el objetivo de la prueba general al cual ésta hoja pertenezca: _____

Equipos involucrados: _____

Identificar procedimientos relevantes del PLRD: _____

Describir resultados anticipados de pruebas: _____

Requerimientos de recursos de la prueba

Recursos de sistema: _____

Recursos de redes: _____

Almacenamiento externo: _____

Formas y registros: _____

El pie de la forma se utiliza para registrar los requerimientos de los recursos de la prueba. Los encargados de la planeación deben identificar qué recursos de sistema, redes, almacenamiento externo se usarán y que otras formas, registros se necesitarán.

5.5 *Organizando las pruebas*.

Las estrategias de pruebas, frecuentemente son desarrolladas como el esfuerzo de un equipo, como una entrada de los líderes del equipo de recuperación, unidad administrativa, representantes de proveedores, autores y otros. Generalmente, uno o más miembros de éste equipo de planeación de pruebas, será el responsable de seguir con otras actividades de pre-planeación, que están resumidas en la figura (5-9).

FIG(5-9) LISTA DE REVISIÓN DE PRE-PLANEACIÓN DE PRUEBAS.

¿se han confirmado las fechas de la prueba? ☐

¿se les ha avisado a los participantes de las pruebas? ☐

¿se les ha avisado a los proveedo-res? ☐

¿se les ha avisado a los gerentes de las unidades de trabajo? ☐

¿se le ha avisado a la gerencia corporativa de la prueba? ☐

¿se han revisado los medios de almacenamiento para enviarse? ☐

¿se han arreglado el hospedaje y los viajes para los participantes de la prueba? ☐

¿los procedimientos relevantes de recuperación han sido copiados y repartidos a los participantes de la prueba? ☐

la estrategia de prueba, objetivo, las hojas de evaluación de pruebas, ¿se han preparado? ☐

¿han dado instrucciones los observadores y participantes acerca de los objetivos de las pruebas? ☐

Preparado por: _____
Fecha: _____
Aprobado por: _____
Fecha: _____

Preplanear una prueba es un componente importante para el éxito de una prueba. La pre-planeación se usa para definir los requerimientos logísticos de una prueba: establecer el marco de tiempo de prueba y asi organizar la instalación de respaldo del mainframe, para saber qué personal estará involucrado en la prueba, qué arreglos de almacenamiento y viajes se deben hacer, etc.

En la pre-planeación, también se incluyen unas cintas de emergencia y accesorios almacenados en el off-site con el objetivo de asegurarse de que todas los respaldos estén listos para usarse. Mientras que esto se debe ver como un arreglo de la prueba, es importante verificar que todas las cintas de respaldo estén disponibles y en buenas condiciones para asegurarse de tener una prueba bien preparada. En una crisis actual, pre-probar las cintas de respaldo seria imposible. Hasta que exista un objetivo de la prueba actual para ver cómo los

equipos de recuperación se enfrentan con cintas dañadas, ésta variable puede ser controlada para propósitos de pruebas. Por otro lado, si se descubren respaldos inadecuados o dañados en la preplaneación, esto será notorio, se descubrirá la causa, y se tomará una acción preventiva de los respaldos defectuosos en caso de un desastre real.

Otro aspecto importante en la preplaneación, son los pasos de preparación que se toman antes de implementar la prueba. Una sesión de planeación es un excelente foro para reunir a representantes de proveedores y a los participantes de la prueba para tomar un camino estructurado para los procedimientos de pruebas. Revisando los procedimientos relevantes del PLRD con todos los que estarán involucrados, algunos descuidos podrán ser identificados antes de que la prueba comience. El personal del site de respaldo, también debe estar disponible para que contribuya con su conocimiento específico del site para refinar los procedimientos y objetivos de la prueba. Las sesiones de planeación también dan un foro para las ideas geniales acerca de los desastres actuales. Cada procedimiento de recuperación descansa en una suposición no discutida o comentada acerca de las condiciones en las que el procedimiento será iniciado. Pasar un tiempo con el equipo de pruebas para identificar y desafiar algunas de éstas suposiciones, puede ayudar a identificar algunas contingencias que puedan ser adoptadas en el informe del procedimiento.

En la conclusión de la preplaneación, serán confirmadas las fechas establecidas para la prueba, sus participantes, proveedores, unidad administrativa, y los directivos serán notificados de la prueba, los recursos serán revisados y verificados, viajes, hospedajes, preparaciones logísticas serán completadas, procedimientos relevantes serán fotocopiados y distribuidos a los líderes de los equipos de planeación, se completarán todas las formas necesarias y los participantes de las pruebas y observadores serán completamente informados de lo que se requerirá de ellos en la documentación y evaluación de los resultados de la prueba.

5.6 *Implementando la prueba y documentando resultados*.

Se implementará el plan en las fechas y tiempo establecidos. Se debe hacer notar que casi cada prueba incluye la restauración del sistema operativo, y muchos incluyen las pruebas de las aplicaciones seleccionadas, o la restauración de las funciones de negocios, que las aplicaciones soportan.

Las pruebas también se deben enfocar en la restauración de las redes, aumentando el interés para los encargados de la planeación, para el momento en el que el servicio (carriers) de las comunicaciones sea interrumpido. La restauración de redes tiene algunos problemas especiales para la recuperación (tanto en el punto de vista del cambio administrativo como en la perspectiva de los requerimientos de pruebas). Ahora, la restauración de redes se requiere para reconectar los sistemas recuperados para los usuarios que hagan un trabajo importante.

Cualquiera que sea el objetivo y enfoque de la prueba, una hoja adicional, mostrada en la figura (5-10) debe ser adaptada para que ayude en la evaluación de la prueba. El coordinador de la prueba, debe preparar la hoja ingresando el objetivo general en la parte superior de la forma, entonces, se resumen los objetivos y criterios de la prueba en la columna izquierda de la forma. Se le sacan copias a la forma y se distribuyen a los individuos que estarán involucrados en la prueba, ya sea como participante u observador, y que se requerirá para dar un reporte de los resultados.

Siguiendo la implementación de la prueba, los resultados y observaciones de los evaluadores, serán ingresados en la columna derecha de la forma y en la parte baja de la segunda página. Ésta forma nos da una documentación fácil de usarse de los resultados de la prueba que el coordinador pueda revisar para identificar los requerimientos de los cambios del

plan. Además de las hojas, las ideas de los participantes y observadores de la prueba, también deben ser analizadas para ver si pueden ofrecer algo a los requerimientos para refinar los procedimientos y ayudar en los objetivos para futuras pruebas. Cada participante debe ser interrogado, y se deben incluir sus observaciones en los documentos de la prueba. Esto se logra comúnmente en un grupo, donde los participantes y observadores estén disponibles para revisar los resultados de la prueba de manera conjunta y aclarar sus propios informes.

Los resultados de las formas están resumidas en una hoja de reportes mostrada en la figura (5-11). La hoja empieza con una forma de llenado con la descripción de la prueba, indicando cuándo y dónde se llevó a cabo y su enfoque general. Se hace una lista con los participantes y observadores. Éstos se identifican por su nombre, organización y función. Cada participante/observador debe completar las hojas de evaluación.

En la segunda página, se resumen los resultados de la prueba. El primer resumen indica la información que se obtuvo de la prueba. Los resúmenes deben incluir una variedad de información, por ejemplo; una prueba modular debe haber revelado que un conjunto de procedimientos no lograrán los objetivos deseados en el marco de tiempo requerido. Ésta información no debe ser interpretada como una falla en la prueba, pero sí como una información importante de viabilidad de un procedimiento probado y debe ser registrado en la forma del reporte.

FIG(5-10) HOJA DE EVALUACIÓN DE PRUEBAS .

INSTRUCCIONES: (Para el coordinador de pruebas) Copiar en ésta forma los criterios específicos y las finalidades para un objetivo de prueba. Copiar y distribuir a cada participante y observador de la prueba. (para el participante/observador) Junto a cada objetivo o criterio relacionado al objetivo de prueba indicado, señalar el resultado de la prueba. Resumir las observaciones en la página 2. si se requieren los cambios en el procedimiento en el plan de recuperación, agregar una copia del procedimiento en existencia al reverso de éste documento y presentar la forma completa, con todo los anexos al coordinador de la prueba.

Objetivo de la prueba: ______________________________
____
____
____

OBJETIVOS O CRITERIOS DE LA PRUEBA	RESULTADOS DE LA PRUEBA

página 1 de 2

OBJETIVOS O CRITERIOS DE LA PRUEBA	RESULTADOS DE LA PRUEBA

Fecha de evaluación: Evaluado por:

RESUMEN DE OBSERVACIONES (Firmar y poner fecha. Agregar páginas adicionales si es necesario.)

Página 2 de 2

Fig (5-11) HOJA DE PRUEBA CON REPORTE

Resumen de la prueba

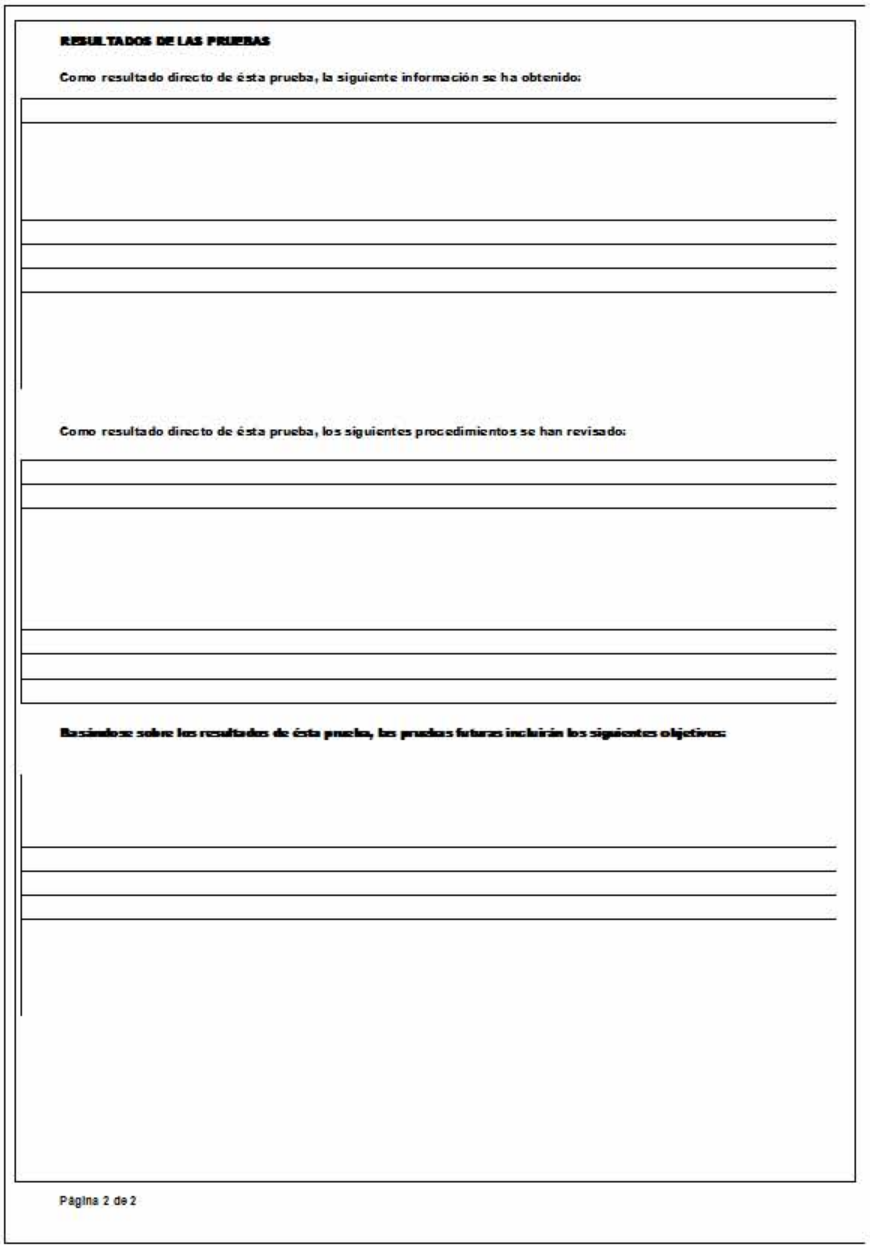
Una prueba de la empresa ____________ del Plan de Recuperación de Desastre se realizó desde (fecha/duración): __/___ ____:____ hasta (fecha) ____/____ ____:_____ en (locaciones)______________________________
____
____
____

La prueba abarcó (revisión de todas las aplicaciones): ( ) recuperación de sistemas operativos, ( ) recuperación de aplicaciones, () ( ) recuperación de redes, ( ) recuperación en función de negocios. Se anexan los objetivos específicos de las pruebas y las evaluaciones.

Participantes de la prueba. Las siguientes personas participaron en la prueba y han completado las evaluaciones.

NOMBRE	UNIDAD DE TRABAJO O EMPRESA CARGO

Página 1 de 2



RESULTADOS DE LAS PRUEBAS

Como resultado directo de ésta prueba, la siguiente información se ha obtenido:

Como resultado directo de ésta prueba, los siguientes procedimientos se han revisado:

Basándose sobre los resultados de ésta prueba, las pruebas futuras incluirán los siguientes objetivos:

Página 2 de 2

Por otro lado, la información obtenida de una prueba debe ser completamente objetiva. En una prueba de procesamiento paralelo, por ejemplo, el tiempo y otra información de rendimiento deben ser tomados de tal forma que nos dé una entrada útil para el plan administrativo de emergencia. Ésta información, también debe ser registrada.

Las locaciones adicionales también aparecen en la parte superior de la forma para especificar los cambios de los procesamientos que se han hecho como resultado de la prueba y para indicar nuevos objetivos (en la pagina 2), sugeridos por la prueba actual, que guiarán el desarrollo de las estrategias de prueba en el futuro. Como parte de la evaluación de la prueba, los participantes revisan los errores en los procedimientos de pruebas existentes y se les pide anexar las versiones revisadas de los procedimientos de sus evaluaciones. Estas revisiones deben ser examinadas por el coordinador de la prueba y si es apropiado, se registrará en el PLRD.

Los nuevos objetivos deben surgir de las evaluaciones de las pruebas. Los nuevos objetivos, también deben repetir los objetivos pasados que no fueron realizados o los cuales necesiten volverse a probar por las revisiones de los procedimientos.

Diseñar e implementar el sistema administrativo de cambios.

Porque dan una retroalimentación al proceso del desarrollo del plan, las pruebas son más que un ensayo o ejercicios de entrenamiento. Son el comienzo de un proceso de cambio administrativo que continuará después de que se complete el proyecto del PLRD.

Este cambio de procedimiento administrativo tendrá muchos componentes, incluyendo los siguientes.

5.7 *Políticas de la empresa en el mantenimiento del PLRD.*

Los encargados de la planeación deben esforzarse para salvaguardar la inversión de la empresa en la preparación de los anteproyectos (borradores) de muchas políticas, exhortar la adopción y apoyo de los directivos. El establecimiento de políticas, debe dirigirse por la necesidad de las pruebas en marcha del PLRD; se requiere a la unidad de trabajo administrativa para comprometerse en revisiones periódicas y actualizaciones de sus propios planes de recuperación; para dar los fondos necesarios para el mantenimiento del plan, entrenamiento del equipo de recuperación, programas para conciencientizar a toda la empresa, y para dar un reporte anual de todas las actividades de preparación de desastres a la parte directiva.

El establecimiento de un coordinador de tiempo completo del PLRD.

Idealmente, las políticas también establecerán la función del coordinador del plan en una posición de tiempo completo en la empresa. Éste debe trabajar para asegurarse que otras políticas previstas sean tomadas en cuenta y puedan servir como la conexión con el actual proveedor y coordinador de pruebas.

Sistemas administrativos de cambio formal.

Se deben establecer reportes para facilitar la comunicación de las revisiones del plan con el coordinador, de tal forma que el plan pueda ser revisado y mantenido en un estado de constante actualización. Tal sistema se arma con las figuras (5-12) hasta la (5-16).

Los cambios en la administración dependen de la comunicación. Formalizando la comunicación con el uso de las formas, aquellos que requieran cambios pueden expresar sus necesidades de manera simple y directamente. (El uso de un cuestionario de cambios estándar también ayuda en la conversión de lo escrito a mano a un medio electrónico. Por eso, las formas descritas aquí, se pueden usar para iniciar una base de datos para cambio administrativo más sencillo).

Las tablas (5-12) a la (5-14), tienen gran similitud. Son iguales excepto por las selecciones de definición de cambios y sus títulos. Como se indica en los títulos, la (5-12) se utiliza por la unidad de trabajo administrativa o sus coordinadores de recuperación, para presentar la solicitud de cambios al coordinador de recuperación corporativo. La tabla (5-14), se usa para el personal de administración de redes.

En cada caso, el uso de la forma es simple. El solicitante pone fecha a la petición, se identifica con su nombre y unidad de trabajo (o puesto), y da su teléfono.

Después, el solicitante identifica los cambios que puntualiza la petición. Esto se hace revisando las opciones apropiadas en una lista de opciones. Los detalles de los cambios se resumen en el espacio dado, y al solicitante se le pide dar documentación adicional para que se describa mejor el cambio.

En muchos casos, se usará la forma para aconsejar o avisar al coordinador del plan, en los cambios de información (por ej., cuando un contacto o un subordinado cambia de trabajo, se reasigna o reemplaza, un nuevo contacto, se da un número telefónico al coordinador y así se mantenga el directorio de notificaciones). En otros casos, cambios igual de simples facilitarán la petición.

HOJA DE CAMBIO ADMINISTRATIVO.
VERSIÓN DE LA UNIDAD DE TRABAJO

IDENTIFICACIÓN DEL ENCUESTADOR /PROPÓSITO DE LA ENCUESTA

Fecha de la encuesta:
Nombre del entrevistador: _____
Unidad de trabajo del administrador: _____
Teléfono del entrevistador: _____
_____

_____ Cambios en los procedimientos de la unidad de trabajo
_____ Cambios en el personal
_____ Cambios en el equipo
_____ Cambios en el software de aplicación
_____ Cambios en los requerimientos de registros
_____ Cambios en seguridad
_____ Cambios en procedimientos de seguridad
_____ Cambios en la tabla de notificación
_____ Cambios en los requerimientos de prevención
_____ Cambios en los requerimientos de comunicaciones
_____ Otros cambios (ver abajo)

DESCRIPCIÓN DE LOS CAMBIOS (Agregar páginas adicionales como sea necesario. Indicar los módulos afectados del procedimiento del PLRD).

Por favor entregar ésta solicitud de cambios a:
Mario Olivos Rojas
Coordinador de Recuperación de Desastres
Empresa Patomex

Tabla (5-12)

HOJA DE CAMBIO ADMINISTRATIVO.
VERSIÓN DE SISTEMAS DE INFORMACIÓN

IDENTIFICACIÓN DEL ENCUESTADOR /PROPÓSITO DE LA ENCUESTA

Fecha de la encuesta:
Nombre del entrevistador: _____
Unidad de trabajo del administrador: _____
Teléfono del entrevistador: _____
_____

____ Cambios en los procedimientos
____ Cambios en el personal
____ Cambios en el equipo
____ Cambios en el software de aplicación
____ Cambios en los requerimientos de configuración
____ Cambios en procedimientos de seguridad
____ Cambios en la tabla de notificación
____ Cambios en los requerimientos de prevención
____ Cambios en los requerimientos de comunicaciones
____ Otros cambios (ver abajo)

DESCRIPCIÓN DE LOS CAMBIOS (Agregar páginas adicionales como sea necesario. Indicar los módulos afectados del procedimiento del PLRD).

Por favor entregar ésta solicitud de cambios a:
Mario Olivos Rojas
Coordinador de Recuperación de Desastres
Empresa ¨X¨

Tabla (5-13)

HOJA DE CAMBIO ADMINISTRATIVO.
VERSIÓN DE REDES

IDENTIFICACIÓN DEL ENCUESTADOR /PROPÓSITO DE LA ENCUESTA

Fecha de la encuesta:
Nombre del entrevistador: _____
Unidad de trabajo del administrador: _____
Teléfono del entrevistador: _____
_____

_____ Cambios en los procedimientos operación
_____ Cambios en el personal
_____ Cambios en el equipo
_____ Cambios en las instalaciones
_____ Cambios en los servicios del proveedor
_____ Cambios en procedimientos de seguridad
_____ Cambios en la tabla de notificación
_____ Cambios en los requerimientos de prevención
_____ Cambios en los requerimientos de comunicaciones
_____ Otros cambios (ver abajo)

DESCRIPCIÓN DE LOS CAMBIOS (Agregar páginas adicionales como sea necesario. Indicar los módulos afectados del procedimiento del PLRD).

Por favor entregar ésta solicitud de cambios a:
Mario Olivos Rojas
Coordinador de Recuperación de Desastres
Empresa ¨X¨

Tabla (5-14)

HOJA DE RESPUESTA DEL CAMBIO ADMINISTRATIVO

INSTRUCCIONES: (Para el coordinador) Agregar la hoja de solicitudes del cambio administrativo. Copiar y agregar la documentación de procedimientos relevantes. Circular para su aprobación y revisión. (Para el revisor) Revisar la solicitud de cambio administrativo anexa. Indicar el impacto en el plan y las recomendaciones para revisarse y probarse. Regresar en una semana a Mario Olivos Rojas, coordinador del plan de recuperación de Patomex.

Dirigido a (nombre del revisor): _____
Teléfono/ correo: _____
Fecha de envío: _____
Objetivo del cambio:

RESULTADOS DE LA REVISIÓN

Acciones requeridas:

___ Revisar procedimientos
___Obtener información adicional
___Volver a probar el módulo del plan
___Volver a probar la estrategia del plan

NOTAS

Secciones del plan impactadas:

___Descripciones de la Unidad de Trabajo
___Módulos de procedimiento
___Descripciones de estrategia
___Configuración
___Plan administrativo de emergencia
___Directorio de proveedores
___Directorio de notificaciones
___Plan de respaldo externo
___Sistemas preventivos

NOTAS

Tabla (5-15)

SOLICITUD DE CAMBIO ADMINISTRATIVO

# SOL	CAMBIO SOLICITADO	REVISADO POR	CAMBIO RECOMENDADO	FECHA DE CAMBIO	PRUEBA	FECHA DE PRUEBA

Tabla (5-16)

De todas formas, los cambios tendrán consecuencias de difícil alcance para el plan de recuperación. Este es el caso especial cuando hay una reorganización de todas las unidades de trabajo de la empresa, cuando se agregan nuevos sistemas, o cuando las redes experimentan reingeniería sustancial. Éstos son puntos más difíciles que el coordinador debe manejar solo.

Por eso, la tabla (5-15), da una manera para solicitar la asistencia de técnicos expertos. Con esto se facilita la revisión de las peticiones de cambio con gente con conocimiento (idealmente con el equipo de recuperación o directamente con los líderes de equipos de recuperación). La parte superior de la forma consiste en un espacio usado para dirigir la petición de cambio a un revisor designado, para escribir la fecha de envío, etc. También se da el objetivo general de la solicitud de cambio.

En la parte baja, las respuestas del revisor se capturan en un formato de lista y se resumen los comentarios. Se les pide a los revisores que indiquen, en su opinión, qué acción es requerida. Las acciones deben consistir de procedimientos de revisión, obteniendo información adicional del cambio, volviendo a probar un módulo del plan, o a probar otra vez toda la estrategia del plan. Obviamente, se debe revisar más de una categoría de acción. Se da

un espacio adyacente a las categorías para que el revisor note cualquier consideración o comentario especial.

Una vez que la acción se halla recomendado, el revisor (que debe tener acceso para a una copia completa del PLRD de su versión actual) debe indicar cuál de las secciones listadas del plan, siente que será afectada por el cambio. Los revisores indican sus opciones revisando una o más categorías opcionales y resumiendo cualquier consideración especial en la sección de notas.

Identificando la proposición, resultados de las peticiones de cambio administrativo, y las revisiones, se facilitan con el uso de una forma, como la mostrada en la tabla (5-16). Se puede iniciar una base de datos para suplantar éste documento.

Debido a esto, por el uso de estas formas es posible obtener una retroalimentación directamente de las unidades de trabajo de negocios, del procesamiento de datos y administración de redes para evaluar la retroalimentación y determinar qué es lo que se debe hacer. Los resultados de las pruebas, también, nos darán una entrada útil para mantener el plan al día.

Agenda regularizada de pruebas.

Las empresas deben probar sus PLRD por lo menos una vez al año. Las pruebas deben ser más frecuentes si se considera la aparición de varios cambios administrativos.

Resumen.

Las pruebas del plan y cambios administrativos son herramientas usadas para mantener la capacidad de recuperación que se ha desarrollado por el proyecto de planeación. Por eso, la parte final del proyecto es también la más importante. En ésta parte, las pruebas son realizadas para validar la línea base del plan y el sistema de cambios administrativos se implementa y desarrolla para dar soporte al plan después de que el equipo del proyecto se halla dispersado.

El cambio administrativo también es un candidato de automatización. Los encargados de planeación, deben considerar una base de datos de cambios administrativos usando algún simple programa, y utilizando alguna herramienta de PLRD que lleva integrada ésta parte.

CONCLUSIONES

Sería un desastre, si el evento provoca la interrupción de los servicios de información en una misión crítica a una empresa.

¿Cómo se determina lo que en realidad constituye un desastre para una empresa?

Hay muchos factores por considerar y muchas formas de interpretar y presentar la información, pero éste es un cálculo que es muy específico para cada compañía. Al final, cada encargado de la PLRD (Planeación y Recuperación en Caso de Desastre) debe tener su propia conclusión acerca de la tolerancia de su compañía en caso de tener una interrupción de los servicios de información.

Los planes de acción de emergencia y procedimientos de recuperación son guías y no modelos, que están sujetos a cambiar con el tiempo,

Justificación.

Lo que se espera es justificar los gastos para conducir de una manera formal el análisis de riesgos y así identificar el nivel actual de preparación de la compañía, y sus riesgos específicos. De esta forma se pueden desarrollar sugerencias para realizar un plan que proveerá seguridad a los empleados y dará continuación a los negocios en el momento de un desastre.

Las empresas financieras son las menos tolerantes a las interrupciones, sólo unas 48 horas, antes de que las pérdidas de las funciones de negocios se vuelvan irrecuperables. Las industrias encargadas de distribución pueden mantener sus operaciones hasta 72 horas, mientras que en las industrias de manufactura, compañías aseguradoras, y otras pueden sobrevivir hasta 6 días después de la interrupción. Ésta información representa un porcentaje basado en estimaciones hechas por inspectores del tema. Los encargados de las funciones de negocios pueden ayudar para obtener mayor información para poder calcular el tiempo estimado de interrupción para la empresa

Según los expertos, 72 horas son consideradas ideales para el tiempo de recuperación. Algunos negocios pueden soportar interrupciones más prolongadas, mientras que otras deben realizar los cálculos completos de las pérdidas financieras en el menor tiempo posible. El marco de tiempo para la recuperación que se presentará a la gerencia debe corresponder a los requerimientos de la compañía y no a las 72 horas recomendadas por expertos.

Las grabaciones críticas son aquellas que son requeridas para la recuperación y que sin ellas la recuperación sería imposible. Para los requerimientos legales y auditorias, se recomienda cierto tipo de grabaciones (reportes administrativos, datos de contabilidad, contratos, los libros de la compañía), también deben ser protegidos de una pérdida. También, documentos de propiedad, código fuente del software, patentes en trámite de la compañía, etc. representan una inversión de tiempo y recursos de la empresa, por lo tanto ésos documentos ameritan ser protegidos. Éstos datos también son críticos, aunque no se requieran para mantener las operaciones diarias de la empresa.

Las estrategias a tomar en cuenta son las siguientes:

- Desarrollar una configuración mínima de equipos.- Usando una colección de datos como parte de un análisis de riesgos, es necesario definir cuál es la configuración más adecuada, combinando todas las aplicaciones críticas que el sistema, para la estrategia de respaldos, busca recuperar.
- Identificar los requerimientos en las comunicaciones de datos.- Ya que el proceso de aplicación en el sistema de respaldos será conducido en una locación remota (alternativa al site del servidor), es necesario desarrollar algo para entender cómo es que ésto impactará a las comunicaciones normales con el sistema. Los requerimientos para el usuario

remoto de alguna terminal y redes periféricas deben ser identificados al igual que otras aplicaciones relacionadas con las necesidades de comunicaciones.

- Identificar los requerimientos del usuario.- Dependiendo de la naturaleza del desastre, los usuarios deben permanecer en sus lugares normales de trabajo o ser cambiados a otro lugar para seguir trabajando. La información debe ser recolectada, para definir qué recursos se requerirán en la locación del usuario para reestablecer el proceso y seguir trabajando.
- Evaluar las opciones de respaldo.- Identificando la configuración y otros requerimientos para el sistema de respaldos, el equipo de la PLRD debe buscar una estrategia de respaldos para el mainframe, que cumplirá con todos los requerimientos.
- Evaluar y seleccionar a los proveedores.- El hecho es que más y más compañías están seleccionando proveedores comerciales de recuperación de mainframes, como su solución de respaldos del sistema. En reconocimiento de éste hecho, los encargados de la planeación necesitan saber qué buscar en un vendedor y cómo seleccionar al mejor de acuerdo con sus necesidades.

En otros casos, es preferible documentar todo el hardware de comunicaciones de datos y alinear los requerimientos durante la fase de planeación de recuperación de sistemas, y es ahora cuando se pueden hacer las sugerencias y peticiones a los proveedores de servicios y productos de sistemas de respaldo.

Determinar el número de integrantes del equipo principal de la empresa, los requerimientos de los dispositivos acceso/terminal, y lo necesario para el acceso en comunicaciones de datos, es sólo una parte en la tarea para describir el uso del sistema de recuperación.

El caso más claro en la PLRD reside en una evaluación de riesgo del desastre y los correspondientes potenciales de pérdidas para la compañía. Se debe hacer notar que es difícil o imposible establecer una estadística confiable para saber la probabilidad de que exista un desastre que afecte a una empresa.

Las estrategias de recuperación de sistemas vienen en todas las variedades de gastos y complejidad. La estrategia apropiada para cualquier empresa, es la estrategia que dará la restauración de las funciones mínimas aceptables, periodos de tiempo, y costos.

Se debe tener en cuenta que las estrategias de recuperación de sistemas no son como recetas de cocina. Están inexorablemente relacionadas al usuario final, y a estrategias de recuperación de redes que deben ser revisadas siempre que ésta u otras estrategias, sean armadas completamente.

Las empresas localizadas en pequeñas ciudades que carecen de instalaciones comerciales con éstos servicios, deben hacer acuerdos cooperativos con otras empresas.

Una PLRD no tiene como objetivo recuperar todo en su forma original, en vez de éso, se busca mantener una organización eficiente y temporal diseñada para mantener los requerimientos necesarios hasta que la crisis termine. El objetivo principal es recuperar las configuraciones mínimas tanto de redes como de sistemas que darán soporte a los requerimientos específicos para funciones de negocios que han sido identificados como críticos y vitales.

Las aplicaciones del software deben ser legibles independientemente de las diferentes plataformas que se tengan para facilitar la comunicación entre las aplicaciones, nuevos dispositivos y diferentes tipos de terminales.

Los archivos de información deben estar en un formato compatible con el sistema de operación de destino.

Aunque esto es más complejo de lo que parece, todo esto debe ser examinado meticulosamente y es una tarea más en el esfuerzo para reunir la información.

En una red:

Todo lo anterior también se puede aplicar a transmisión de voz y redes de comunicación de datos. A los cuales se les ha incrementado su uso en soporte.

Trabajar sin consultor externo es conveniente cuando el gasto por el mismo, es demasiado, cuando las capacidades técnicas del encargado de la planeación de la propia

empresa compensen la complejidad técnica que se tenga, o cuando se esté esperando la respuesta por parte del gerente general.

El encargado de la planeación, como gerente del proyecto de recuperación de desastre, es el responsable de la administración y el presupuesto. Ésta responsabilidad incluye:

1 Formular un presupuesto; aprobando los gastos; coordinando con la nómina de la empresa, contabilidad, y documentar los gastos.

2 Hacer contacto con el director general, para presentar, justificar y revisar los planes del proyecto para presentar progresos y solicitar soporte en actividades de planeación y gastos.

3 Hacer contacto con los gerentes de departamento y administradores de sistemas para obtener su cooperación y asistencia en la obtención de datos, implementación de políticas de respaldos y refuerzos, pruebas del plan e instalación de las capacidades de prevención de desastre, trabajar con los gerentes y administradores para resolver conflictos.

4 Seleccionar y contratar a los miembros del equipo del proyecto, trabajar con recursos humanos de la empresa y gerentes de departamento para coordinar los horarios de trabajo, y otros puntos personales.

5 Monitorear el rendimiento del equipo, asignar tareas y responsabilidades, evaluar la calidad del trabajo, entrenamiento y disciplina.

6 Negociar disputas, construir solidaridad en el equipo, servir como abogado y mediador para el equipo.

El encargado de la planeación como administrador del proyecto, tiene responsabilidades adicionales que lo relacionan con el mismo proyecto, específicamente, el encargado de la planeación debe:

A Establecer el enfoque del plan, articular los objetivos, definir tareas de planeación.

B Establecer estándares para el rendimiento del trabajo y las herramientas del proyecto.

C Definir los componentes de trabajo, recursos requeridos e identificar un camino de tareas críticas.

D Hacer un horario de trabajo, monitorear el horario, identificar y superar los obstáculos del horario de trabajo.

E Mantener registros exactos de trabajo, incluyendo un modelo de proyecto e información actual, identificar variaciones y sus causas, hacer reportes periódicos para el director general o a su representante designado.

F Validar o verificar el trabajo completado.

G Establecer un criterio aceptable y manejar el proceso de aprobación.

El entrenamiento imparte un conocimiento del plan para aquellos que deban actuar en él en una emergencia.

El entrenamiento es un componente importante para la preparación en caso de que exista algún desastre. El personal que estará involucrado directamente en la implementación de

las estrategias de recuperación, y el resto que trabaja en la empresa, debe ser entrenado para reconocer y responder a las situaciones y potenciales de desastre.

La asignación de estos equipos varía de un plan a otro, dependiendo de los requerimientos exclusivos de recuperación.

El plan documentado sirve para regular y actual los cambios izar

La fase de reacción de tareas, son una serie de pasos tomados metódicamente en el avance de un desastre. Por ejemplo; para confrontar un huracán, en la empresa se deben tener varias horas para realizar los respaldos de último minuto, para quitar la electricidad, cubrir el hardware, y realizar otros procedimientos para reducir las consecuencias desastrosas de una tormenta.

Otras emergencias, tales como incendios repentinos, ocurrirán sin una previa advertencia. Los pasos tomados en respuesta a ésta emergencia, son menos preactivos.

Para que el PLRD nos dé la capacidad de recuperar a una empresa, éste debe ser probado. Las pruebas validan la integridad de las estrategias, procedimientos de recuperación documentada y familiariza a los participantes de las pruebas con sus funciones en el momento de un desastre.

Las pruebas son un medio para adquirir información acerca del plan, los resultados de las pruebas son usados invariablemente para mejorar la capacidad de recuperación.

Los propósitos de las pruebas incluyen:

- Validar (e identificar defectos) las estrategias y procedimientos del plan.
- Obtener información acerca de los tiempos de implementación de la estrategia de recuperación (para demostrar qué tan rápido una estrategia de recuperación de redes, por ejemplo, puede ser implementada y usarse).
- Para demostrar el rendimiento de salida de los sistemas y redes operando en modo de recuperación o para comparar el rendimiento de los sistemas de respaldo y redes con sistemas de producción y redes.
- Para demostrar la efectividad a examinadores, auditores y gerentes.
- Para adaptar los planes existentes y encontrar los nuevos requerimientos resultando de negocios, sistemas, redes o cambios de personal.
- Para familiarizar a los integrantes de equipos con sus funciones en el PLRD.

De hecho, como se ha venido mencionando, los planes de recuperación se construyen mejor por módulos, organizados alrededor de las funciones discretas de negocios y sus recursos de automatización asociada.

La recuperación exitosa en una crisis actual, es comúnmente el resultado de una combinación de factores, incluyendo la estrategia de recuperación probada, un equipo ingenioso y leal, buena administración, la participación efectiva de los proveedores, y muchísima suerte.

Es imposible predecir, todas las consecuencias de un desastre. Debido a esto, ninguna prueba puede equipar completamente a una empresa para recuperarse de por sí misma en una emergencia.

Las pruebas validan las salidas o resultados específicos de las tareas del proyecto y verifica que los resultados combinados encuentren los objetivos del proyecto en general.

El resultado de todo esto es formativo; con lo que se logrará lo siguiente:

- Ayuda al equipo de planeación en afinar las estrategias de recuperación de manera individual.
- Provee en base a los datos, sobre el rendimiento del sistema, que es lo que se requiere para construir un plan administrativo de emergencia confiable.
- Al final, se prueba qué tan bien los diferentes componentes de estrategias trabajan juntas para dar un soporte completo de recuperación de los sistemas críticos y redes en el centro de respaldo del mainframe.

Glosario.

PBX
(Private Branch Exchange), Central Privada de Conmutación que está ubicada por lo general en empresas o negocios para proporcionar servicio telefónico entre sus empleados, que cuenta además con una interfase para el acceso a la red telefónica conmutada PSTN. Central telefónica en el lugar del usuario. Ofrece facilidades de conmutación de circuitos para líneas telefónicas dentro del edificio y además acceso a la red pública telefónica.

GATEWAY
Dispositivo que conecta dos sistemas, especialmente si los sistemas usan diferentes protocolos.

CONMUTACIÓN
Método de comunicación en el cual un enlace dedicado de comunicación es establecido entre dos dispositivos a través de uno o más nodos de conmutación intermedios.

CONMUTACIÓN DE PAQUETES
Método de transmisión de mensajes a través de una red de comunicaciones, donde los mensajes son divididos en paquetes cortos. Cada paquete es pasado de la fuente
a su destino a través de nodos intermedios. En cada nodo, el mensaje entero es recibido, almacenado momentáneamente, y entonces se pasa al siguiente nodo.

RUTEO
Es la forma en que se transporta la información a través de una red. Proceso de encontrar un camino hacia el anfitrión de destino.

T1
Terminología Bell que se refiere a un sistema de portadora digital usada para la transmisión de datos a través de la jerarquía telefónica.

MAINFRAME
Computadora de gran capacidad que actúa como servidor o como equipo de procesamiento intensivo. Son comúnmente usados en bancos, universidades, líneas aéreas, etc.

LAN
(Por sus siglas en inglés Red de Área Local) Grupo de computadoras normalmente establecidas en el mismo cuarto o edificio, que están conectadas entre sí con el objeto de intercambiar documentos, correos y trabajar en proyectos conjuntos.

WAN.- Red de área amplia.

Repetidores (channel extension).- Son un conjunto de tecnologías diseñadas para extender y multiplexar los canales del mainframe a cualquier distancia, facilitando la operación remota a los dispositivos conectados al canal a unos niveles de rendimiento cercanos a lo normal.

Interruptor (switch).- Concentrador más inteligente (y caro) capaz de enviar la información a la PC que se programó para recibirla. Un concentrador regular (pasivo) envía la información a todos sus puertos (sólo la PC que solicita es la que acepta la información), lo que demora todo el proceso.

Hot site.- Son instalaciones con mainframes comerciales de recuperación con un servicio que consiste de aire acondicionado, seguro, con área de piso elevado, y uno o más mainframes disponibles para la empresa.

Respaldos.
"volumen total": copia total del sistema, incluyendo el software, utilerías, aplicaciones y datos,
"en incremento"
Estos cambios se hacen comúnmente en la noche y en medios removibles, y es lo que a menudo se le llama respaldo en incrementos.

Respaldos lógicos
El proceso lógico, es independiente del hardware y reorganizará la información, en el momento en que halla una recuperación de los datos, para mandar los datos a los dispositivos de almacenamiento de la manera más eficiente posible.

Respaldos de imágenes físicas
Operan a nivel de hardware y la información se respalda desde discos de la manera más rápida posible.
MIPS not sites.- Son una estrategia de mainframes comerciales de respaldo, en la cual se les vende a los clientes un servicio de respaldos en vez de una locación específica del hot site de respaldo. En el momento de un desastre, se le restaura al cliente, en la instalación seleccionada por el proveedor.

Hot site.- Son instalaciones con mainframes comerciales de recuperación con un servicio que consiste de una ambientación controlada, segura, un área con piso elevado, y uno o más mainframes disponibles para la empresa.

Cold site (Shell site).- Son instalaciones de recuperación que consisten de un ambiente controlado, seguro, con piso elevado y utilidades necesarias con conexiones de comunicaciones para facilitar una instalación rápida de un nuevo sistema de mainframes.

Repetidores (channel extension).- Son un conjunto de tecnologías diseñadas para extender y multiplexar los canales del mainframe a cualquier distancia, facilitando la operación remota a los dispositivos conectados al canal a unos niveles de rendimiento cercanos a lo normal.

DSU/CSU (Digital Subscriber Unit).- Equipo terminal que traduce el protocolo de comunicaciones para ser leído por la PC.

BIBLIOGRAFÍA

Exercising Your Contingency Plan
Philip Jan Rothstein 1995

Exercise Planning and Evaluation
Staff of Emergency Response Institute, Inc. 2001

Emergency Exercise Handbook
Evaluate & Integrate your Company's Plan
Tracy Knippenburg Gillis. 1996

Disaster Recovery Planning for Telecommunications
Leo Anthony Wrobel 2005

Disaster Recovery Planning: Strategies for Protecting Critical Information
Jon William Toigo 2003