Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Industrial

DESARROLLO DE UN PLAN DE RECUPERACIÓN DE INFORMACIÓN EN CASO DE DESASTRES PARA UNA INDUSTRIA GUATEMALTECA

Julio César Catalán Tobar
Asesorado por el Ing. Gustavo Adolfo Camas Salgado

Guatemala, marzo de 2007

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DESARROLLO DE UN PLAN DE RECUPERACIÓN DE INFORMACIÓN EN CASO DE DESASTRES PARA UNA INDUSTRIA GUATEMALTECA

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

JULIO CÉSAR CATALÁN TOBAR
ASESORADO POR EL INGENIERO GUSTAVO ADOLFO CAMAS SALGADO

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO INDUSTRIAL

GUATEMALA, MARZO DE 2007

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE LA JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Inga. Glenda Patricia García Soria
VOCAL II	Inga. Alba Maritza Guerrero de López
VOCAL III	Ing. Miguel Ángel Dávila Calderón
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
VOCAL V	Br. Elisa Yazminda Vides Leiva
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Sergio Antonio Torres Méndez
EXAMINADOR	Ing. Jaime Humberto Baten Esquivel
EXAMINADOR	Ing. César Augusto Akú Castillo
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

DESARROLLO DE UN PLAN DE RECUPERACIÓN DE INFORMACIÓN EN CASO DE DESASTRES PARA UNA INDUSTRIA GUATEMALTECA,

tema que me fuera asignado por la Dirección de la Escuela de Mecánica Industrial, el 29 de septiembre de 2006.

Julio César Catalán Tobar

ACTO QUE DEDICO A:

DIOS	Por ser mi guía y fuente de sabiduría, mi apoyo en los momentos difíciles.
MIS PADRES	Julio y Selina, por toda su ayuda y confianza.
ALEX	Por su confianza y apoyo incondicional.
TOTY	Por toda su ayuda, sabios consejos.
SIOMARA	Mi amor, por haber estado conmigo en todo momento, ser mi motivo de seguir adelante.
MIS HERMANOS	Fede y Ana, por todo su apoyo.
MIS FAMILIARES	Abuelita Oly, Tío Lico, tíos y demás familia con mucho cariño.
MIS AMIGOS	Gracias por la amistad y el apoyo que me brindaron.

"ID Y ENSEÑAD A TODOS"

AGRADECIMIENTOS A:

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA	Casa de estudios que me brindó la oportunidad de alcanzar mis metas.
FACULTAD DE INGENIERÍA	Por brindarme los conocimientos necesarios para desarrollarme como ingeniero.
MI ASESOR	Ing. Gustavo Camas, por sus consejos y asesoramiento.
ESCUELA DE MECÁNICA INDUSTRIAL	

“ID Y ENSEÑAD A TODOS”

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES V

RESUMEN IX

OBJETIVOS XI

INTRODUCCION XIII

1 ANTECEDENTES HISTÓRICOS 1

1.1 Historia del DRP 1

1.1.1 Orígenes 1

1.1.2 Evolución 2

1.1.3 Situación Actual 3

1.2 Desastres 4

1.2.1 Definición de desastre 5

1.2.2 Posibles desastres en Guatemala 7

1.2.2.1 Tormentas Eléctricas 8

1.2.2.2 Erupciones volcánicas 8

1.2.2.3 Inundaciones 10

1.2.2.4 Huracanes 11

1.2.2.5 Terremotos 12

1.2.2.6 Deslizamientos 13

1.2.2.7 Incendios 14

1.2.2.8 Terrorismo 14

2 FUNCIONES DEL DRP 17

2.1 Características 17

2.1.1 Tiempo objetivo de recuperación 17

2.1.2 Análisis de Impacto de una empresa 18

2.1.2.1 Crítico: 19

2.1.2.2 Vital: 20

2.1.2.3 Sensitivo: 20

2.1.2.4 No Crítico: 20

2.1.3 Punto objetivo de recuperación 20

2.1.4 Análisis de riesgo 21

2.1.5 Acuerdos del nivel de servicio 23

2.2 Requerimientos 24

2.3 Funcionamiento 26

2.4 Limitaciones 28

2.5 Rol de un DRP en la industria guatemalteca 29

3 SITUACIÓN ACTUAL DE LAS EMPRESAS GUATEMALTECAS 31

3.1 Análisis de la situación actual 31

3.1.1 Infraestructura 31

3.1.2 Procedimientos 33

3.1.3 Planes de emergencia 34

3.2 Información Crítica 36

3.3 Recursos críticos 37

4 DISEÑO, IMPLANTACIÓN Y EJECUCIÓN DEL DRP 39

4.1 Diseño de un DRP 39

4.1.1 Análisis de una empresa 40

4.1.1.1 Requerimiento de equipo 44
4.1.1.2 Recurso humano 46
4.1.1.3 Análisis de seguridad y riesgo 46
4.1.1.4 Análisis de impacto de la empresa 49
4.1.1.5 Manual de procedimientos 50
4.1.1.6 Desarrollo del plan de recuperación 54
4.1.1.7 Declaraciones y acciones post-desastre 55
4.1.1.8 Autorizaciones 56
4.1.1.9 Plan piloto 57
4.1.2 Políticas de recuperación de desastre 57
4.2 Simulación de un desastre 58
5 SEGUIMIENTO Y MEJORA CONTINUA DEL DRP 65
5.1 Registros de cumplimientos 65
5.1.1 Procedimiento 66
5.1.2 Formularios 67
5.1.3 Inspecciones 67
5.2 Retroalimentación de la información 68
5.2.1 Programa de mejora continua 69
5.2.2 Programa de auditorias 70
5.3 Actualización permanente de requerimientos y funciones 73
CONCLUSIONES 75
RECOMENDACIONES 77
BIBLIOGRAFÍA 79

ÍNDICE DE ILUSTRACIONES

FIGURAS

1	Tormenta Eléctrica	8
2	Erupción Volcánica	9
3	Inundaciones	10
4	Huracanes	11
5	Terremotos	12
6	Deslizamientos	13
7	Incendios	14
8	Terrorismo	15
9	Población empleada por sectores	32
10	Calendarización del diseño de un DRP	43
11	Organigrama del departamento de permisos	51
12	Estructura de dominios del control para la seguridad	71
13	Nivel de cumplimiento de normas ISO 17799	73

TABLAS

1	Población empleada por sectores	32
2	Check list servidores, redes, telecomunicaciones	45
3	Reporte de equipos de computo	45
4	Check list factores externos e internos	47
5	Tolerancia de las operaciones	49
6	Checklist operaciones y su descripción	49
7	Listado proveedores	50
8	Registro de cumplimiento	66

GLOSARIO

Accidente	Evento casual en cuya génesis está involucrada, por acción u omisión, la actividad humana y que resulta en lesiones o daños liberados.
Administración para desastres	Componentes del sistema social constituido por el planeamiento, la organización, dirección y control de las actividades relacionadas con el manejo de los desastres en cualquiera de sus fases.
Alerta	Estado declarado con el fin de tomar precauciones específicas, debido a la probable y cercana ocurrencia de un evento destructivo.
Contingencia	Posibilidad de que una cosa suceda o no suceda, riesgo, peligro, evento.
Desastre	Acontecimiento en el cual una ciudad o una comunidad sufren grandes pérdidas humanas y materiales, en el que se necesita de la ayuda externo para atenderlo, debido a que la situación social ha sido trastornada.

Emergencia	Estado excepcional de una comunidad amenazada o afectada por un desastre, el cual implica la aplicación de medidas de prevención, protección y control sobre los efectos del riesgo.
Hardware	Substracto físico en el cual existe el software. Abarca todas las piezas físicas de una computadora.
Información	Conjunto organizado de datos, los cuales constituyen un mensaje sobre determinado ente o fenómeno.
Operación	Método, acto, proceso o efecto de utilizar un dispositivo o sistema.
Proceso	Conjunto de las fases sucesivas de un fenómeno natural o de una operación artificial.
Simulacro	Ejercicio de ejecución de acciones, previamente planeadeas, para tener una respuesta ante una emergencia, accidente.
Software	Programas y hardware almacenados en una computadora

RESUMEN

Este trabajo de graduación presenta una guía, en la cual se describe un plan de recuperación de información en caso de desastres. Pretende que las personas interesadas en salvaguardar su información, tengan todos los parámetros a seguir para su diseño, implementación y ejecución. Un plan de recuperación de desastre Disaster Recovery Plan, DRP es un documento que define las fuentes, acciones, tareas e información requerida para manejar la recuperación de los procesos de una empresa en el momento en que ocurra un incidente.

Un desastre es un acontecimiento en el que una ciudad o comunidad sufre grandes pérdidas humanas y materiales, en el que se necesita ayuda externa para atenderlo, debido a que la situación social ha sido trastornada. Todo esto es debido a un suceso natural o generado por el ser humano o por tecnología de destrucción. Dentro de las características del DRP se encuentran el tiempo objetivo de recuperación, análisis de impacto de una empresa, punto objetivo de recuperación, análisis de riesgos y acuerdos de nivel de servicio.

Un coordinador de recuperación de desastre es el encargado de las tareas de diseño del plan. Dentro del diseño del plan se deben de incluir diferentes etapas como el requerimiento de equipo, requerimiento de recurso humano, análisis de seguridad y riesgo, análisis de impacto de la empresa, manual de procedimientos, desarrollo del plan de recuperación, definir declaraciones y acciones que se tomarán durante el desastre, autorizaciones, plan piloto, simulacros y actualizaciones, seguimiento y mejora continua.

Dentro de los costos que provoca un desastre se pueden mencionar las interrupciones del flujo de caja, pérdida de clientes, pérdida del mercado, erosión de la imagen del negocio, violaciones legales y pérdida de inversionistas, por mencionar algunos. Dentro del plan de recuperación de desastres se deben incluir nueve secciones: procedimiento de emergencia, notificaciones, movilización de las operaciones, recuperación del sistema, recuperación de la red, recuperación de usuarios, operaciones de recuperación, mantenimiento y restablecimiento de funciones.

Hay dos tipos de pruebas: la simulación pasiva y la simulación activa. Se aconseja realizar primero una simulación pasiva y luego una simulación activa. En un plan de recuperación de desastres es necesario llevar un control de todas las acciones preventivas y correctivas, los registros de cumplimiento son documentos que nos servirán para presentar resultados obtenidos y proporcionar evidencia de las actividades correspondientes.

Realizar una revisión periódica y auditar los planes de contingencia son dos seguimientos esenciales para asegurar que la empresa podrá seguir laborando sin atrasos y recuperarse fácilmente de un incidente mayor. La norma ISO 17799 define a la información como un activo que posee valor para la organización y requiere, por tanto de una protección adecuada. Es una norma no certificable.

OBJETIVOS

General

Desarrollar un plan de recuperación de información en caso de desastres para las industrias guatemaltecas

Específicos

1. Describir el rol y la responsabilidad de cada involucrado en la cadena de acción en cada uno de los escenarios de desastre considerados.

2. Minimizar el tiempo de recuperación de la información en una situación de desastre mediante la aplicación de un protocolo de emergencia para que la empresa pueda continuar con sus operaciones diarias.

3. Establecer el mecanismo para recuperar la mayor cantidad de información posible utilizando los recursos humano y tecnológico disponibles asignados.

4. Desarrollar un programa de actualización y mejora continua de los planes de recuperación de desastre utilizando una metodología de inspecciones, simulacros y auditorias periódicos para garantizar su efectividad en el transcurso del tiempo.

INTRODUCCIÓN

En toda empresa, al ocurrir un incidente natural o provocado por el hombre, en el que exista potencial pérdida de infraestructura y/o información, lo primero que se necesita es encontrar una herramienta de apoyo, en el momento inmediato después de ocurrido el incidente, la cual permita a la empresa continuar con su operaciones diarias, teniendo el menor número de pérdidas. Al pensar en esto, se incluyen la infraestructura, el personal, las comunicaciones y la información, siendo esta última uno de los elementos más importantes para una empresa a nivel operativo.

La información es administrada, actualmente, por medio de sistemas de computación, organizadas en bases de datos, y localizadas en servidores y unidades secundarias de reserva, backups. El Plan de Recuperación de Desastre - DRP – Disaster Recovery Plan, por sus siglas en inglés - busca restaurar la información guardada en los servidores de backup en el ambiente de trabajo para que las operaciones, tanto financieras como de logística, puedan tener la información necesaria para continuar con su trabajo diario en caso de un incidente.

Los antecedentes históricos muestran los orígenes del DRP, su evolución y situación actual. Muestran, también, lo que son los desastres naturales y los posibles desastres que pueden ocurrir en Guatemala.

En las funciones del DRP se dan a conocer las características básicas que éste contiene, los requerimientos que permitirán que esta herramienta sea útil en cualquier escenario, el funcionamiento y los pasos a seguir al momento de poner en marcha esta herramienta. Las limitaciones con las que cuenta este plan y el rol que este plan puede llegar a jugar en la industria guatemalteca.

Se describe de forma global cuál es la situación actual de las empresas guatemaltecas en lo que respecta a infraestructura, procedimientos y planes de emergencia ante un posible desastre. Se define que es lo que se considera información crítica, vital para que la empresa pueda seguir sus operaciones del día a día, así como los recursos que se consideran críticos.

Se muestra un ejemplo en el que se diseña, implementa y ejecuta un plan de recuperación de desastres, se hace un análisis de la empresa, se determina cual es la información privilegiada o crítica y que equipo va a ser necesario tener para poder poner en marcha las operaciones de la empresa luego del desastre; las personas con las que se necesita contar, luego del desastre, y la elaboración de un plan piloto, en el cual se realizan diferentes escenarios para verificar que los procedimientos establecidos hayan sido cumplidos en su totalidad.

Se elabora un plan de seguimiento y mejora continua del plan de recuperación de desastre en el que se proponen constancias de cumplimiento que incluyen registros de los procedimientos, formularios en los que se anotan los comentarios de las inspecciones y simulaciones. Se realiza, también, una retroalimentación de la información en la que se incluye un programa de mejora continua y un programa de auditorias, así como actualizaciones permanentes de requerimientos y funciones.

1 ANTECEDENTES HISTÓRICOS

Un plan de recuperación de desastre (Disaster Recovery Plan, DRP) es un documento que define las fuentes, acciones, tareas e información requerida para manejar la recuperación de los procesos de una empresa en el momento en que ocurra un incidente.

1.1 Historia del DRP (Plan de Recuperación de Desastres)

Desde su concepción a finales de los años 70, los planes de recuperación de desastre han continuado su expansión a nivel mundial. Esta herramienta tuvo sus orígenes en las empresas multinacionales norteamericanas, en las que muchas de sus operaciones offshore sufrieron durante muchos años los problemas de desastres, tanto naturales como deliberados.

1.1.1 Orígenes

Al principio, estos planes eran únicamente aplicables a la infraestructura y el recurso humano, ya que la información era almacenada físicamente en archiveros y se necesitaba lugares amplios. Un estudio hecho por la Universidad de Minnesota en 1978, demostró que, mientras más largo sea el período que una empresa está sin telecomunicaciones debido a un desastre, más crítico será el impacto.

Se estimó que durante la primera hora de ocurrido el desastre, el 80% de las empresas norteamericanas perdían alrededor de $.1, 000.00.

1.1.2 Evolución

De acuerdo con Jon William Toigo, hace 15 ó 20 años eran muy pocas las empresas en las que si hubiera ocurrido una amenaza de fuego, hubieran utilizado un plan con el que pudieran retomar sus actividades en el menor tiempo posible o con la menor pérdida permitida. Es normal que una empresa gaste menos del 5% de su presupuesto en planes de contingencia.

Se estima que entre los años 1982 y 1985 la pérdida de información a nivel mundial se debió en un 28% a problemas con la corriente eléctrica, un 11.7% por tormentas eléctricas, 9.6% por inundaciones, 7.7% por problemas con el equipo de computación, 7.2% por atentados terroristas, 6.3% por huracanes, 5.6% por incendios, 5.4% por errores de software, terremotos 4.9% y otros desastres 5.1%.

En 1995, el gasto mundial en planes de recuperación de desastres fue de aproximadamente $3,100 millones de dólares (Q25, 000 millones de quetzales) y se estimó que crecería en un 20% anual de acuerdo con la revista Forbes. 335 horas hombre trabajadas promedio son perdidas por las compañías cada vez que ocurre un incidente, anualmente se pierden 38.1 millones de horas hombre trabajadas promedio.

Desde 1995, se calcula que se han cobrado seguros en las industrias por $180 billones de dólares, (Q2, 400,000 millones de quetzales) y se calcula que esa cifra se duplicó en el año 2000.

1.1.3 Situación Actual

En Estados Unidos, después del atentado de Nueva York del 11 de septiembre del 2001, se reporta que solo un 50% de las empresas norteamericanas poseen un plan de recuperación de desastre; de estas, menos de la mitad han probado su plan. Las primeras 72 horas siguientes al incidente son las más críticas en lo que respecta a esfuerzo de recuperación. Como responda la empresa a este período es lo que determinará si sobrevivirá o no.

Frecuentemente, no son los desastres en sí los que motivan a la gerencia de las empresas a implementar un plan de recuperación de desastres; sino, que son las instituciones financieras con las que se tienen créditos monetarios las que han motivado a que se adopten estos planes. Muchos ejecutivos no se dan cuenta de la importancia que tienen estos planes debido a que un desastre lo ven como un hecho “posible”. La realidad es que cada día, las empresas dependen más de la informática, y empresas pequeñas o medianas que no tienen bien estructurados sus planes de recuperación son los primeros en desaparecer durante y después del desastre.

60% de las compañías afectadas en un 100% por un desastre, tienden a dejar de operar en menos de 2 años. La hora siguiente al incidente es la más importante, ya que generalmente en este momento es cuando se determina que tan grave fue el impacto y que es lo que se requiere realizar. Parte del proceso de la evaluación de riesgo es determinar los tipos de eventos que podrían interrumpir las actividades de la empresa.

Muchos de los planes de recuperación de desastres están hechos tomando en cuenta el peor escenario posible, generalizando el tipo de desastre, no importa si es un tornado, terremoto, huracán, inundación, igual se perderán las instalaciones, información, etc.

Actualmente se cuenta también con las normas ISO17799, estas fueron publicadas por primera vez en febrero de 1995 como un juego de controles comprometiendo a las mejores prácticas de seguridad de información a las organizaciones bajo el nombre de BS7799, en mayo de 1999 fue revisado y en diciembre de 2000 fue finalmente publicado bajo el nombre de ISO17799.

El estándar es intencionado a servir como un punto de referencia para identificar un rango de controles necesarios para la mayoría de situaciones donde la informática es usada en la industria y el comercio. Esta certificación puede volverse un benchmark con el que cualquier organización será comparada.

Estas normas cubren todo los problemas de seguridad en informática. Consiste en diez discretas secciones, cada sección se enfocan en un aspecto específico.

1.2 Desastres

Guatemala es un país propenso a los desastres naturales, es un área que topográficamente en la que tienden a ocurrir sismos, erupciones volcánicas, incendios, entre otros.

1.2.1 Definición de desastre

Un desastre es un acontecimiento en el que una ciudad o comunidad sufre grandes pérdidas humanas y materiales, en el que se necesita ayuda externa para atenderlo, debido a que la situación social ha sido trastornada. Se sufren alteraciones intensas en las personas afectadas, bienes, servicios y el medio ambiente. Todo esto es debido a un suceso natural o generado por el ser humano o por tecnología de destrucción.

Hay ciencias dedicadas al estudio de los desastres como lo son la geología, economía, meteorología, ingeniería, entre otras. Los desastres se pueden dividir en los siguientes grupos:

Desastres Ambientales:

- Tornados,
- Huracanes,
- Inundaciones,
- Tormentas de nieve,
- Terremotos,
- Tormentas eléctricas,
- Incendios,
- Deslaves de tierra,
- Epidemias,

Interrupciones organizadas y/o deliberadas:

- Actos de terrorismo,
- Actos de sabotaje,

- Actos de guerra,
- Robos,
- Disputas laborales,

Pérdida de servicios:

- Falla de la energía eléctrica,
- Pérdida de suministro de gas,
- Pérdida de suministro de agua,
- Falta de petróleo y aceite,
- Falla de telecomunicaciones,
- Daño de drenajes,

Falla de equipos o sistemas:

- Fallo de corriente eléctrica interna,
- Fallo de aire acondicionado,
- Fallo de líneas de producción,
- Fallo de planta de enfriamientos,
- Fallo de equipo de informática,

Serios incidentes de seguridad de la información:

- Robo cibernético,
- Pérdida de información almacenada,
- Discrepancias en información privada,
- Fallo de equipo de informática,

Otras situaciones de emergencia:

- Violencia en el lugar de trabajo,
- Interrupción del transporte público,
- Peligros en el área aledaña a la empresa,
- Regulaciones de salud y seguridad,
- Moral de los empleados,
- Publicidad negativa,
- Problemas legales,

1.2.2 Posibles desastres en Guatemala

En Guatemala los desastres que pueden ocurrir son los siguientes:

- Tormentas Eléctricas,
- Erupciones volcánicas,
- Inundaciones,
- Huracanes,
- Terremotos,
- Deslizamientos,
- Incendios,

1.2.2.1 Tormentas Eléctricas

Son aquellas tormentas en las cuales la lluvia está acompañada de rayos, los cuales son descargas eléctricas que producen calor y son responsables de incendios. Estos rayos tienden a alcanzar, generalmente, los objetos más elevados; es por esto que se utilizan pararrayos, cuya función es interceptar al rayo antes de que alcance la estructura que se desea proteger, descargando la corriente a tierra a través de un cable grueso y de muy baja resistencia eléctrica.

Figura 1 Tormenta Eléctrica

Fuente: CONRED - TIPOS DE DESASTRES EN GUATEMALA

1.2.2.2 Erupciones volcánicas

Una erupción volcánica es la liberación violenta de energía desde el interior de la tierra.

El magma en ascenso llega a la superficie por el conducto y se produce la erupción, que se inicia generalmente con el escape de gases que acompaña al magma.

La intensidad de la explosión depende del tipo de magma, sin embargo, casi todas las erupciones forman nubes obscuras que suben 30 o más kilómetros y producen derrames de productos volcánicos o incandescentes como lava y flujos piro clásticos y/o caídas de cenizas.

Las erupciones se clasifican por la intensidad y naturaleza de la actividad explosiva del volcán. El grado de explosividad depende, en gran parte, de la viscosidad de la lava; los más viscosos producen erupciones más violentas que generan nubes ardientes, mientras que otras erupciones con magma de baja viscosidad no son muy violentas.

Figura 2 Erupción Volcánica

Fuente: CONRED - TIPOS DE DESASTRES EN GUATEMALA

1.2.2.3 Inundaciones

Fenómeno por el cual una parte de la superficie terrestre queda cubierta temporalmente por el agua, ante una subida extraordinaria del nivel de ésta.

Causas frecuentes de este fenómeno son las fuertes lluvias en un período relativamente corto, represamiento de un río, destrucción de una presa, expansión de un lago o laguna por fuertes o continuas precipitaciones, ascenso del nivel del mar. Este fenómeno ocurre cuando la carga (agua y elementos sólidos) rebasa la capacidad del cauce, por lo que se vierte en los terrenos circundantes.

Figura 3 Inundaciones

Fuente: CONRED - TIPOS DE DESASTRES EN GUATEMALA

1.2.2.4 Huracanes

Manifestaciones violentas del clima y cuyo síntomas son lluvias intensas, vientos de fuertes a fuertísimos y posteriormente problemas de precipitación lenta. La depresión tropical es el nacimiento del huracán, se caracteriza por los vientos máximos de 63 KM/H. La tormenta tropical es cuando los vientos alcanzan velocidades entre los 63 y 118 KM/H, es aquí cuando se le asigna un nombre por orden de aparición y de forma alfabética.

Huracán es cuando el viento alcanza la velocidad de 119 KM/H; se origina de aire caliente y húmedo que viene del océano e interacciona con el aire frío. Estas corrientes giran y se trasladan entre 10 y 50 Km. en una hora, con un área de aproximadamente 100 Km. de diámetro. Su trayectoria es totalmente errática.

La temporada de huracanes va desde junio a noviembre, presentándose con mayor frecuencia en agosto y septiembre.

Figura 4 Huracanes

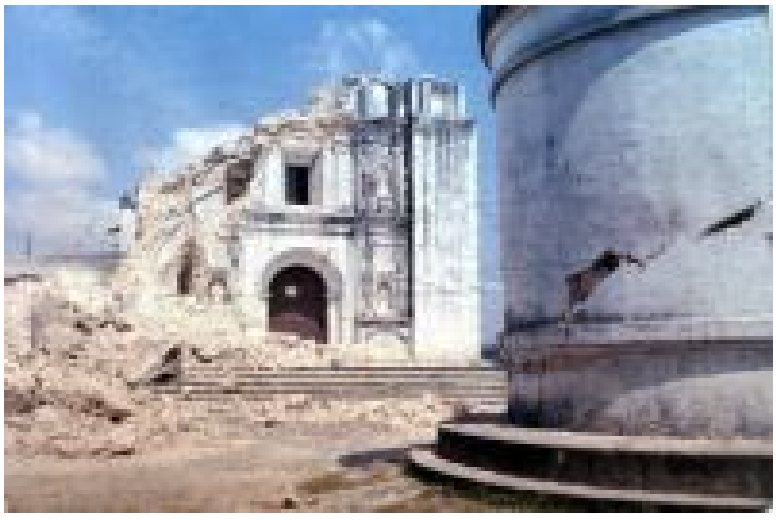
Fuente: CONRED - TIPOS DE DESASTRES EN GUATEMALA

1.2.2.5 Terremotos

Vibración de las diferentes capas de la tierra, que se produce por la liberación de la energía que se da al rozarse o quebrarse un bloque de la corteza terrestre. Pueden ocurrir terremotos por movimiento de las placas tectónicas, estos son gigantescos fragmentos que abarcan superficies continentales y fondo oceánico. Por acción volcánica, cuando el magma tiende a subir por la chimenea del volcán, éste ejerce una gran presión sobre los estratos superficiales y sobre las paredes internas de la chimenea, cuando llega a su máximo nivel produce los terremotos.

Por ruptura de la corteza terrestre o falla local, es un espacio de liberación de energía al interior de las placas y ocurre cerca de la superficie, este tipo de terremoto no es continuo en el tiempo. Por explosiones subterráneas realizadas por acciones humanas, son terremotos originados por cargas explosivas que el hombre ha hecho detonar en la superficie o en lo subterráneo.

Figura 5 Terremotos



Fuente: CONRED - TIPOS DE DESASTRES EN GUATEMALA

1.2.2.6 Deslizamientos

Movimiento pendiente abajo, lento o súbito de una ladera, formada por materiales naturales, roca, suelo, o vegetación. Los deslizamientos se producen debido a la interacción de los procesos naturales y la acción del hombre sobre la tierra, se produce generalmente en las áreas marginales.

Puede ser por actividad sísmica, composición del suelo y subsuelo, orientación de las fracturas o grietas en la tierra, cantidad de lluvia en el área, erosión del suelo, deforestación de laderas y barrancos, construcción de edificios, carreteras, edificaciones con material pesado sobre terrenos débiles, falta de canalización, etc.

Figura 6 Deslizamientos

Fuente: CONRED - TIPOS DE DESASTRES EN GUATEMALA

1.2.2.7 Incendios

Uno de los riesgos que se acrecienta en Guatemala, es un fuego no controlado de grandes proporciones que puede surgir súbita, gradual o instantáneamente y puede llegar a ocasionar lesiones o pérdida de vidas humanas, animales, materiales o deterioro ambiental. Los incendios forestales son muy comunes en este país, se dan en su mayoría en los departamentos de Petén, Alta Verapaz, Quiche, Izabal y parte de Huehuetenango.

Figura 7 Incendios

Fuente: CONRED - TIPOS DE DESASTRES EN GUATEMALA

1.2.2.8 Terrorismo

El terrorismo es una sucesión de actos de violencia que se caracteriza por inducir terror en la población civil de forma premeditada. Dentro de los comportamientos forzados por la amenaza del terrorismo en dicha población civil se incluyen la aceptación de condiciones de muy diversa índole: políticas, económicas, lingüísticas, de soberanía, religiosas, etc.

Cuando este tipo de estrategias es utilizado por gobiernos oficialmente constituidos, se denomina terrorismo de Estado. El terrorismo (proveniente de la palabra francesa del siglo XVIII terrorisme, "bajo el terror") es el término que se refiere al uso calculado de violencia o la amenaza de la misma contra la población civil, normalmente con el propósito de obtener algún fin político o religioso. En su sentido actual, el término fue acuñado extensivamente por la propaganda nazi para hacer referencia a los movimientos de resistencia de los países ocupados por el ejército alemán.

Dentro de los instrumentos utilizados para implementar dicho mecanismo, o actos terroristas, se incluyen diversas formas de violencia física contra las personas, como el secuestro, la tortura o la ejecución extrajudicial; diversas formas de violencia moral, como la amenaza de las anteriores o la presión social; diversas formas de violencia contra los bienes privados y públicos, como la destrucción de los mismos con materiales explosivos o incendiarios. Finalmente, uno de los instrumentos más utilizados por los grupos terroristas es el atentado con explosivos contra blancos militares o civiles para provocar muertes indiscriminadas o no.

Figura 8 Terrorismo

Fuente: CNN NOTICIAS - 2005

2 FUNCIONES DEL DRP

Un plan de recuperación de desastres es conocido también como un plan de continuidad de negocios (Business Continuity Plan), ó plan de contingencia de los procesos del negocio (Business Process Contingency Plan), describe como una organización debe lidiar con un potencial desastre. Así como un desastre, es un evento que interrumpe la continuidad de las funciones normales de una actividad, este plan consiste en las precauciones tomadas para que el efecto del desastre se minimice y la organización pueda seguir sus operaciones normales o al menos continuar con sus operaciones críticas.

2.1 Características

Dentro de las características del DRP podemos mencionar:

- Tiempo objetivo de recuperación,
- Análisis de impacto de una empresa,
- Punto objetivo de recuperación,
- Análisis de riesgo,
- Acuerdos de nivel de servicio.

2.1.1 Tiempo objetivo de recuperación

El tiempo objetivo de recuperación (Recovery Time Objective, RTO) es la duración máxima de tiempo tolerable en la que una computadora, sistema, red o aplicación puede permanecer apagado después de que ocurre un desastre.

El RTO es una función que calcula la interrupción normal de las operaciones mediante la cantidad de ventas perdidas por unidad de tiempo que ha transcurrido desde que sucedió el desastre. Estos factores dependen del equipo y aplicaciones afectadas, se puede calcular en segundos, minutos, horas, o días y es muy importante considerarlo dentro de un plan de recuperación de desastre.

El costo de estar sin información en una empresa en caso de un desastre de pende de efectos a largo plazo así como de efectos inmediatos y a corto plazo o factores tangibles. Una vez que un RTO para una aplicación o sistema ha sido definido, los gerentes o encargados podrán decidir que tecnología es la más adecuada para utilizar en caso de un desastre. Por ejemplo, si el RTO de una aplicación de control de inventarios es de una hora, información almacenada en un backup o disco duro externo puede ser la mejor solución. Si el RTO es de 5 días, entonces un almacenaje exterior puede ser la mejor solución y la más práctica.

2.1.2 Análisis de Impacto de una empresa

El análisis de impacto de una empresa (BIA, Business Impact Analysis), es un componente esencial de un plan de recuperación, este análisis incluye una investigación en la que se determinan vulnerabilidades, y componentes que desarrollaran estrategias para minimizar el riesgo. Identifica costos asociados a fallas o faltantes, como lo son flujos de caja, reposición de equipo, salarios extras a pagar para llevar todo al día, pérdida de ganancias, etc.

Este tipo de reporte cuantifica la importancia de los componentes de un negocio. Los impactos de un desastre son expresados monetariamente para propósitos de comparación. La información recolectada en este análisis debe incluir un listado de computadoras, hardware de telecomunicaciones y un listado de todo el software que utilice la empresa.

Es necesario determinar que tan crítico es cada una de la información recolectada, en base a esto se puede determinar la tolerancia que la empresa puede tener ante un desastre y el hecho que no puedan laborar con normalidad; por lo general, esta tolerancia está expresada en dólares. Por ejemplo, una empresa de telemarketing al sufrir un desastre pierde las telecomunicaciones, cada minuto que la empresa pase sin telecomunicaciones representa pérdida de ventas, clientes, ingresos, etc., debido a esto en esta empresa las telecomunicaciones son un sistema crítico.

La información se puede clasificar según las siguientes tolerancias:

- Crítico,
- Vital,
- Sensitivo,
- No Crítico.

2.1.2.1 Crítico:

Funciones que no pueden ser desempeñadas a menos que se cuente con equipo o sistemas idénticos a los que fueron dañados durante el desastre. La tolerancia hacia la interrupción es poca y el costo de interrupción es elevado, se recomienda utilizar backups para la información.

2.1.2.2 Vital:

Estas funciones son aquellas que pueden ser realizadas de forma manual pero por un cierto período corto de tiempo, hay mayor tolerancia y el costo de interrupción es menor, puede esperarse hasta 5 días para que sea reestablecido pero será necesario ponerse al día con todo el trabajo acumulado que se tendrá.

2.1.2.3 Sensitivo:

Estas funciones son aquellas que pueden ser realizadas de forma manual por un período amplio de tiempo, son realizadas de forma dificultosa pero con un costo bajo.

2.1.2.4 No Crítico:

Funciones que pueden ser interrumpidas por un período amplio de tiempo, su costo de interrupción es nulo o mínimo.

2.1.3 Punto objetivo de recuperación

El punto objetivo de recuperación (Recovery Point Objective, RPO) es la edad de los archivos que se deben recuperar del backup para continuar con las operaciones normales de una empresa, esto ayudará también a determinar si una computadora, sistema o red necesita ser dada de baja debido a un problema de hardware, software o de telecomunicación.

El RPO es expresado en tiempo atrás, es decir, hacia el pasado, desde el momento en el que ocurrió el incidente; puede ser especificado en segundos, minutos, horas o días.

Una vez que el RPO de una computadora, sistema o red ha sido definido, es necesario determinar el período con el que se realizarán los backups; este período puede ser diario, semanal o mensual. Esta herramienta, en conjunto con el tiempo objetivo de recuperación (RTO), ayuda a los gerentes a seleccionar tecnologías y procedimientos óptimos. Se aconseja que el RPO se realice en un período similar al RTO, ya que esto permitirá tener la información más actualizada en el momento de un desastre y la pérdida sería mínima.

2.1.4 Análisis de riesgo

Un análisis de riesgo es un procedimiento para identificar riesgos y vulnerabilidades, analizarlas para determinar posibles daños y establecer vías por medio de las cuales el impacto pueda ser eliminado o reducido. Es un proceso para determinar qué nivel de seguridad es apropiada para un sistema o ambiente.

Un análisis de riesgo cualitativo puede ayudar a estructurar un modelo de seguridad; se deben de considerar los siguientes elementos:

- Amenaza: Situaciones no deseadas pueden pasar.
- Ataque: Consumación de un hecho anunciado o no anunciado.
- Vulnerabilidad: Debilidad, se deberá diseñar un sistema en el que el ataque tenga la menor cantidad de bajas posibles.
- Control: El control es un contra-ataque a la vulnerabilidad.
- Impacto: Severidad de las consecuencias del ataque.

- Impacto en el negocio: Esto es lo que se debe prevenir o eliminar.

Todo esto en conjunto permite tener un área de trabajo en la que se pueda manejar la seguridad. Todas las organizaciones deben estar preparadas para una posible situación de emergencia, y deben considerar qué tipo de backups y estrategias preventivas son las apropiadas para cada actividad.

Hay que ser sistemáticos durante la elaboración del plan de recuperación de desastres; no se deben de subestimar ni la naturaleza ni el entorno y debe planearse exhaustivamente qué se va a hacer en caso de un incendio, huracán, inundación, apagón, ataque terrorista, etc. Lo mejor es ir buscando elementos comunes en todos estos desastres:

- Pérdidas de información,
- Pérdidas de acceso a las instalaciones e información,
- Pérdidas de personal.

Posteriormente se puede realizar una matriz, en la que se contenga estas tres pérdidas como las columnas, y cada una de las actividades de la empresa como las filas. La matriz definirá cómo se responderá a la pérdida de información, acceso y personal para cada actividad.

Es importante establecer una persona que pueda estar a cargo del departamento en el caso de que el gerente del departamento no se encuentre disponible para laborar. Esta persona debe de estar establecida en el plan, y se le debe delegar completa autoridad en este tipo de situación; si no se puede nombrar a alguien, entonces se tiene una gran debilidad ya que esto implica que no hay una persona capaz de realizar las tareas diarias del departamento en el momento del desastre.

También es necesario crear un listado de tareas individuales, con asignaciones para cada empleado. Se debe incluir tareas en las que se notifiquen a los proveedores donde tienen que despachar o asistir a realizar mantenimiento de equipo, informar a los clientes más importantes de cuál es la situación de la organización, e informar a la junta directiva de las acciones a tomar; proteger registros de información escrita, tales como contratos pendientes, publicidad, investigaciones, garantía de equipos, etc. Deben finalmente establecerse prioridades dentro de las tareas, no se puede regresar todo a la normalidad al mismo tiempo; se debe de establecer el tiempo máximo que podemos estar sin realizar estas tareas.

2.1.5 Acuerdos del nivel de servicio

Acuerdos del nivel de servicio (Service Level Agreements) son fundamentales para la continuidad del negocio. Esto define el mínimo nivel de disponibilidad que debe de haber de los proveedores y a su vez que acciones se deben de tomar en caso se interrumpa el intercambio de bienes con ellos.

Por ejemplo, si HP no tiene distribuidor disponible en el país y se necesita equipo nuevo para continuar con las operaciones, que posibilidad hay de tener equipo guardado en alguna bodega exterior de la compañía o la posibilidad de que la representación de esta marca pueda brindarnos el equipo proveniente de otro país cercano. Si es una empresa multinacional, este tipo de acuerdos permite establecer que operaciones pueden ser realizadas en otras localidades la organización.

Por ejemplo, si ocurre un terremoto en el país y la organización cuenta con oficinas en El Salvador, Honduras y México, ver la posibilidad de continuar con las operaciones en estos países de tal forma que el negocio no paralice sus actividades; en el momento en que las condiciones sean adecuadas para la continuidad del negocio en Guatemala, se da por terminada la operación en el país seleccionado y se continúa con el día a día localmente.

2.2 Requerimientos

El plan de recuperación de desastres debe incluir una lista descriptiva de las áreas de mayor importancia de la empresa. En esta lista se debe calificar a las áreas más importantes de la organización.

Cada área debe incluir una breve descripción de los procesos del negocio y las principales dependencias en los sistemas, comunicaciones, personal y la información. Documentos que se deben incluir en el momento de la creación del plan son:

a) Organigrama de la empresa,
b) Plan existente (si aplica),
c) Información del personal de emergencia,
d) Listado de proveedores y números de contacto,
e) Direcciones y mapas de ayuda,
f) Procedimientos de evacuación existentes,
g) Procedimientos de salud y de seguridad,
h) Procedimientos administrativos y de operación,
i) Listado de consultores y de a quien contactar en caso de emergencia,
j) Procedimientos del personal administrativo,

k) Copia de los planos del edificio,
l) Inventario de activos,
m) Inventario de activos de informática,
n) Inventarios de IT,
o) Especificaciones del sistema de IT,
p) Especificaciones del sistema de comunicación,
q) Procedimientos de almacenamiento fuera de las instalaciones,
r) Regulaciones industriales relevantes,
s) Información de seguros,

Áreas funcionales a calificar dentro del plan de recuperación de desastres debe incluir:

a) Procesos que incluyan e-commerce,
b) Comunicaciones basadas en correo electrónico,
c) Otros servicios al cliente de tipo on-line,
d) Líneas de producción,
e) Información de recursos humanos,
f) Servicios informáticos,
g) Mercadeo y relaciones públicas,
h) Servicios de mantenimiento y soporte,
i) Mecanismos de calidad de control,
j) Manejo de servicio al cliente,
k) Ventas y su administración,
l) Información financiera,
m) Actividades de investigación y desarrollo,
n) Contabilidad,
o) Auditoría interna.

2.3 Funcionamiento

El plan de recuperación de desastres entra a funcionar desde el momento en que ocurre el desastre; este plan debe de estar almacenado en un lugar físico exterior a las instalaciones de la empresa, como por ejemplo una bodega, caja fuerte de alguna institución de seguridad o bancaria. A su vez, todos los key staff deben poseer una copia de este plan, ya que ellos son las primeras personas a las que se contacta en caso ocurra un desastre.

Si el incidente ocurre en horas hábiles, el coordinador del Comité de DRP debe de evaluar si las infraestructuras han sufrido daño o si es posible regresar a las instalaciones a seguir laborando. Si no es posible regresar a las instalaciones se necesita poner en marcha la movilización de los key staff (disponibles, si por algún motivo no se contará con algún key staff, se designa a otra persona del departamento para que cubra esa posición) al lugar que se tenga designado como área de trabajo en caso de desastre.

Esta movilización se realiza en base a las operaciones críticas establecidas en el análisis de impacto, se empezará con las operaciones que son críticas tomando en cuenta el tiempo que se tiene antes de que las operaciones cambien su tolerancia. El proceso de recuperación en caso las instalaciones no han sufrido daños es el mismo.

Si el incidente ocurre en horas inhábiles, todos los key staff tienen de su conocimiento que deben presentarse a las instalaciones de manera normal, si las condiciones no lo permitieran entonces deben dirigirse al área de trabajo en caso de desastre designado. El proceso de recuperación se realiza en base a las operaciones críticas.

La información es manipulada de la siguiente forma:

Si el incidente ocurre en horas hábiles, el coordinador del Comité de DRP debe de evaluar si las infraestructuras han sufrido daño o si es posible regresar a las instalaciones a seguir laborando. Si no es posible regresar a las instalaciones es necesario movilizar el equipo de resguardo que se posee, este equipo es el que se tiene guardado en bodegas exteriores.

El lugar de la movilización debe de contener la infraestructura adecuada para que se pueda instalar todo el equipo de computación; por lo general, estas instalaciones son hoteles o centro de convenciones. Si las instalaciones se encuentran en buen estado se hace un análisis de que equipo está en buenas condiciones. Servidores, redes, son los primeros servicios que se analizan y reestablecen. A continuación, se reestablece los sistemas y accesos de los usuarios.

Es importante tomar en cuenta que los servicios de redes y de almacenamiento deben de reestablecerse en su totalidad, para posteriormente ir estableciendo los sistemas y accesos de los usuarios según su tolerancia de su operación.

Al establecer que las condiciones son óptimas para reanudar las operaciones diarias de forma normal el DRP entra en la fase de control y seguimiento, es decir, se anota todos los hechos y acciones tomadas para mejora del plan actual y por proceso de auditoría.

2.4 Limitaciones

Dentro de las limitaciones de un DRP podemos encontrar las siguientes:

- Presupuesto para mantenimiento y control del plan de recuperación de desastre.
- Infraestructura adecuada para aplicar el área de trabajo en caso de desastre.
- Personal que este asignada como Key Staff y que en el momento de ocurrido un desastre pueda acudir a las instalaciones o área de trabajo en caso de desastre asignado.
- Equipo de informática se encuentre dañado o destruido, esto hará que la reanudación de las operaciones críticas se alargue.
- Equipo de informática de resguardo que se encontraba en una bodega externa se encuentre dañado o destruido.
- Problemas locales de movilización debido a destrucción parcial o total de los medios de comunicación.
- Problemas locales con la telecomunicación y energía eléctrica.
- Problemas locales de fallecimiento de empleados o familiares.

Estas limitaciones son necesarias tomarlas en el momento de diseñar un plan de recuperación de desastres, debido a que no se sabe la magnitud que pueda tener el desastre, es necesario, establecer guías con varias opciones las cuales permitan la continuidad del negocio en el menor tiempo posible.

2.5 Rol de un DRP en la industria guatemalteca

Actualmente en Guatemala son pocas las empresas que cuentan con un plan de recuperación de desastre. Empresas multinacionales son las que en su mayoría poseen este tipo de planes, en gran parte a que su costo es elevado. Industrias de alto nombre en Guatemala son las indicadas para implementar este tipo de estrategias, ya que las condiciones geográficas del país permiten que haya diversidad de desastres los cuales pueden afectar de gran manera a la industria Guatemalteca.

Para las empresas medianas y pequeñas, este tipo de plan puede realizarse de tal forma que no desaparezcan después de ocurrido el desastre.

3 SITUACIÓN ACTUAL DE LAS EMPRESAS GUATEMALTECAS

Guatemala se encuentra actualmente dentro de un panorama poco prometedor, la tasa de desempleo incrementa anualmente, existe una balanza comercial negativa agregando una violencia social y política que desequilibran las inversiones extranjeras.

3.1 Análisis de la situación actual

La industria guatemalteca se encuentra en una etapa de desarrollo pero a la vez inestable, la inversión extranjera crece a paso lento y las pocas industrias guatemaltecas se ven obligadas a fusionarse entre ellas o con capital extranjero.

3.1.1 Infraestructura

El Banco Mundial define a la infraestructura como un conjunto de elementos o servicios que se consideran necesarios para la creación y funcionamiento de una organización cualquiera; es un factor de desarrollo económico de primer orden, una infraestructura en buenas condiciones y abundante contribuye de forma significativa al desarrollo económico, multiplica el rendimiento de las inversiones, la competitividad y la riqueza de una nación.

La infraestructura reduce costos, una buena red vial hace que los costos de transporte bajen, además de economizar tiempo. Pone en comunicación más fácilmente a la oferta y la demanda. Mejorar directamente el nivel y la calidad de vida.

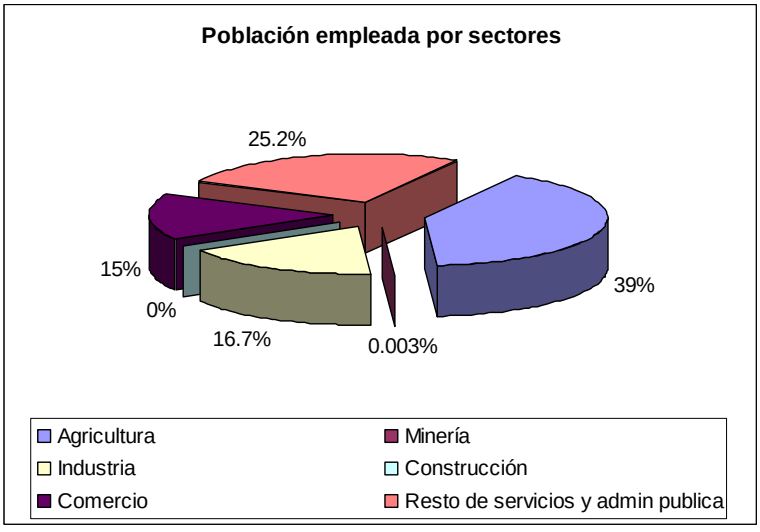
Guatemala se encuentra actualmente con una población económicamente activa de 8.1 millones de habitantes y con una población inactiva estimada del 1.7 millones de habitantes. La población se encuentra empleada de la siguiente forma:

Tabla I Población empleada por sectores

Agricultura	39%
Minería	0.003%
Industria	16.7%
Construcción	0%
Comercio	15%
Resto de servicios y admin publica	25.2%

Fuente: Cámara de Comercio de Guatemala – Enero 2007

Figura 9 Población empleada por sectores



FUENTE: Cámara de Comercio de Guatemala – Enero 2007

Es necesario que Guatemala aumente de forma paralela su infraestructura y el crecimiento de la población nacional. Esto permitirá que las industrias de Guatemala, cuenten con mano de obra más calificada, productos de mejor calidad, más inversión extranjera y más empleos con mejores sueldos.

3.1.2 Procedimientos

Toda industria debe contar con manual de procedimientos, tanto administrativos como de operaciones. Un manual de procedimientos contiene una descripción precisa de cómo deben desarrollarse las actividades de cada empresa. Es un documento interno, del cual las copias deben ser clasificadas según su tolerancia y registrarlas.

Los procedimientos administrativos deben contener, por ejemplo, inventarios, flujos de caja, reconciliación de cuentas bancarias, reclutamiento del recurso humano, contratos de proveedores, ventas, compras, etc. Los procedimientos de operaciones deben contener, por ejemplo: Información técnica, formularios, autorizaciones, descripción de funcionalidad y mantenimiento de equipo técnico, de informática, entre otros.

Un procedimiento de operaciones estándar (Standard Operation Procedures, SOP) es un juego de instrucciones que cubren aquellos detalles de las operaciones que pueden ser adaptadas en otras operaciones similares. Una industria debe de tratar de establecer SOP que se adapten a cualquier proceso, tarea administrativa, y en el caso de la informática, establecer SOP para todas las tareas de backup, mantenimiento, uso de aplicaciones, equipo de computación, etc.

Debido a que el plan de recuperación de desastres es un conjunto de procedimientos, es necesario que las empresas sí cuenten con procedimientos establecidos para cada operación ya que esto permitirá desarrollar herramientas que reestablezcan rápidamente las operaciones en caso de un desastre.

Guatemala cuenta con pocas empresas que tienen sus procedimientos establecidos para cada operación que realicen, estas empresas son multinacionales, instituciones bancarias, industrias que están certificadas bajo estándares internacionales, entre otras.

3.1.3 Planes de emergencia

Son todos aquellos planes que tratan con los desastres o accidentes en el momento que están ocurriendo. Son planes que ayudan a disminuir el impacto físico negativo que un desastre puede tener con las personas. Se deben de establecer actividades en conjunto en todos los niveles (individuales, organizacionales, comunidades).

Un plan de emergencia efectivo es aquel que contiene las siguientes cuatro fases:

- Mitigación,
- Preparación,
- Respuesta,
- Recuperación.

Mitigación es la fase en la que se trata de disminuir el efecto que un desastre puede ocasionar. Esta fase se enfoca en mediciones a largo plazo en la reducción o eliminación de riesgos, esta fase se implementa después de haber ocurrido el hecho y aquí está incluido el plan de recuperación de desastres. Es el método más costoso pero más eficiente para reducir o eliminar el impacto del incidente.

Preparación es la etapa en la que se desarrollan planes de acción para utilizarlos en el momento del desastre. Aquí se incluye capacitación al personal de posibles desastres que puedan afectar a la empresa, el desarrollo de simulacros combinados con planes de evacuación, albergues de emergencia, inventario de activos, mantenimiento de equipo, la coordinación con entidades gubernamentales que puedan dar asistencia y la designación de un área de trabajo en caso de desastre a donde se pueda movilizar las operaciones de la empresa.

La fase de respuesta es en la que se incluye la movilización de servicios de emergencia necesarios así como las personas designadas para asistir en el área de desastre, como lo son policías, bomberos, voluntarios, entre otros. Es un ensayo esencial para lograr el desempeño óptimo de rescate con recursos limitados en el menor tiempo posible.

La fase de recuperación empieza cuando la amenaza inmediata hacia las vidas humanas ha sido eliminada. Es aquí cuando se quiere reconstruir lo que fue dañado o eliminado que se pone en marcha el plan de recuperación de desastre. Según el tipo de plan que se haya adoptado o que tan bien estructurado se tenga, así será el tiempo en el que la implementación del mismo sea exitosa.

En Guatemala, de acuerdo con estudios realizados por la Cámara de Industria, el 65% de las industrias guatemaltecas poseen un plan de emergencia, mientras que el 100% de las empresas multinacionales poseen este tipo de plan. Es importante tomar en cuenta que entre el 35% de las empresas que no poseen un plan de emergencia están aquellas medianas y pequeñas empresas, o empresas en formación.

3.2 Información Crítica

Información crítica es aquella que es de vital importancia para una empresa. Generalmente esta información está ligada a datos como ventas, compras, información de proveedores y clientes, activos de la empresa, recurso humano, producción y almacenamiento.

Esta información crítica es la que se guarda generalmente en servidores los cuales sirven de protección contra la manipulación no autorizada. A su vez, se guarda una copia de seguridad en unidades de backup, las cuales son almacenadas en bodegas o refugios que se encuentran fuera de las instalaciones de la empresa. Con la protección de la información se utiliza el término protección continua de la información (Continuos Data Protection, CDP)

Esta protección se refiere al continuo almacenamiento de la información en una ubicación diferente a donde se tiene el almacenamiento primario. Este tipo de almacenamiento se diferencia del tradicional en que este no tiene un calendario determinado de cuando hará la copia de seguridad, sino que, guarda la información según sea almacenada por los usuarios finales.

3.3 Recursos críticos

En el caso de la información, los recursos críticos son aquellos equipos donde se almacena o se manipula la información, y que al momento de haber un desastre son los equipos que se necesitan para seguir con las tareas diarias de la empresa. Todas aquellas tareas que no sean críticas o cuya tolerancia no sea alta, poseen equipos de capacidad compartida; durante una emergencia este equipo puede servir como equipo de respaldo para operaciones críticas.

En momentos de desastres el hardware que servirá para reestablecer operaciones debe de ser simple, es decir, debe de ser hardware que tenga la configuración mínima aceptable, que la implementación se realice lo más rápido posible y que tenga la asistencia técnica para diseñar, montar y mantener el área de trabajo.

4 DISEÑO, IMPLANTACIÓN Y EJECUCIÓN DEL DRP

Al momento de establecer que la empresa necesita un plan de recuperación en caso de desastre, la junta directiva o gerente general necesitan aprobar un plan que se pueda cumplir en todas las jerarquías de la compañía y que contenga suficientes razones que permitan establecer que hay peligro de pérdida de información.

4.1 Diseño de un DRP

Algunas razones por las cuales es necesario realizar un plan de diseño de recuperación pueden ser las siguientes:

- El incremento en la dependencia de la empresa en los últimos años en mecanismos de producción o ventas computarizados: Ejemplo de este caso puede ser una maquila, las máquinas de bordado operan mediante un software el cual tiene el diseño del bordado, al no contar con la información del diseño la producción queda paralizada; así mismo, las ventas mediante una caja registradora en una tienda de conveniencia pueden verse perdidas si no se cuenta con el programa que realiza la reclasificación de cuentas o flujo de caja.

- El incremento en la dependencia de la empresa en los últimos años en sistemas computarizados en general: Ejemplo de este caso puede ser un Call Center, sin un sistema de computación la empresa no puede llevar un registro de las llamadas entrantes, así como de las distintas operaciones que deban realizar, como cobros, soporte técnico, control de activos, manejo de rutas, etc.

- El incremento en el reconocimiento del impacto negativo que se tendría en el caso de un serio incidente en el negocio: Ejemplo de este caso puede ser un incendio en una embotelladora, se pueden perder toda la información de mezclas químicas, ventas, inventarios, transacciones, etc.

- La necesidad de establecer un procedimiento formal a seguir en el momento inmediato de haber ocurrido un desastre: Ejemplo de este caso puede ser un terremoto que suceda en horas hábiles, cómo se puede recuperar la información de que se estaba procesando en el momento del incidente, qué transporte se encontraba repartiendo en sus rutas, qué empleados se encontraban en las instalaciones en el momento del incidente, etc.

- La necesidad de establecer sistemas de backup efectivos y estrategias de recuperación para mitigar el impacto negativo de un desastre.

4.1.1 Análisis de una empresa

Al hacer un análisis en la empresa, es necesario ir analizando, área por área, tanto infraestructura, como al recurso humano que integra los grupos de trabajo. Aspectos que son necesarios incluir dentro de este análisis son los siguientes:

- Alternativas de manejo de procesos de la empresa: ¿Es posible que áreas no afectadas por el incidente puedan realizar tareas de áreas que han sido muy dañadas?

- Sistemas de backup y recuperación de información: ¿Qué departamentos cuentan con información vital para la continuidad del negocio?

- Equipo de informática necesario para realizar el backup y recuperación de la información: ¿Se necesitan discos duros externos, CDS, etc., y cuál será la ubicación de estos?

- Backup y recuperación de la información del área de servicio al cliente,

- Backup y recuperación de la información del área administrativa y de operaciones.

- Backup y recuperación de la documentación técnica propia del departamento de informática.

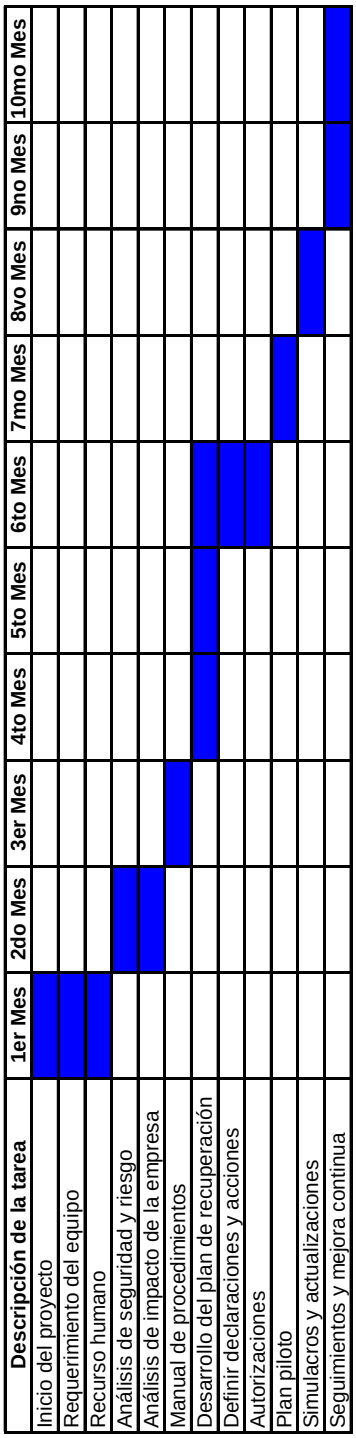
Es después de realizado este análisis en que una junta directiva o gerencia se dan cuenta que un plan de recuperación de desastre es necesario y vital para continuar con el día a día de la empresa y que un coordinador de recuperación de desastre es necesario, para que empiece con las tareas de diseño del plan. En empresas grandes este trabajo es de tiempo completo ya que, esta persona es responsable por todas las instalaciones que la empresa pueda tener.

En empresas medianas o pequeñas esta persona puede ser el gerente o responsable de cada área. Es importante capacitar a esta persona y que tenga conocimiento pleno de todos los desastres para que pueda desenvolverse plenamente en cualquier situación.

Esta persona debe ser organizada, con habilidades ortográficas, habilidad para trabajar con problemas complejos, experiencia en el manejo de proveedores, experiencia en la evaluación y compra de productos, experiencia en manejo de proyectos y conocedor de la tecnología moderna, paciente y perseverante. El coordinador, como primera función, debe de establecer un calendario para el proceso de diseño del plan; este calendario debe contener las siguientes etapas:

- Disponibilidad actual del equipo,
- Disponibilidad actual del recurso humano,
- Análisis de seguridad y riesgo,
- Análisis de impacto de la empresa,
- Manual de procedimientos,
- Desarrollo del plan de recuperación,
- Definir declaraciones y acciones que se tomarán durante el desastre,
- Autorizaciones,
- Plan Piloto,
- Simulacros y actualizaciones,
- Seguimiento y mejora continua.

Figura 10 Calendarización del diseño de un DRP



Fuente: Trabajo de campo – Octubre 2006

4.1.1.1 Requerimiento de equipo

En caso el equipo ha sido dañado y se ha comprobado que el total de éste no se puede utilizar, es necesario contar con una cobertura de seguro; esto permitirá adquirir equipo idéntico o similar que cumplan con las características necesarias para continuar con las operaciones.

Cada vez que se compra un equipo es necesario solicitar su garantía sobre defecto así como establecer una cobertura en caso de desastres o robo con la respectiva almacenadora o bodega donde se encuentren estos equipos. En esta etapa se analizan los servidores, qué capacidad tienen, cuántos hay, para qué tipo de software tienen instalados cada uno, es un servidor de aplicación o de red; se analiza la red que se tenga, si es LAN (Red de área local) o WAN (Red de área mundial), equipo específico que se tenga: Switches, routers, planta telefónica, cableado de red, cableado telefónico, software para el manejo de la planta telefónica, etc.

Es importante que el departamento de IT (Informática y tecnología) proporcione un listado con todo este equipo, en el momento de estar realizando el desarrollo del plan y se definirá qué partes de este equipo son necesarios para la continuidad del negocio en el momento del desastre; es por eso, que el inventario de equipo es el primer punto de control.

Tabla II Check list servidores, redes, telecomunicaciones

FECHA: _____

CHECK LIST SERVIDORES, REDES, TELECOMUNICACIONES				
ACTIVIDAD	**PROCEDIMIENTO**	**CHECK**	**Ticket Number**	**OBSERVACIONES**
ENLACE hacia XXXX trace router	ping xxx.xx.xxx.xxx tracert xzx.xx.xxx.xx			
ENLACE hacia XXXX	ping xxx.xx.xxx.xxx tracert xzx.xx.xxx.xx			
XXXX Switche Main Office 1	ping xxx.xx.xxx.xxx			
XXXX Switche Main Office 2	ping xxx.xx.xxx.xxx			
Router XXXX main office	ping xxx.xx.xxx.xxx			
Revisar servidores: servicios, aplicaciones, conexion a red				
Revisar lineas PBX entrantes	LINEAS xxxx-xxxx, xxxx-xxxx, xxxx-xxxx			
Revisar Alarmas PBX	Display Alarms			
REVISAR BACKUP	Servidores 1, 2,3, 4			
REVISAR TEMPERATURA A/C	VER CONTROL DE TEMPERATURA no > a 70F			
CAMBIAR CARTUCHOS BACKUP	Unidad 1, 2, 3, 4			

NOMBRE Y FIRMA DEL RESPONSABLE: _____

HORA: _____

Fuente: Trabajo de Campo – Noviembre 2006

Tabla III Reporte de Equipos de Cómputo

Reporte de Equipos de Computo

	Area	Nombre Usuario	Desktop	Laptop	Fecha	CPU S/N	Monitor S/N	Actualizacion
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								

Fuente: Trabajo de Campo – Noviembre 2006

4.1.1.2 Recurso humano

El coordinador de recuperación debe tener conocimiento de las personas que laboran en cada operación dentro de la empresa. Es necesario que sea proporcionado un organigrama de la empresa, así como un listado con toda la información de las personas que en ella trabajan; esto servirá para que el coordinador pueda empezar a formar un equipo de planeación, el cual debe de estar conformado por personal de todas las áreas funcionales de la empresa, a estas personas se les llama Key Staff, las cuales generalmente son las personas que tienen más conocimiento en los procesos, procedimientos, proveedores, manejo de cuentas, entre otros. Este equipo debe de definir el alcance que tendrá este análisis e involucrarse en establecer prioridades entre las operaciones, revisar el BIA y sus respectivas recomendaciones y mejoras.

4.1.1.3 Análisis de seguridad y riesgo

Una de las primeras tareas del equipo de planeación es determinar los posibles riesgos que existen en el área donde se encuentra ubicada la empresa, y las medidas de seguridad que se pueden tomar para combatir estos riesgos. Los beneficios de realizar un análisis de riesgo son las siguientes:

Reducir los riesgos legales,
Minimizar la pérdida económica potencial,
Reducir la posibilidad de un desastre,
Reducir la interrupción de las operaciones normales,
Asegurar la estabilidad organizacional,
Asegurar la recuperación ordenada, sistemática y a tiempo.
Minimizar los costos de primas de seguro,

Aumentar la protección contra los activos de la empresa,
Aumentar la seguridad de los empleados,
Cumplir con los requerimientos legales.

Es necesario realizar un listado donde se muestre si hay factores externos e internos que puedan afectar a la empresa, si la empresa se encuentra por donde hay una falla geológica, cerca de combustibles, etc. Se debe realizar un listado parecido al que a continuación se muestra:

Tabla IV Check list factores externos e internos

	Afecta Si / No	**Comentarios**
Localización geográfica		
Topografía del área		
Proximidad a plantas eléctricas		
Proximidad a ríos, lagos, océanos		
Proximidad a aeropuertos		
Grado de accesibilidad a la empresa		
Historial de empresas de servicio locales que provean servicios ininterrumpidos		
Historial de la susceptibilidad del área hacia desastres naturales		
Proximidad a carreteras		
Proximidad a edificios gubernamentales		
Proximidad a instituciones educativas		

Fuente: Trabajo de Campo Noviembre 2006

Este listado se muestra a modo de ejemplo. El realizado por el comité de recuperación debe ser exhaustivo, y con frecuencia contendrá cuarenta rubros o incluso más.

Luego se analizan las diferentes probabilidades de riesgo que pueden ocurrir en donde se encuentra la empresa localizada. Este análisis sirve para plantear el peor de los escenarios para cada uno de los desastres; si hubiera un terremoto de 9.0 grados Richter, entonces las oficinas de la empresa quedarían destruidas por completo, todo el equipo de informática fue destruido y murieron varios trabajadores.

Posteriormente, se hace una relación general entre las diferentes amenazas, dándoles una clasificación que va desde bajo, mediano y alto; se puntea: alto =10, mediano = 5, bajo= 1. El impacto en las funciones del negocio se puede clasificar de la siguiente forma:

0 = No impacto o interrupción en las operaciones,
1 = Impacto notable, interrupción en las operaciones hasta por 8 horas,
2 = Daño al equipo o facilidades, interrupción en las operaciones hasta por 48 horas,
3 = Daño mayor al equipo o facilidades, interrupción en las operaciones por más de 48 horas.

Este análisis sirve como punto de partida para establecer el costo de un desastre, y las vulnerabilidades que se poseen ante el mismo. Dentro de los costos a incluir se pueden mencionar los siguientes:

- Interrupciones del flujo de caja,
- Pérdida de clientes,
- Pérdida del mercado,
- Erosión de la imagen del negocio,
- Violaciones legales,
- Pérdida de inversionistas.

4.1.1.4 Análisis de impacto de la empresa

En esta etapa se define cuál es la tolerancia de cada una de las operaciones de la empresa, se realiza un listado en el que analiza cuáles son los impactos negativos del desastre en varios momentos del tiempo posterior al evento, y cuál es el momento más crítico y que tan rápida tiene que ser la respuesta de recuperación.

Tabla V Tolerancia de las operaciones

	< 2 horas	< 24 horas	24 - 48 horas	2 - 5 días	> 5 días
Impacto en el servicio al cliente					
Pérdida de clientes					
Pérdida de ganancias					
Costo potencial de recuperación en caso de desastre					
Exposición a posibles penalidades					
Pérdida de información crítica					
Impacto negativo financiero					

Fuente: Trabajo de campo – Noviembre 2006

Luego se verifica qué tipo de funciones se realizan, si operacionales o administrativas, una descripción del proceso, si algún otro departamento depende de ellos, si la información es crítica, información del encargado del área y quien es su Key Staff.

Tabla VI Checklist operaciones y su descripción

ANALISIS DE OPERACIONES

	Area del Negocio	Breve descripción del proceso del área	Dependencias	Información Crítica Si/No	Gerente	Key Staff
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Realizado por _____ Fecha: _____

Revisado por _____ Fecha: _____

Fuente: Trabajo de campo – Noviembre 2006

También se debe de realizar un listado de todos los proveedores, qué equipo o servicio es el que brindan, contactos normales y contactos de emergencia.

Tabla VII Listado proveedores

ANALISIS DE PROVEEDORES

	Nombre del proveedor	Equipo y/o servicio que prestan	Contacto	# de Teléfono	Contacto de emergencia	Teléfono de emergencia
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Realizado por _____ Fecha: _____

Revisado por _____ Fecha: _____

Fuente: Trabajo de campo – Noviembre 2006

4.1.1.5 Manual de procedimientos

En este manual de procedimientos se detallan paso a paso las operaciones de las diferentes áreas, los datos a incluir en este manual, por área, son los siguientes:

- Nombre del departamento o área,
- Nombre del encargado del departamento,
- Nombre, número de teléfono de los key staff,
- Organigrama del departamento,
- Equipo de computación que utilizan,
- Equipo de telecomunicaciones que utilizan,
- Tareas asignadas a ese departamento,
- Análisis de impacto del departamento,
- Tiempo objetivo de recuperación del departamento,
- Punto objetivo de recuperación,
- Backup de tareas.

Ejemplo de un manual de procedimientos:

Empresa de Lubricantes Pato Oil, S.A.

Departamento de Permisos

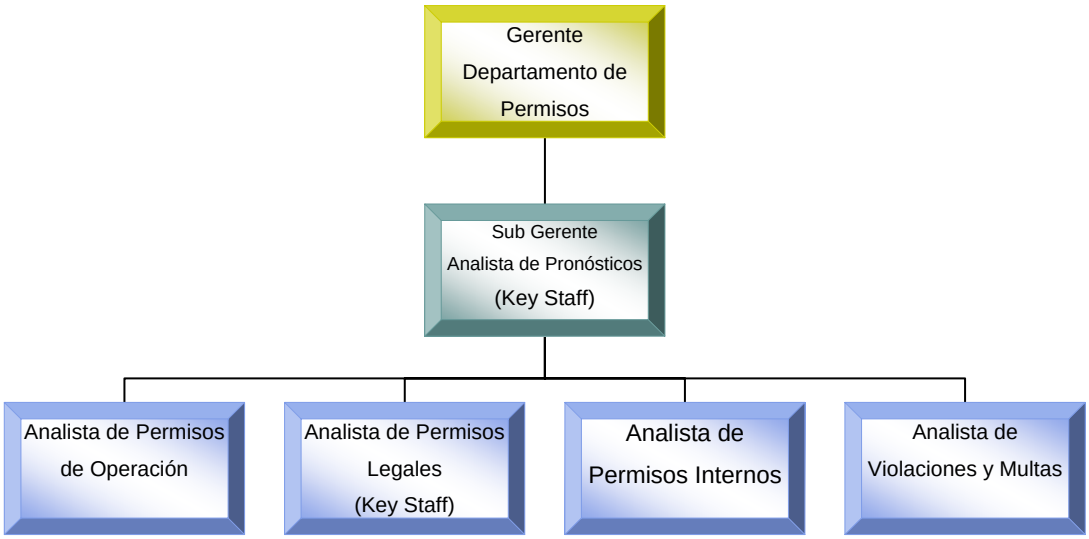
Gerente: Carlos Ruiz

Key Staff:

NOMBRE	TELEFONO	TELEFONO EMERGENCIA
Julio Alvarado	2541-1234	9465-7842
María Hidalgo	2541-1233	4567-1211

Organigrama del departamento de permisos:

Figura 11 Organigrama del departamento de permisos



Equipo de Computación:

2 Laptop (Gerente y Subgerente)
4 PC (Analistas)
6 Monitores
2 Impresoras
1 Scanner

Equipo de Telecomunicaciones:

6 Teléfonos con headset
1 Fax

Tareas:

- Encargados de tramitar licencias de operación para la empresa Pato Oil, S.A.
- Encargados de realizar los pronósticos de venta de los diferentes lubricantes que se venden en la empresa.
- Encargado de problemas legales.
- Utilizan programa contable de donde obtienen la información de venta de los años anteriores.
- Utilizan programa de cálculo para realizar los pronósticos de venta.
- Utilizan programa de almacenaje de copia de documentos.

Aquí se debe detallar cada uno de los procedimientos de las tareas.

En el análisis de impacto del departamento de permisos podemos encontrar la siguiente clasificación para las tareas:

Trámite y control de permisos: Sensitivo
Pronósticos de ventas: Crítico

Suponiendo que la empresa se encuentra perdiendo un promedio de Q.1000.00/hora y que la empresa tarda 3 días sin poder operar, tomando en cuenta también que la empresa solo puede perder Q.40000.00 para no quedar por debajo de su punto de equilibrio.

$$1000\frac{Q}{hr} * 72hrs = Q72000.00 \qquad \frac{72000}{40000} = 1.8\_días \cong 1\_día\_con\_19hrs$$

La empresa puede estar 1día con 19 horas sin operaciones para no empezar a tener déficit. El punto objetivo de recuperación puede ser de 1 día, ya que es necesario tener actualizadas las ventas.

Backups:

- Analista de permisos de operación es backup de analista de permisos internos,
- Analista de permisos internos es backup de analista de violaciones y multas,
- Analista de permisos legales es backup de sub gerente,
- Analista de violaciones y multas es backup de analista de permisos legales,
- Analista de permisos internos es backup de permisos de operación,
- Subgerente es backup de gerente.

4.1.1.6 Desarrollo del plan de recuperación

En el plan de recuperación consideraremos las acciones necesarias para reestablecer la información de las operaciones críticas del departamento de permisos. El plan debe de ir dividido en nueve secciones:

Sección 1: Procedimiento de emergencia, en los cuales se encuentran las acciones a tomar durante el desastre, evacuación, asistencia médica, movilización, etc.

Sección 2: Notificaciones, si fuese una empresa que tiene operaciones en otro país, es necesario avisar a sus afiliados; si el desastre ocurre en horas inhábiles, un directorio con nombres y teléfonos de emergencia con el Key Staff.

Sección 3: Movilización de las operaciones, establecer el área de trabajo donde se continuarán las labores y con qué mobiliario se contará en ese lugar, si no se contara con algún servicio o necesidad, se conseguirá de tal forma que se llenen los requisitos.

Sección 4: Recuperación del sistema: Pasos en los que se establece como se recuperará toda la infraestructura y aplicaciones del departamento de IT; si en caso hubiera equipo con desperfectos o destruidos, se necesita comprar equipo nuevo que sustituya al equipo no disponible.

Sección 5: Recuperación de la red: Procedimientos para re-establecer la red de información y telecomunicaciones de la empresa en el área de trabajo designada.

Sección 6: Recuperación de usuarios: Procedimientos con los cuales se reúne al Key Staff y por si algún motivo no se encontrara alguno de ellos se establecerá alguna otra persona que pueda cubrir esa vacante.

Sección 7: Operaciones de recuperación: Procedimientos para re-establecer la información que se encuentra en las unidades.

Sección 8: Mantenimiento: Se deberá revisar periódicamente que todos los sistemas funcionen con normalidad en el área de trabajo designada.

Sección 9: Restablecimiento de funciones: Se deberá hacer una revisión de las instalaciones y reconstrucción de las mismas, luego de restablecer las instalaciones físicas se equipa nuevamente todas las áreas y se empieza a movilizar en horas inhábiles todas las operaciones. Una forma muy efectiva de reestablecer operaciones en las instalaciones de la empresa es que las personas de cada departamento que no son Key Staff sean las primeras en ser instaladas para que así en horas inhábiles puedan ser trasladados los Key Staff y que las operaciones no sufran ninguna tardanza.

4.1.1.7 Declaraciones y acciones post-desastre

Después de ocurrido el desastre, es aconsejable que la junta directiva o gerencia general establezca que postura tomará ante el incidente. Esta postura debe incluir lo siguiente:

- El sentir de la empresa hacia el país, que ayuda social brindarán (si la empresa se encuentra en posibilidad de realizar donaciones económicas, voluntariado, etc.). Hacia los empleados, si brindarán ayuda económica para la reconstrucción de los activos de los empleados.

- El status de la empresa, si fuera una empresa financiera, es necesario comunicarles a los clientes qué daños sufrieron los bancos, y a partir de cuándo se restablecerán operaciones y qué transacciones serán las que estarán realizando en las agencias. Si fuera una industria, a partir de cuando estarán brindando su producto al mercado.

4.1.1.8 Autorizaciones

Se deben de establecer jerarquías y autorizaciones en un desastre. Durante el desastre, no cualquier persona puede entrar al área de trabajo designada y no todos tendrán acceso a las mismas áreas. Sólo ciertas personas pueden dar declaraciones, asumir ciertas funciones y coordinar actividades críticas de la organización. El organigrama funcional de la empresa se ve generalmente alterado durante una situación de emergencia, y debe adoptarse un liderazgo situacional de acuerdo con lo establecido en el procedimiento de emergencia.

Estas autorizaciones las designa el comité de recuperación y se asigna identificación especial a cada uno de los Key Staff y personas que tengan accesos y privilegios.

4.1.1.9 Plan piloto

El plan piloto nunca tiene que ser perfecto, es más, un plan piloto funcional es aquel en el que se encuentran miles de errores, los cuales permitirán ir eliminando las pérdidas y retrasos.

Un entrenamiento apropiado permitirá establecer que métodos son los mejores a utilizar en un plan de recuperación de desastre. El método de prueba y error es el más común para este plan, ya que permite ir probando procedimiento por procedimiento y a su vez establecer qué errores o problemas se pueden dar y corregirlos de una vez. Es necesario capacitar a todos los empleados para que sepan qué hacer en el momento de un desastre.

4.1.2 Políticas de recuperación de desastre

Estas políticas determinan las prácticas fundamentales y culturales dentro de la empresa; éstas se encuentran ligadas a las políticas de seguridad, ambas con el fin común de permitir la continuidad del negocio. Se pueden establecer charlas de seguridad semanal o mensual, en las que se le informe al personal cuáles son los procedimientos tanto en su departamento, como a nivel general, así como cambios en los procedimientos, etc.

También deben efectuarse simulacros periódicos que deben ser registrados y que permitirán mejorar el plan de recuperación de desastre, suponiendo que se desarrollan estos simulacros una vez cada seis meses, los empleados tendrán la oportunidad de establecer si cuentan con la información suficiente que les permita continuar con sus actividades laborales diarias.

4.2 Simulación de un desastre

Las pruebas son una ventana para ver como las ideas funcionan en la práctica. Es la única forma de establecer si lo que se ha planteado en el plan de recuperación de desastres es funcional y se adecua a la empresa. Durante los últimos 9 años se ha visto como este tipo de pruebas han ayudado a encontrar una solución optima a las necesidades actuales de las empresas.

Un 65% de las empresas que cuentan con un plan de recuperación de desastre nunca han realizado pruebas; el no hacerlo puede ser fatal para la organización, aunque esta etapa este casi al final del ciclo es quizás la etapa más importante del plan de recuperación.

El ir realizando pruebas en cada área es tal vez la opción más aconsejada, siempre tomando en cuenta el mismo escenario o desastre para todas las áreas. Es aconsejable que en el momento del desarrollo del plan se tome en cuenta que éste debe de ser simple, y conforme se van realizando las pruebas, se va aumentando la complejidad y la perfección del plan.

Hay dos tipos de pruebas que se pueden realizar que son efectivas en un plan de recuperación de desastre:

- Simulación pasiva,
- Simulación activa.

Se aconseja realizar primero una simulación pasiva y luego una simulación activa.

La simulación pasiva es aquella en la que se describe un escenario, se le informa al Key Staff del desastre y sus características, estas personas deben de estar familiarizadas con sus procedimientos internos descritos en los manuales de procedimientos. Usualmente lo que se hace es ir realizando paso a paso todo lo que dice el plan de recuperación de desastre para cada posible escenario de acuerdo a la ubicación de la empresa.

Este tipo de simulación permite recabar ideas de que hacer en caso de cada desastre y todos los posibles escenarios que se pueden dar. Es muy útil en los casos en que se está implementando este tipo de plan en una empresa.

La simulación activa presenta una interrupción ficticia sin interrumpir operaciones normales de la empresa. El escenario es presentado a los Key Staff, los cuales son movilizados al área de trabajo designada por el comité de recuperación, a continuación se presentan los pasos a seguir en el área de trabajo de recuperación:

a. Se debe instalar mobiliario y asegurar el área designada para este departamento.

b. Realizar cableado telefónico desde donde se encontrara el área de trabajo de IT hacia el nuevo lugar de trabajo.

c. Realizar cableado eléctrico desde donde está la planta eléctrica o UPS hasta el nuevo lugar de trabajo.

d. Instalar aire acondicionado o ventiladores para mantener un ambiente fresco.

e. Configurar las telecomunicaciones de cada uno de los key staff.

f. Instalar el servidor de red, con el que se realizara el cableado desde los routers, switches o hubs hacia el área de trabajo.

g. Instalar y configurar los servidores de aplicaciones.

h. Instalar y configurar los servidores de información (generalmente son servidores compartidos).

i. Instalar y configurar los servidores de correo electrónico.

j. Instalar y configurar servidores de backup.

k. Instalar y configurar servidores de WAN e Internet (si aplica).

l. Instalar y configurar los equipos de computación de los key staff del departamento de permisos.

m. Hacer pruebas con los equipos de los key staff de permisos, estas pruebas serán realizadas durante aproximadamente 1 hora en las cuales se probarán todos los programas utilizados por el departamento, también se debe verificar la información con que se cuenta y la antigüedad de la misma.

n. Brindar soporte técnico hacia los key staff.

o. Normalizar operaciones de los diferentes departamentos en las instalaciones de la empresa.

Realizar este tipo de simulaciones con frecuencia, permitirá estar preparados ante cualquier desastre y capacitar de una forma práctica a todas las personas involucradas en el plan. Los simulacros permiten ver deficiencias que se tengan en alguno de los pasos descritos anteriormente; también permite establecer particularidades para cada departamento.

Esto se puede lograr después de haber simulado varios desastres en los que se puede tomar en cuenta casos específicos (ejemplo, gerentes necesiten línea telefónica directa). Es importante el compromiso de la gerencia general o junta directiva hacia este tipo de pruebas, ya que muchas empresas no están de acuerdo en realizar con frecuencia las mismas.

Generalmente, las gerencias no están muy de acuerdo con desconectar los sistemas informáticos para ver que tan efectivas son las reacciones ante algún desastre o parar operaciones normales para hacer una evacuación de emergencia e iniciar el plan de recuperación. Es bueno establecer reglas y autorizaciones para que se sigan las instrucciones del plan al 100%. Puede establecerse también observadores los cuales servirán de auditores y anotarán cualquier deficiencia o anomalía que ayude a mejorar el plan.

Ejemplos de desastres que pueden ocurrir en Guatemala:

- Una organización financiera experimentó una pérdida millonaria debido a un hacker que corrompió una base de datos de cuentas de ahorro.

- Un hospital sufre de cortes del servicio eléctrico de hasta 8 horas, realizando cirugías cada hora en cada una de sus 3 salas de operaciones, además cuenta con una tasa de servicio en la emergencia de 10 pacientes por hora de los cuales 8 son tratados por enfermedades o situaciones crónicas.

- Un call center sufre un corte del servicio de telefonía debido a un problema laboral en la empresa proveedora, y se calcula la duración de la misma en 1 semana.

- Una empresa petrolera sufre una pérdida de la Terminal en Puerto Quetzal debido a un Tsunami, todas las instalaciones quedan destruidas y se calcula que no habrá acceso a las mismas por aproximadamente 3 semanas.

- Una embotelladora sufre pérdidas significativas por un terremoto que ocurre en horas hábiles, destruyéndose ¾ partes de la infraestructura y perdiendo la vida del 30% de sus empleados, más un 20% de empleados lesionados que no se encuentran en condiciones de seguir laborando por un período de 2 semanas.

- Un huracán destruye una maquila que se encuentra en la parte nor-este de Guatemala, inundando las instalaciones y destruyendo todo el equipo y materia prima de la empresa.

- Una explosión volcánica hace que residuos de humo y arena sean transportados por el viento hacia una empresa de alimentos en Amatitlán, por lo que las instalaciones han quedado cerradas al menos por 2 días.

- Disturbios sociales prohíben el acceso a un periódico localizado en el centro de la ciudad capital, esto hace que no se pueda presentar ningún trabajador a las instalaciones y se calcula que las manifestaciones durarán 3 días.

Todos estos ejemplos son situaciones potenciales para las cuales puede hacerse una simulación que evidencie las necesidades de mejoramiento en el diseño de un DRP.

5 SEGUIMIENTO Y MEJORA CONTINUA DEL DRP

En un plan de recuperación de desastres es necesario llevar un control de todas las acciones preventivas y correctivas, esto permitirá establecer puntos críticos, deficiencias y demoras los cuales pueden ser motivo de pérdida de dinero o vidas humanas.

5.1 Registros de cumplimientos

Los registros de cumplimientos son documentos que nos servirán para presentar resultados obtenidos o proporcionar evidencia de las actividades correspondientes. Se debe recolectar información detallada donde se indique las acciones paso a paso que se desarrollan en las operaciones críticas, analizando si la acción conviene o no para la situación de emergencia en la que se encuentren.

Estos registros darán muestra de que todas las herramientas y requerimientos necesarios para el cumplimiento del plan de recuperación de desastre, estén listas en el momento del incidente.

Estos registros pueden ser establecidos periódicamente, en el que se realicen inspecciones con cada departamento, revisando que tengan el equipo y la información necesaria para enfrentarse a un incidente. Ejemplo: Revisar cada mes que todos los departamentos tengan su equipo de seguridad que consta de casco, chaleco, etc. Un registro puede tener el siguiente formato:

Tabla VIII Registro de cumplimiento

Revisión Equipo de Seguridad
Empresa Pato Oil, S.A.

Fecha de revisión: _____

	Nombre	Chaleco	Casco	Copia DRP	Copia Manual de Procedimientos	Listado de emergencia	Listado proveedores	Firma
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								

Firma Revisor:

Fuente: Trabajo de campo – Diciembre 2006

5.1.1 Procedimiento

Debido a que un procedimiento es una forma específica de llevar a cabo una actividad o un proceso. Es necesario incluir la siguiente información en todo procedimiento que se desarrolle dentro del plan, seguimiento o cualquier otro control que se tenga en la empresa:

- Identificación (Logotipo, Nombre oficial, Denominación, Lugar y fecha, clave de la forma, número de revisión, unidades responsables)
- Índice o contenido.
- Prólogo y/o introducción,
- Objetivos de los procedimientos,
- Áreas de la aplicación y/o alcance de los procedimientos,
- Responsables,
- Políticas o normas de operación,
- Conceptos,
- Procedimientos,
- Formularios de impresos,

- Diagramas de flujo,
- Glosario de términos.

Es importante analizar la información, detallar paso a paso cómo se realizan las operaciones, qué se utiliza para desarrollarla, quién es el encargado de hacer cada operación, cuánto tiempo es lo aconsejable que se tarde esa persona en realizar la operación, quién supervisa la operación y qué control llevará como registro de las actividades, entre otras.

5.1.2 Formularios

Se desarrollan y mantienen para registrar los datos que demuestran el cumplimiento de los requisitos de los estándares establecidos. Los documentos del DRP deberán hacer referencia a los formularios (Instrucciones de trabajo, manual de procedimientos, etc.).

Los formularios deben de realizarse de forma específica, por tareas, esto permitirá que la información que se desea obtener sea más exacta, a la vez permitirá reducir la cantidad de errores y facilitará la mejora continua.

5.1.3 Inspecciones

Inspecciones son exámenes sistemáticos y planificados de los sistemas implantados en las empresas, tanto de naturaleza técnica como de organización y gestión, de tal manera que se pueda demostrar que unas instalaciones son seguras, la información se encuentra resguardada correctamente y se han tomado las medidas posibles para prevenir o limitar las consecuencias de accidentes graves.

Se debe desarrollar un programa de inspección que abarque instalaciones donde se encuentra resguardada la información, en él se debe de incluir:

- Detalles del área donde se encuentra todo el equipo de informática,
- Definición del período de tiempo en el que se harán las inspecciones, así como cada cuánto se realizarán estas,
- Detalle de previsiones y procedimientos para la revisión de riesgos.

Luego de haberse realizado el programa de inspección, se debe realizar un informe posterior a la inspección, esto deberá contener el alcance de cada inspección y de las instalaciones afectadas, evaluación de los sistemas inspeccionados, análisis del cumplimiento del personal de IT con los estándares establecidos por la empresa, medidas acordadas con el personal de IT que incluyan plazos de aplicación.

Se debe dar seguimiento a la inspección realizada, el informe de la inspección identificará aquellos casos en los que será necesario desarrollar un plan de acción con el personal de IT para demostrar posteriormente que se han tomado las medidas necesarias para corregir situaciones anómalas.

5.2 Retroalimentación de la información

Mantener informados a los empleados de los cambios e innovaciones es un aspecto importante que toda empresa debe tomar en cuenta, esto permitirá tener empleados capacitados que desarrollarán las tareas asignadas en una emergencia de la mejor forma y con la mayor efectividad posible. Dentro de los programas que se pueden implementar se aconsejan dos:

- Programa de mejora continua,
- Programa de auditorías.

5.2.1 Programa de mejora continua

Las empresas se ven cada día en la obligación de mejorar procesos para afianzar su competitividad, satisfaciendo de la mejor forma sus necesidades. Para lograr que se pueda reconocer fácilmente los problemas y de esa forma ir mejorando continuamente, se aconseja realizar lo siguiente:

Tratar de involucrar a los empleados a través de sus sugerencias, formar círculos de calidad para que los empleados compartan sus experiencias personales y laborales. Generar el pensamiento orientado al proceso, ya que los procesos deben ser mejorados antes de que se obtengan resultados mejorados. La resolución de problemas apunta a la causa-raíz y no a los síntomas o causas más visibles. Construir la calidad en los procesos, diseñándolos y desarrollándolos según sus necesidades.

Dentro del control total de calidad que se debe tener en una mejora continua y se debe incluir:

Aseguramiento de la calidad,
Reducción de costos,
Cumplir con las operaciones,
Seguridad,
Mejoramiento de la productividad,
Administración más eficiente de los recursos.

Hay que recordar que un plan de recuperación de desastre nunca es un documento que se encuentre terminado, este evoluciona con el cambio de la tecnología, en especial con la informática

5.2.2 Programa de auditorías

Realizar una revisión periódica y auditar los planes de contingencia son dos seguimientos esenciales para asegurar que la empresa podrá seguir laborando sin atrasos y recuperarse más fácil de un incidente mayor.

ISO17799 fue publicado por primera vez en febrero de 1995 como un juego de controles comprometiendo a las mejores prácticas de seguridad de información a las organizaciones bajo el nombre de BS7799, en mayo de 1999 fue revisado y en diciembre de 2000 fue finalmente publicado bajo el nombre de ISO17799.

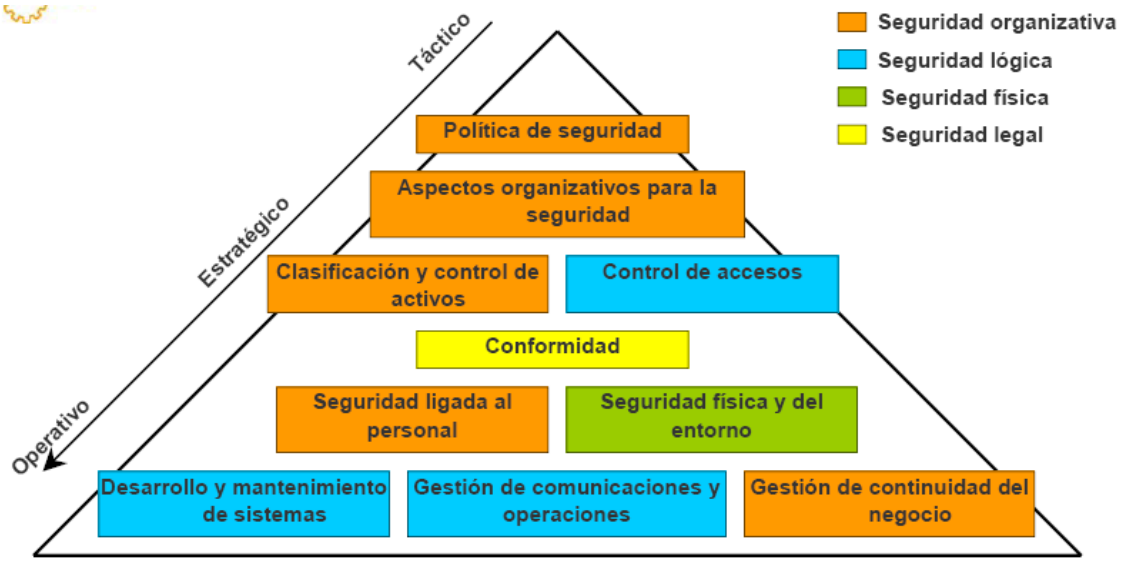
El estándar es intencionado a servir como un punto de referencia para identificar un rango de controles necesarios para la mayoría de situaciones donde la informática es usada en la industria y el comercio. Esta certificación puede volverse un benchmark con el que cualquier organización será comparada.

Define a la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada. Es una norma NO CERTIFICABLE, pero que recoge la relación de controles a aplicar para establecer un Sistema de Gestión de la Seguridad de la Información (SGSI). Se establece diez dominios de control que cubren por completo la Gestión de la Seguridad de la Información:

- Política de Seguridad,
- Aspectos organizativos para la seguridad,
- Clasificación y control de activos,
- Seguridad ligada al personal,
- Seguridad física y del entorno,
- Gestión de comunicaciones y operaciones,
- Control de accesos,
- Desarrollo y mantenimiento de sistemas,
- Gestión de continuidad del negocio,
- Conformidad con la legislación.

Estructura de dominios del control para la seguridad de la información:

Figura 12 Estructura de dominios del Control para la seguridad de la información



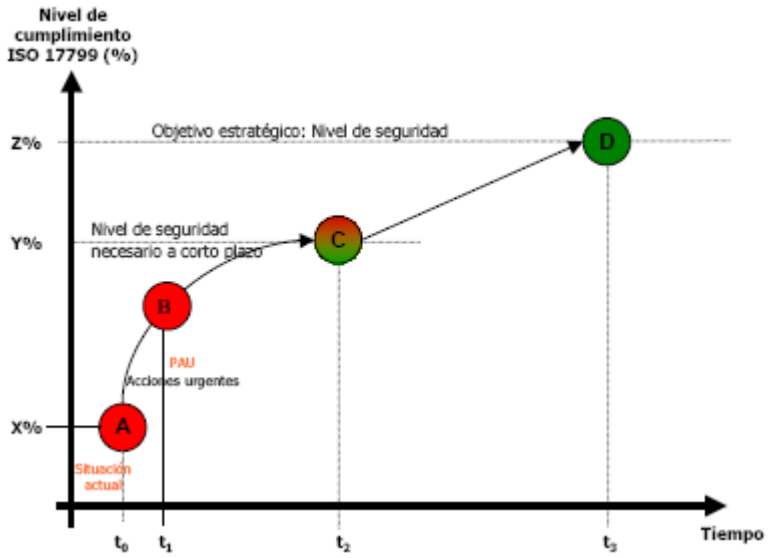
Fuente: Trabajo de campo – Enero 2007

La política de seguridad trata de dirigir y dar soporte a la gestión de la seguridad de la información. Los aspectos organizativos para la seguridad gestionan la seguridad de la información dentro de la organización, mantiene la seguridad de los recursos de tratamiento de la información, mantiene la seguridad de la información cuando la responsabilidad de su tratamiento se ha externalizado a otra organización.

La clasificación y control de activos es mantener una protección adecuada sobre los activos de la organización, asegurar un nivel de protección adecuado a los activos de la información. Seguridad ligada al personal es reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios. Seguridad física y del entorno es evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización. La gestión de comunicaciones y operaciones es asegurar la operación correcta y segura de los recursos de tratamiento de la información.

Control de accesos es controlar los accesos a la información, desarrollo y mantenimiento de sistemas es asegurar que la seguridad está incluida dentro de los sistemas de información. Gestión de la continuidad del negocio es reaccionar a la interrupción de actividad del negocio y proteger sus procesos críticos frente a fallos o desastres. Conformidad es evitar el incumplimiento de cualquier ley, estatuto, regulación y obligación contractual y de cualquier requerimiento de seguridad.

Figura 13 Nivel de cumplimiento de normas ISO 17799



Fuente: Trabajo de campo – Enero 2007

5.3 Actualización permanente de requerimientos y funciones

Periódicamente se estarán revisando los formularios, registros y/o procedimientos para su actualización, esto debido, a que la tecnología y las necesidades cambian constantemente. Por ejemplo: La cantidad de información de una institución bancaria crece cada año, es por eso que ellos deben de contar un banco de datos que posea un sistema de almacenamiento de información suficientemente grande, debido a esto los controles que se puede tener pueden variar y se puede establecer que la revisión de daño en el disco o sistema se realice con más frecuencia y que se analicen más detalles, esto con el fin de evitar la pérdida de la información.

Un Directorio de recuperación de desastre (Disaster Recovery Directory) es un directorio de servicio y soluciones en las que se registran todas las soluciones a los problemas encontrados en las simulaciones de los planes de recuperación de desastre. Este directorio a su vez puede ser colocado en el Internet y compartir diferentes escenarios entre empresas de similares características.

CONCLUSIONES

1. El rol de un coordinador de recuperación de desastre es estar a cargo de la planeación del plan y su control, el tiene a su cargo armar un comité de recuperación, el cual se encargará de la planeación del plan, puesta en marcha, simulación y mejora continua del mismo. Los key staff son las personas que poseen la mayor cantidad de conocimientos y que, a su vez, serán los responsables de realizar las operaciones críticas.

2. Para minimizar el tiempo de recuperación se debe analizar que tan críticas son las operaciones, la información debe de ser también la más actualizada. El protocolo de emergencia debe contar con las nueve secciones que incluye un plan de recuperación de desastre siendo un componente importante las personas que posean el conocimiento necesario para que ellos puedan agilizar la restauración del sistema, infraestructura y procesos.

3. El mecanismo para recuperar la mayor cantidad de información es utilizando almacenaje externo como lo son las unidades de backup. Con este almacenaje se guarda solo la información crítica lo que hace que su reinserción al sistema sea más efectiva, la protección que se les de puede ser el almacenarlos en bodegas externas o lugares donde la seguridad sea mayor.

4. El programa de actualización y mejora continua desarrollado incluye registros de cumplimientos, procedimientos que detallan paso a paso las tareas de cada departamento los cuales son revisados, periódicamente, formularios, inspecciones, círculos de calidad y auditorías a realizar

periódicamente. También, se deben de realizar directorios de recuperación de desastres en los cuales se lleva el record de acontecimientos y las soluciones encontradas a dichos problemas.

RECOMENDACIONES

1. Informarse acerca de los desastres que, históricamente, han afectado al área donde se encuentre la empresa.

2. Establecer y someter a consideración un presupuesto para diseñar, implantar y mejorar los planes de recuperación de desastre en empresas medianas y pequeñas de Guatemala.

3. Realizar simulacros con frecuencia para establecer los efectos potenciales causados por deficiencias en el manejo de la información y realizar una mejora continua al sistema de DRP. El realizar simulaciones permitirá cerciorarnos de que los procedimientos y guías establecidas son funcionales; la observación y completación de formularios servirá para analizar, posteriormente, todos los errores posibles que tengamos en nuestros procedimientos.

4. Tomar en cuenta casos ocurridos en otros países del mundo, y prevenir estas situaciones con base en las experiencias de planes de recuperación de desastres, exitosamente, aplicadas.

BIBLIOGRAFÍA

1. Devlin, Edward S., **Business Redumption Planning**, USA: CRC Press, 1999.

2. Esso Standard Oil, S.A., **Disaster Recovery Plan Guatemala, Guatemala**: Esso Standard Oil, S.A., 2006.

3. Hiatt, Charlotte J, A **primer for Disaster Recovery Planning in an it Environment**, USA: Idea Group Inc, 2000.

4. Hodson, William K. **Manual del ingeniero industrial.** 4ta edición Tomo I y II. México: McGraw Hill, 1996.

5. Jeet Sandhu, Roopendra, **Disaster Recovery Planning**, USA: Thomson Course Technology, 2002.

6. Núñez Sandoval, Alejandro, **Estándares de seguridad en la información**, España: Thomson Learning Ibero, 2000.

7. Sangüesa Sánchez, Marta, **Teoría y práctica de la calidad**, España: Thomson Learning Ibero, 2006.

8. Villalón Huerta, Antonio, **El sistema de gestión de seguridad de la información**,España: S2 Grupo, 2004.

Referencias electrónicas

9. Cámara de Comercio de Guatemala
   http://negociosenguatemala.com/
   Diciembre 2006

10. Cámara de Industria de Guatemala
    http://industriaguate.com/
    Diciembre 2006

11. Corred
    http://www.conred.org
    Diciembre 2006

12. Especialistas en recuperación
    http://recoveryspecialties.com
    Noviembre 2006

13. Guía de la recuperación de desastres
    http://www.disaster-recovery-guide.com/
    Octubre 2006

14. Mundo de la recuperación de desastres
    http://www.disasterrecoveryworld.com/
    Octubre 2006