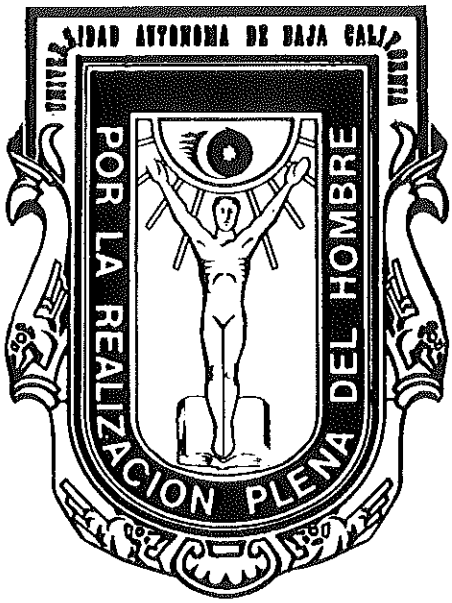
UNIVERSIDAD AUTONOMA DE BAJA CALIFORNIA

FACULTAD DE CIENCIAS



GUIA GENERALIZADA PARA IMPLANTAR UN PLAN DE CONTINGENCIAS OPTIMO PARA PROTECCION A RECURSOS DE INFORMACION (HARDWARE, SOFTWARE,PERSONAL, INFORMACION)

TESIS

Que para obtener el título de

Lic. en Ciencias Computacionales

presenta:

DALILA VAZQUEZ ROMERO

Ensenada, Baja California. Diciembre de 1996

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE CIENCIAS

GUÍA GENERALIZADA PARA IMPLANTAR UN PLAN DE CONTINGENCIAS ÓPTIMO PARA PROTECCIÓN A RECURSOS DE INFORMACIÓN (HARDWARE, SOFTWARE, PERSONAL, INFORMACIÓN)

TESIS PROFESIONAL

QUE PRESENTA:

DALILA VAZQUEZ ROMERO

APROBADO POR:

MAI Omar Alvarez Xochihua
Presidente del Jurado

MAI José Manuel Valencia Moreno
Secretario

LCC Carlos Flores Campos
1er. Vocal

DEDICATORIA

A ti *MAMÁ*,

con todo mi cariño,

donde quiera que estés, ...

AGRADECIMIENTOS

A **Dios**, por todo.

Al **MAI Omar Álvarez Xochihua**, por su asesoramiento, su gran colaboración, su tiempo, paciencia y gran apoyo en la realización de mi tesis, *un agradecimiento muy especial.*

A mis sinodales **MAI José Manuel Valencia Moreno** y **LCC Carlos Flores Campos** por su tiempo, su gran colaboración y sus sugerencias en la revisión de mi tesis.

Al **Lic. Inf. Alfonso Talavera Hernández**, por su gran apoyo brindado para la implantación de mi tesis.

A mi **Papá** y **Hermano**, por su apoyo.

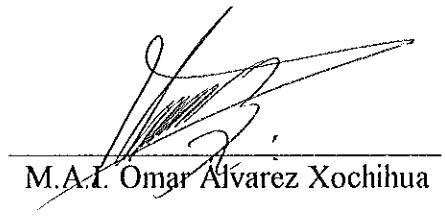
A mis compañeros de generación y amigos, Roberto, Ernesto.

Y por ultimo a todas las personas que de alguna manera contribuyeron para la realización de mi tesis.

RESUMEN de la tesis de *Dalila Vazquez Romero* presentada como requisito parcial para la obtención de la *Licenciatura en Ciencias Computacionales*. Ensenada, Baja California, México. Diciembre de 1996.

Guía generalizada para implantar un plan de contingencias óptimo para protección a recursos de información (hardware, software, personal, información)

Resumen aprobado por:



M.A.I. Omar Alvarez Xochihua

Dada la gran importancia actual de los centros de cómputo en las instituciones en general, surge la necesidad de contar con material de apoyo para proteger los recursos de información de los mismos.

La presente tesis, propone una guía generalizada de apoyo para las instituciones que lo requieran, para proteger sus recursos de información. Ya que en base a bibliografía, un diplomado de auditoría en informática, y en una encuesta realizada en la localidad y en parte a nivel nacional, se pudo confirmar la importancia de un trabajo de esta índole.

Para validar la guía propuesta, se implantó en una de las instituciones encuestadas, Comisión Estatal de Servicios Públicos de Ensenada (C.E.S.P.E.).

CONTENIDO

Página

Lista de figuras

Página

Lista de tablas

Página

Lista de gráficas

CAPÍTULO I

INTRODUCCIÓN

Actualmente algunas de las instituciones que cuentan con centros de cómputo, tratan de proteger al máximo sus recursos de información (hardware, software, personal, información), pero siempre están expuestas a contingencias, ya sean éstas de mayor o menor impacto.

Una contingencia es un suceso que puede presentarse en cualquier momento, interrumpiendo el funcionamiento normal de una institución, teniendo como consecuencias daños de mayor o menor impacto (Valerio,94).

Entre las contingencias de mayor impacto y menor probabilidad de ocurrencia podemos citar a: incendios, temblores, inundaciones, tormentas, huelgas, fraude, sabotaje, entre otras; y las de menor impacto pero con mayor probabilidad de ocurrencia: descompostura de equipo, fallas de energía, ineficiencia del personal, robo de material o de recursos de información, mal manejo de información y en consecuencia pérdida de la misma, entre otras (Valerio,94).

A pesar de las medidas de seguridad que han tomado las instituciones para evitar contingencias, muchas de ellas han llegado a vivir malas experiencias al materializarse alguna situación de conflicto, interrumpiendo su operación diaria, y ha consecuencia de esto, han tenido pérdidas financieras, de tiempo e imagen muy grandes.

Es muy importante para cualquier institución que cuente con un centro de cómputo, la seguridad de sus recursos de información. Por lo tanto, es relevante saber prevenir una contingencia al máximo y en dado caso que se presentara, saber como reaccionar según sea el caso.

La mayoría de las instituciones, se están apoyando últimamente con el uso de redes de área local (LAN's), las cuales eficientizan el manejo de su información y el uso de sus activos de cómputo. Logrando con esto, un mejor rendimiento operativo, pero también, una mayor variedad de riesgos que acechan sus recursos de información.

Obviamente, las instituciones que cuentan con LAN's, protegen de diversas maneras sus recursos de información, pero no todas los protegen con un plan de contingencias óptimo. Esto por diversas razones, dentro de las cuales podemos citar a: presupuestos limitados, no considerarlo necesario, entre otras.

La idea principal de esta investigación, es apoyar a las instituciones en el cuidado de sus recursos de información, y en consecuencia en el soporte de sus actividades productivas. Mediante la elaboración de una guía estructurada, para implantar un plan de contingencias óptimo.

Esta guía será de gran interés y apoyo para las instituciones que cuenten con recursos de información. Dado que todas están expuestas a cualquier tipo de contingencia que se pueda presentar en su ambiente de trabajo.

Para tener una visión real del impacto de la materialización de contingencias en centros de cómputo en instituciones, y por consecuencia de lo útil que es este trabajo de

investigación, se llevará a cabo un estudio de campo en instituciones que cuenten con centros de cómputo. Obteniendo información sobre los problemas que han enfrentado en la realización de sus funciones apoyadas por recursos de cómputo, el daño causado en tiempo y dinero, y la manera en que estos problemas son solucionados.

1.1 Antecedentes.

Los sistemas de información automatizados han sido y son una gran ayuda para las instituciones que manejan volúmenes grandes de información, ya que con ellos eficientizan el proceso de la misma, mejorando sus procesos operativos.

Los centros de cómputo actualmente son una necesidad por las grandes ventajas que proveen, tales como: rapidez en operabilidad, procesamiento de información en volumen, reducción de costos en personal, entre otras. Son de gran ayuda especialmente para instituciones que trabajan con un gran volumen de información.

Las LAN's son una herramienta muy importante para los centros de cómputo, ya que con ellas se comparten recursos informáticos como: programas, datos y equipo de una manera flexible. Lo cual permite una operabilidad mejor y mayor rapidez.

La mayoría, si no es que todas las instituciones que cuentan con centros de cómputo, protegen sus recursos de información, pero un gran porcentaje tienen fallas en la protección a los mismos.

Hay la necesidad actual de generar planes de contingencias, que aporten una eficiente protección a los recursos de información en las instituciones.

1.2 Importancia del uso de planes de contingencias.

La definición, implantación y monitoreo del uso de planes de contingencias es muy importante, ya que con la implantación de los mismos se minimiza el riesgo de vivir malas experiencias, las cuales pueden causar graves daños a los recursos de información y por consecuencia grandes pérdidas de dinero, tiempo, recursos de información y prestigio a la institución afectada.

1.3 Objetivo general.

Diseño de una guía generalizada para cualquier institución que requiera implantar un plan de contingencias óptimo para proteger sus recursos de información.

1.4 Alcance y limitaciones de la tesis.

Se realizará un estudio de campo en la localidad y en parte a nivel nacional, para definir la situación actual en relación a planes de contingencias.

La presente investigación propone una guía generalizada para definir, implantar y monitorear planes de contingencias para cualquier institución que lo requiera.

Se implantará la guía en una de las instituciones encuestadas (C.E.S.P.E.).

La limitación de esta tesis, es que su implantación en el caso real, sólo se validará en una sola institución.

1.5 Organización de la tesis.

El capítulo uno describe una reseña del estado actual de los centros de cómputo, las medidas que se toman para proteger sus recursos de información y la gran importancia de contar con un plan de contingencias óptimo.

El capítulo dos menciona características importantes sobre redes de área local y su importancia.

El capítulo tres presenta un panorama detallado, sobre qué es un plan de contingencias, y la gran importancia de los mismos. Se describen sus usos actuales.

El capítulo cuatro analiza el estudio de campo realizado, y se presentan resultados.

El capítulo cinco expone la guía generalizada para implantar un plan de contingencias y desarrolla sus etapas.

El capítulo seis presenta el desarrollo de la implantación de la guía en el caso real y determina conclusiones.

El capítulo siete especifica las conclusiones generales de la tesis.

CAPÍTULO II

RELEVANCIA DEL USO DE REDES DE ÁREA LOCAL (LAN's)

2.1 Redes de área local.

El uso de sistemas computarizados ha crecido debido a los avances en microelectrónica, y se ha fomentado ampliamente la utilización de un nuevo tipo de enlace de computadoras llamado red de área local (LAN, Local Area Network). (Hopper,89).

Las redes de área local se originaron como un medio para compartir dispositivos periféricos en una organización. Una red de área local es un sistema que permite conectar a varias computadoras entre sí de manera que entre ellas puedan compartir recursos informáticos, esto es, programas, datos y equipo, de una manera flexible. Se les llama de área local debido a que las computadoras conectadas están fisicamente cerca una de otra, se diferencian de las redes de área extendida (WAN, Wide Area Network) en que las computadoras están dispersas en una área geográfica diferente o distante.

La característica principal de una red de área local es:

LA TRANSPARENCIA EN SU USO

En una red, el usuario tiene la sensación de que él es el propietario de los recursos informáticos que está usando, aun cuando éstos están localizados fisicamente en una

máquina distante. Esto significa que el usuario no tiene que tomar acciones especiales para emplear programas, equipo o datos.

La red de área local requiere de dos componentes adicionales; los cuales son:

EL HARDWARE DE RED Y EL SOFTWARE DE RED

El hardware de red lo constituyen los adaptadores de red y el medio físico para conducir la información entre las computadoras. El software de red son los programas que se encargan de coordinar las acciones de la red para que éstas sean transparentes al usuario y a los programas de aplicación. (Hopper,89).

Las redes de área local se pueden usar en cualquier lugar que se necesite el intercambio de información entre grupos de dispositivos a distancias modestas.

Hay varias características de las LAN's las cuales son:

TAMAÑO: El tamaño de una LAN es normalmente el de la organización que la usa. Por lo general, las LAN son redes privadas que se instalan para atender las necesidades de un solo grupo de personas. (Hopper,89).

COSTO: Debido a que muchas aplicaciones de las LAN involucran sistemas de microcomputadores de bajo costo, es deseable que la conexión de tales sistemas a la LAN sea económica. Otro factor que influye en el costo de la LAN es el cableado que hay que instalar, aquí se tiene que considerar el costo del cableado y el de la instalación, aunque en muchos casos es posible tender los cables en los conductos existentes, con un costo bastante reducido. (Hopper,89).

VELOCIDAD: Las velocidades de transferencia de datos de las LAN actuales son muy variadas. La transferencia de datos más lenta es de 100 Kbps, mientras que la más rápida llega a los 100 Mbps. (Hopper,89).

SIMPLICIDAD: En sí, esto se refiere a la forma de la red. El patrón de conexiones en una LAN normalmente es una forma topológica simple, como un anillo o un árbol, y esto tiene implicaciones en las rutas de los paquetes de información sobre la LAN. (Hopper,89).

TASA DE ERRORES: Como las distancias cubiertas por una LAN son pequeñas y se pueden usar cables de una calidad razonable sin incrementar el costo, es usual que la tasa básica de errores en un bit de los cables de la LAN sea baja. (Hopper,89).

En base a lo mencionado anteriormente, el uso de las LAN's incrementa beneficios, pero también con su aparición se generó una mayor variedad de riesgos que acechan a los recursos de información, de los cuales hay que protegerse.

Los planes de contingencias, proveen estrategias factibles para contrarrestar la materialización de estos riesgos, así como el impacto de los mismos.

CAPÍTULO III

PLAN DE CONTINGENCIAS

3.1 ¿ Qué es un plan de contingencias ?.

Una contingencia es un suceso que puede ocurrir en cualquier momento, teniendo potencial para interrumpir el procesamiento normal de la institución afectada, causando daños de mayor o menor impacto (Valerio,94).

Un plan de contingencias identifica y protege los procesos críticos del negocio y los recursos requeridos para mantener un nivel aceptable de procesamiento de los mismos, protegiendo esos recursos y preparando los procedimientos que aseguren la supervivencia de la institución ante una situación de contingencia (Valerio,94).

3.2 Clasificación de contingencias comunes.

Externas

Naturales: temblor, incendio, inundación, tormenta, huracán, otros.

Humanos: robo, sabotaje, fraude, otros.

Materiales: pérdida de información, fallas de energía, otros.

Internas

Naturales: incendio, inundación, otros.

Humanos: robo, destrucción (voluntaria e involuntaria), sabotaje, huelgas, fraude, personal clave, otros.

Materiales: descompostura de equipo, fallas de energía, otros.

3.3 Objetivos de un plan de contingencias.

Los objetivos de un plan de contingencias son:

1) Identificar los problemas y cuidados actuales de las instituciones sobre sus recursos de información.
2) Definir factores necesarios para reducir en gran porcentaje el riesgo de presentarse contingencias en las instituciones, así como el impacto de las mismas.
3) Definir estrategias óptimas para dar soporte a las instituciones en el cuidado de sus recursos de información.
4) Validar las estrategias realizadas implantándolas y monitoreándolas.

3.4 Usos actuales de planes de contingencias.

A las instituciones en general y a los mismos profesionistas en el área de cómputo, les ha tomado mucho tiempo reconocer la importancia de contar con planes de contingencias. Este reconocimiento se ha logrado, en gran parte, gracias a las duras lecciones que los diversos desastres han dejado.

Las amenazas pueden provenir de los más inesperados casos de desastre: temblores, inundaciones, huracanes, otros. Por ello, los resultados de un plan de contingencias pobre, pueden ser devastadores: pérdida de contratos, ingresos, y sobre todo, la pérdida de la confianza de los clientes y el público en general.

Actualmente son pocas las instituciones que cuentan con un plan de contingencias óptimo implantado, ya que no es común encontrar opciones de planes de esta índole.

Pero la mayoría de directivos en informática están conscientes de la necesidad de este tipo de planes, ya que utilizan medios para proteger sus recursos de información, sin embargo, regularmente no son los adecuados.

Lo anterior es validado en base a los resultados obtenidos en el estudio de campo, presentados en el capítulo 4.

CAPÍTULO IV

ANÁLISIS SOBRE EL CUIDADO DE RECURSOS DE INFORMACIÓN EN CENTROS DE CÓMPUTO

4.1 Estudio de campo.

Es muy importante tener una buena base para confirmar la importancia del porqué de la realización de esta investigación, y esto se hace posible por medio de la realización de un estudio de campo en la localidad y en parte a nivel nacional.

El estudio de campo se realizó a instituciones que cuentan con un centro de cómputo, por medio de una encuesta dirigida a los encargados de éstos, ya que ellos interactúan día a día con los problemas reales que se presentan en esta área.

La encuesta realizada es de corte transversal, ya que se requería la información de la misma, para definir o tener una visión de la situación actual ***en ese momento.***

La plancación de la encuesta se basó para su desarrollo, en la realización de los siguientes pasos:

- **Establecimiento de objetivos.**

Se establecieron los siguientes objetivos:

- *Uso actual de los planes de contingencias.*

- *Importancia del uso de los mismos.*

- **Población objetivo.**

La población a muestrear fue:

- Instituciones de tamaños medianas y grandes, que contaran con centros de cómputo.

- **El marco.**

La selección del tamaño del marco a muestrear, se determino mediante la realización de los siguientes pasos:

- Primero se investigo sobre el universo de las instituciones a encuestar en la localidad obteniendo información al respecto de la Cámara Nacional de Comercio Servicios y Turismo de Ensenada, Cámara Nacional de la Industria Pesquera, Cámara Nacional de la Industria y la Transformación, y de las instituciones a encuestar a nivel nacional se investigo del directorio de cuentas por correo electrónico, del Centro de Investigación Científica de Educación Superior de Ensenada.

- Después se definió el tamaño de la muestra, en base a la siguiente fórmula:

$$n = \frac{Npq}{(N - 1) D + pq}$$

donde, $q = 1 - p$ y $D = B^2 / 4$

donde:

n = *Tamaño necesario de la muestra.*

N = *Población objetivo.*

B = *Error de estimación.*

p = *Proporción poblacional.*

El tamaño de la muestra determinada fue con la siguiente proporción:

- *Ensenada 35.*

- *Diversos estados del país 17.*

- **Diseño de muestreo.**

El diseño de muestreo utilizado fue:

- ***Muestreo Sistemático**, el cual consiste en obtener una muestra, seleccionando aleatoriamente un elemento de los primeros k elementos en el marco y después cada **k-ésimo** elemento (donde k= tamaño de la población / tamaño de la muestra).*

- **Método de medición.**

Los métodos de medición utilizados fueron:

- *Encuestas realizadas personalmente.*

- *Encuestas por correo electrónico.*

- **Análisis de los datos.**

Básicamente, se llevo un análisis del uso actual de los planes de contingencias y su importancia.

Un factor relevante de este proyecto de investigación, consiste en obtener información del ambiente real en el que viven las instituciones en relación al cuidado de sus recursos de información. Todo lo anterior con el fin de detectar la importancia que se da al uso de planes de contingencias, la problemática que genera el no tenerlos, e identificar herramientas que brinden un mejor apoyo al manejo de planes de contingencias.

En total se realizaron 52 encuestas (35 en Ensenada y 17 a diversas ciudades del país por correo electrónico), de las cuales sólo se obtuvieron 14 contestadas (11 en Ensenada y 3 por correo electrónico).

Es importante mencionar por lo anterior, que muchas instituciones no le dieron la debida importancia a la encuesta, ya que el solo hecho de contestarla les hubiera ayudado a definir o mejorar su plan de contingencias, si es que contaban con uno. La encuesta realizada se muestra en el anexo 1.

4.2 Resultados obtenidos del estudio de campo.

En base a las encuestas realizadas a diferentes instituciones de la localidad y en diversas ciudades del país, obtuvimos resultados de los cuales definimos diversas conclusiones.

A continuación, se presenta un análisis detallado de la encuesta realizada, en base a las 14 contestadas:

a) De la pregunta uno a la seis, se obtuvo información, referente a datos generales.

b) En la pregunta siete, se obtuvo información sobre el giro de las instituciones, de las cuales se obtuvieron:

GIRO	CANTIDAD
Banca	*2*
Manufactura	*2*
Gobierno	*3*
Educativa	*3*
Transformación	*3*
Privada de Servicios	*1*

Tabla 4.1 Giro del total de las instituciones que contestaron la encuesta.

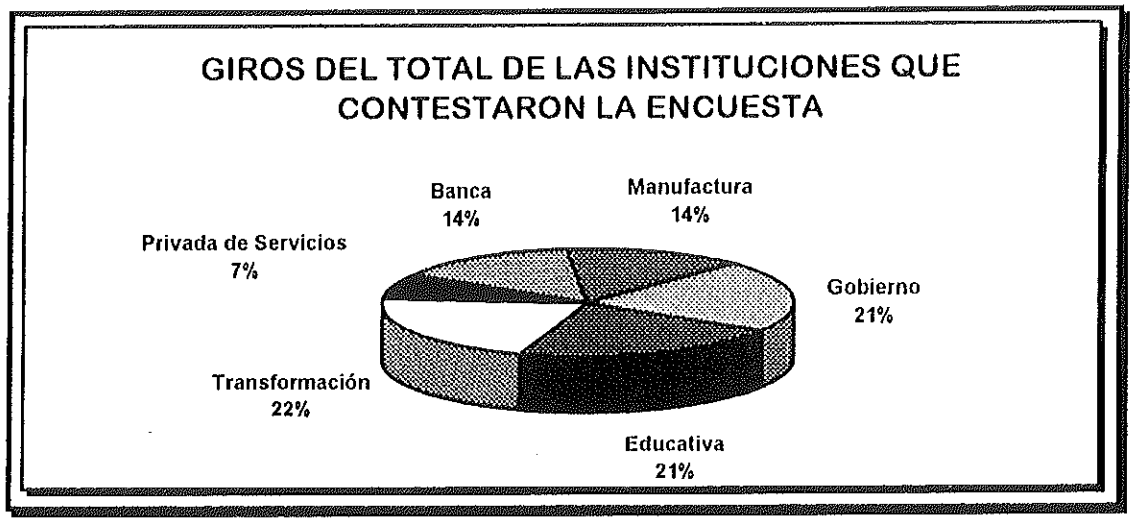
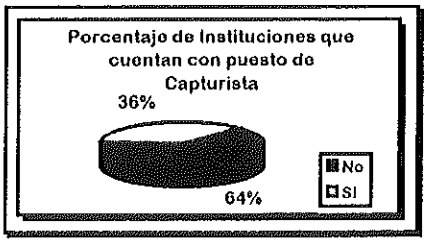
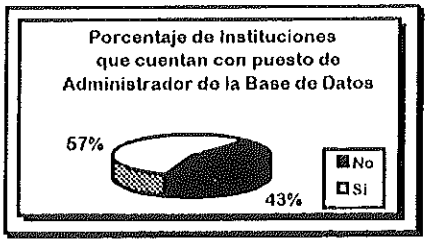


Figura 4.1 Giro del total de las instituciones que contestaron la encuesta.

c) En la pregunta ocho, se obtuvo información sobre los puestos desempeñados en los centros de cómputo de las diversas instituciones encuestadas.





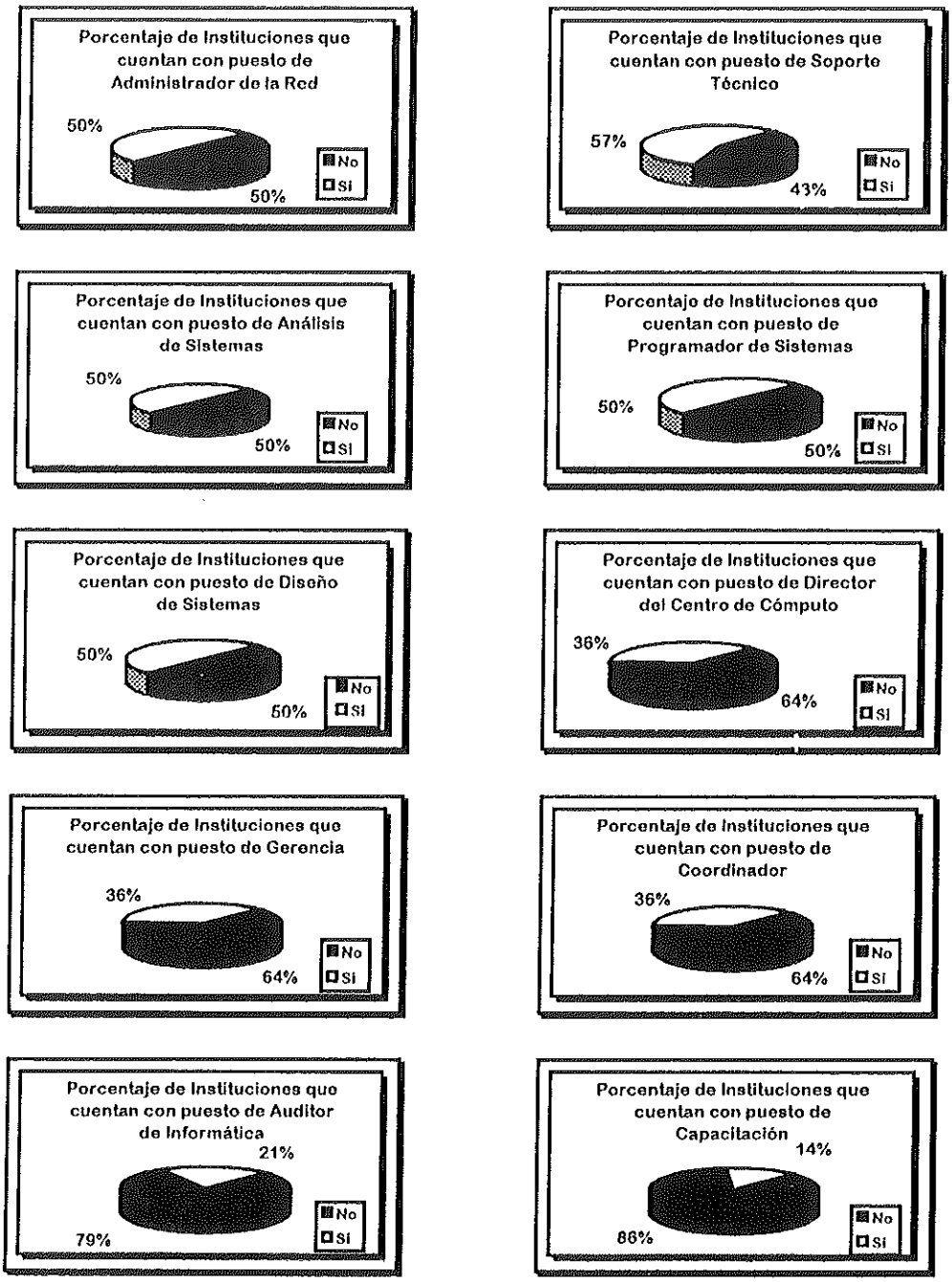


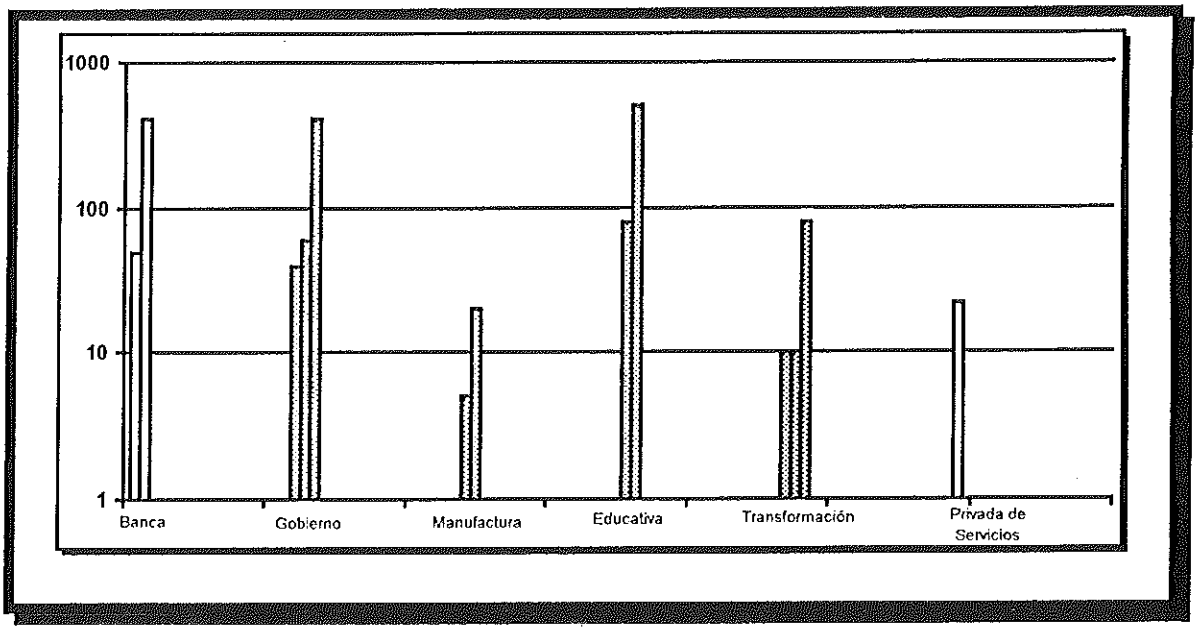
Figura 4.2 Porcentajes de los puestos con los que cuentan las instituciones que contestaron la encuesta.

Por lo anterior, se puede deducir que las instituciones no le dan la importancia debida, al área de capacitación, ni al área de auditoría de informática, lo cual es importante para obtener un buen control en el centro de cómputo.

d) En la pregunta nueve, se obtuvo información sobre el número aproximado de usuarios del sistema de información de cada institución.

El cual fluctúa de 5 a 500 usuarios, las instituciones con mayor número de usuarios son las de giro bancario, gobierno y educativa, y las de menor número de usuarios son las instituciones de giro manufacturero.

Representación del número aproximado de usuarios al sistema de información y giro de cada institución, que contestó la encuesta.



Gráfica 4.1 Fluctuación del número de usuarios.

e) En la pregunta diez, se obtuvo información sobre si las instituciones protegen sus recursos de información, con un plan de contingencias.

De las encuestas contestadas que se obtuvieron en total, el 50% si cuentan con un plan de contingencias y el otro 50% no, pero protegen sus recursos de información, hasta donde se lo permite su presupuesto. Las instituciones que no contestaron la encuesta, es probable que no cuenten con un plan de este tipo y tal vez ni siquiera tengan una idea clara, de lo que éste significa.

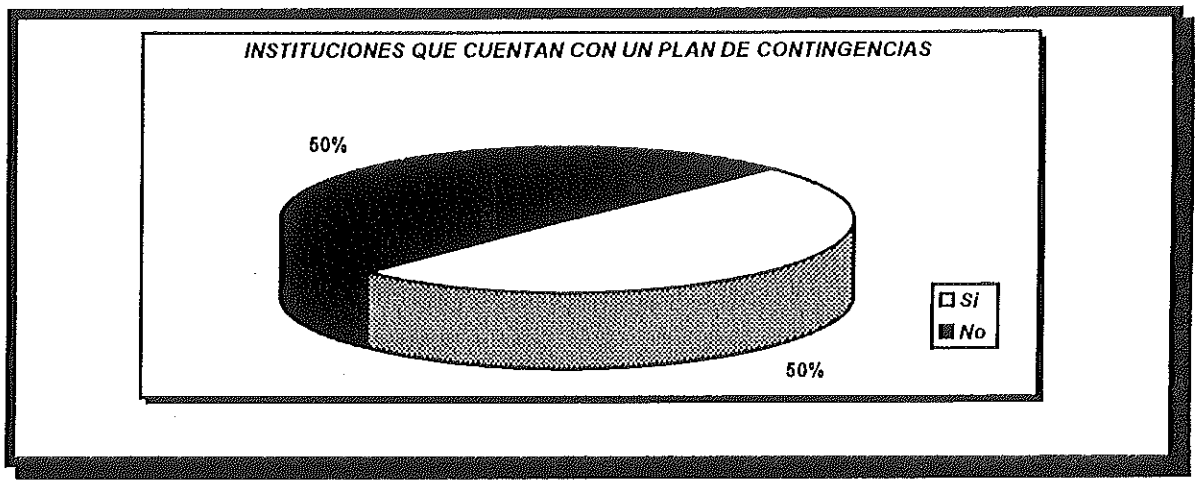


Figura 4.3 Porcentajes de instituciones que cuentan con un plan de contingencias.

f) En la pregunta once, se obtuvo información sobre el porqué, de contar o no con un plan de contingencias óptimo, para proteger sus recursos de información.

El 29% de las instituciones que cuentan con un plan de contingencias, ha sido por haber tenido malas experiencias con contingencias presentadas, por la experiencia vivida se dieron cuenta de la importancia de contar con un plan de contingencias.

El 43% de las instituciones que no cuentan con un plan de contingencias, es más que nada por presupuestos limitados, esto es, no cuentan con los recursos suficientes para dar mantenimiento a un plan de esta índole. El 14%, es porque creen que con la seguridad que tienen es suficiente, y el 14%, si están conscientes de que tienen fallas en su prevención a la seguridad de sus recursos de información, pero como nunca les ha pasado nada, están en espera de que les suceda una contingencia para prevenir las fallas.

g) En la pregunta doce, se obtuvo información sobre las precauciones tomadas para evitar contingencias, las cuales pudieran ser ocasionadas por:

Riesgos externos:

Naturales: temblor, incendio, inundación, tormenta, otros.

- El 57% cuenta con respaldos externos.
- El 21% cuenta con seguro.

Humanos: robo, sabotaje, fraude, otros.

Se protegen por uno o más de los siguientes medios de protección:

- El 100% cuenta con áreas restringidas al centro de cómputo.
- El 100% cuenta con respaldos internos.
- El 71% cuenta con claves individuales.
- El 71% cuenta con servicios de vigilancia.
- El 50% cuenta con alarmas.
- El 50% cuenta con seguros.

Materiales: pérdida de información, fallas de energía, otros.

Se protegen para pérdida de información, por uno o más de los siguientes medios de protección:

- El 100% cuenta con áreas restringidas al centro de cómputo.
- El 100% cuenta con respaldos internos.
- El 79% cuenta claves individuales.
- El 71% cuenta con servicios de vigilancia.
- El 50% cuenta con alarmas.

Y para fallas de energía, se protegen por medio de:

- El 64% cuenta con equipos suministradores de energía eléctrica.
- El 21% cuenta con generadores de energía eléctrica.

Riesgos internos:

Naturales: incendio, inundación, otros.

- El 57% cuenta con respaldos externos.
- El 21% cuenta con seguro.

Humanos: robo, sabotaje, huelgas, fraude, destrucción (voluntaria e involuntaria), otros.

Se protegen por uno o más de los siguientes medios:

- El 100% cuenta con áreas restringidas al centro de cómputo.
- El 100% cuenta con respaldos internos.
- El 57% cuenta con respaldos externos.

- El 79% cuenta con claves individuales.
- El 71% cuenta con servicios de vigilancia.
- El 50% cuenta con alarmas.
- El 79% registros sobre prestamos.
- El 71% cuenta con cambio de contraseña frecuentemente.

Y para destrucción (voluntaria e involuntaria) de: datos, material, equipo. Se protegen con:

- El 100% cuenta con sistemas de antivirus residentes.
- El 36% cuenta con capacitaciones.

Materiales: Descompostura de equipo, fallas de energía, otros.

Se protegen por uno o más de los siguientes medios de protección:

- El 100% cuenta con mantenimiento.
- El 64% cuenta con equipos suministradores de energía eléctrica.
- El 21% cuenta con generadores de energía.

h) En la pregunta trece, se obtuvo información sobre la frecuencia con que revisan las precauciones tomadas para evitar contingencias.

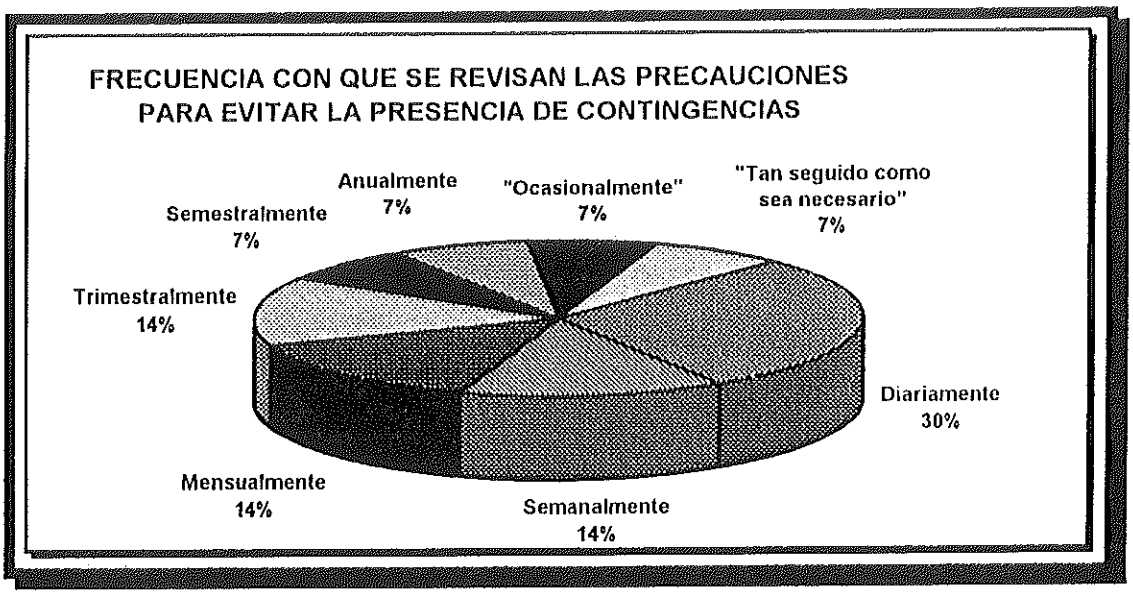


Figura 4.4 Frecuencia con que se revisan las precauciones tomadas para evitar contingencias.

i) En la pregunta catorce, se obtuvo información sobre si a pesar de las precauciones tomadas, se les han presentado contingencias.

A todas las instituciones, se les han presentado al menos una contingencia de menor impacto, dentro de las cuales podemos citar a:

- El 71% daños físicos a hardware.
- El 57% pérdida de información.
- El 21% problemas con software.

No se dieron casos de presencia de contingencias de mayor impacto.

j) En la pregunta quince, se obtuvo información de cómo han solucionado las contingencias presentadas.

Todas las instituciones solucionaron sus contingencias favorablemente, ya que contaban con:

- Respaldos de software.
- Respaldos de información.

Y para los casos de problemas con hardware:

- Se les dio el mantenimiento necesario.

k) En la pregunta dieciséis, se obtuvo información sobre si las contingencias presentadas les han causado pérdidas de tiempo, dinero e información.

A todas las instituciones la presencia de contingencias les han causado pérdidas de tiempo y a veces además del tiempo, pérdidas de dinero e información, pero más que nada una mala imagen hacia sus clientes.

l) En la pregunta diecisiete, se obtuvo información sobre la importancia de contar con un plan de contingencias óptimo.

Todas las instituciones aceptaron la gran importancia de tener un plan de contingencias óptimo. O en su defecto, el proteger al máximo sus recursos de información, hasta donde se lo permita su presupuesto.

CONCLUSIONES:

- El 86% de las instituciones que contestaron la encuesta, no cuentan con ningún tipo de prevención contra fraudes o sabotajes, por no creerlo necesario. Lo cual es lo más común en la ideología actual en cómputo.
- El 79% de las instituciones que contestaron la encuesta, no cuentan con prevenciones para diversas fallas, por falta de recursos económicos, pero están conscientes de la falla.
- El 50% de las instituciones que contestaron la encuesta, no consideran tan necesario el contar con prevenciones para ciertas fallas por no haberlo requerido, se prevendrán después de haber tenido una mala experiencia. Esto es, están en espera de vivir una mala experiencia, para prevenir las posteriores.
- Es importante mencionar, que las instituciones en general, toman protecciones hacia sus recursos de información, pero por lo presentado anteriormente, se pueden apreciar una serie de fallas en la protección a los mismos.
- Es probable que algunas de las 38 instituciones que no contestaron la encuesta no cuenten con un plan de contingencias, lo cual nos da un porcentaje considerable de instituciones sin este tipo de precauciones.

CAPÍTULO V

GUÍA GENERALIZADA PARA IMPLANTAR UN PLAN DE CONTINGENCIAS

5.1 Guía.

Esta guía se basó para su desarrollo, en la encuesta realizada a diversas instituciones sobre el cuidado de sus recursos de información, y de bibliografía sobre auditoría en informática.

La guía se desarrolla de acuerdo a diferentes clasificaciones de etapas, fases y tareas a seguir. La guía se clasificó de la siguiente manera:

I. Primera Etapa

Fase: Evaluación de Riesgos.

Tareas

1. Creación de un comité de contingencias y selección de un responsable del mismo.
2. Identificar riesgos que amenazan los recursos de información.
3. Análisis de la protección actual que se les brinda a los recursos de información.
4. Clasificación de riesgos y de sistemas, determinación del lapso crítico de recuperación y análisis de la materialización de contingencias.
5. Reporte general de contingencias factibles a presentarse y estimación de pérdidas.

II. Segunda Etapa

Fase: Selección de estrategias.

Tareas

1. Identificar estrategias que protejan contra riesgos que amenazan a los recursos de información.

III. Tercera Etapa

Fase: Presentación y mantenimiento del plan de contingencias.

Tareas

1. Preparar el plan de contingencias.
2. Definición de planes de acción.
3. Mantenimiento del plan de contingencias.

5.1.1 Aprobación formal de puntos.

Para cada fase hay que aprobar una tarea para avanzar a la siguiente tarea.

Se debe aprobar o estar de acuerdo en:

- Terminar una tarea.
- Efectuar modificaciones a tareas.
- Preparar a nuevos grupos de trabajo.

5.1.2 Duración y complejidad.

La duración y complejidad son determinadas por la extensión y giro de la institución.

La duración y complejidad de un plan de contingencias varía de acuerdo a:

- El grado de riesgo al que se está expuesto.
- El tamaño del centro de cómputo y el número de usuarios.
- El monto de inversión y el esfuerzo que se emplea para el desarrollo del plan de contingencias.

DESARROLLO

5.2 Primera etapa.

5.2.1 Fase: Evaluación de riesgos.

Introducción

Presencia de desastres.

Un desastre es un suceso que puede ocurrir en cualquier momento, y tiene potencial para interrumpir el funcionamiento normal de una institución (Valerio,94).

Un desastre puede ocurrir por contingencias de menor impacto, tales como: descompostura de equipo, fallas de energía, otros. Aunque también un desastre puede ocurrir por contingencias de mayor impacto, como: temblor, tormenta, otros. Un plan de contingencias óptimo debe prever todo tipo de contingencias que puedan ocasionar un desastre.

Esta fase consiste en identificar riesgos factibles, para la institución en cuestión.

DESARROLLO DE TAREAS

1. Creación de un comité de contingencias y selección de un responsable del mismo.

Esta tarea es la más importante, ya que los planes de contingencias requieren buenas bases para iniciarse.

Es muy importante contar con la aprobación de los altos niveles, por los cambios o movimientos que pueda generar el plan de contingencias.

A continuación se lista una serie de características que deben tener los miembros para integrar el comité de contingencias y el responsable del mismo:

La persona responsable del comité de contingencias debe de:

- Tener capacidad de liderazgo.
- Tener total conocimiento del funcionamiento de la institución e ir al día en su proceso diario.
- De preferencia no ser miembro del departamento de informática, ya que éste puede asesorarlo, en lo técnico y en todo lo relacionado a su área.
- Contar con la aprobación de los altos niveles, para que pueda proponer modificaciones en el plan de contingencias.
- En caso de que el responsable del comité de contingencias, sea una persona externa a la institución, ésta se deberá de apoyar directamente con personal relacionado con el total funcionamiento de la institución.

Los miembros del comité de contingencias, se deben de seleccionar cuidadosamente, y para ello se recomienda que tengan:

- Capacidad analítica y deductiva.
- Capacidad de relaciones humanas.
- Capacidad para trabajar en equipo.
- Total conocimiento del funcionamiento del centro de cómputo, como de la institución en general. Además, es recomendable que los miembros sean en total un número par (2,4), para evitar igualdad de votos al dar soluciones a diferencias presentadas (aunando el voto del responsable del comité de contingencias).

Hay que considerar que se pueden presentar situaciones en las que será necesario el contar con grupos de trabajo, que auxilien a los miembros del comité de contingencias a desarrollar diversas tareas. Los integrantes de estos grupos de trabajo serán definidos por los miembros del comité de contingencias.

2. Identificar riesgos que amenazan los recursos de información.

En esta tarea se deben de identificar los riesgos que amenazan a la institución, analizando la factibilidad de que se materialicen. Un esquema de riesgos factibles a materializarse es presentado a continuación, el cual se clasifica por áreas (Valerio,94).

Para cada uno de los riesgos mencionados, se deberá hacer la siguiente pregunta:

¿ Es factible que se materialice este riesgo en nuestra institución?

Para poder determinar si se tomará en cuenta o no ese riesgo.

RIESGOS					
EXTERNOS			INTERNOS		
NATURALES	*HUMANOS*	*MATERIALES*	*NATURALES*	*HUMANOS*	*MATERIALES*
TEMBLOR	*ROBO*	*PÉRDIDA DE INFORMACIÓN*	*INCENDIO*	*ROBO*	*DESCOMPOSTURA DE EQUIPO*
TORMENTA	*SABOTAJE*	*FALLAS DE ENERGÍA*	*INUNDACIÓN*	*DESTRUCCIÓN VOLUNTARIA E INVOLUNTARIA (SOFTWARE, HARDWARE, INFORMACIÓN)*	*FALLAS DE ENERGÍA*
HURACÁN	*FRAUDE*	*OTROS*	*OTROS*	*SABOTAJE*	*OTROS*
INCENDIO	*OTROS*			*HUELGAS*	
INUNDACIÓN				*FRAUDE*	
OTROS				*PERSONAL CLAVE*	
				OTROS	

Tabla 5.1 Riesgos factibles a materializarse.

Se recomienda analizar detalladamente la existencia de riesgos factibles en cada área, que no se encuentren en el esquema anterior.

Se recomienda el uso del siguiente formato, para puntualizar los riesgos factibles a materializarse en la institución.

Relación de riesgos factibles a materializarse en la institución

Fecha: _____

Externos:

Naturales: _____

_____

Humanos: _____

_____

Materiales: _____

_____

Internos:

Naturales: _____

_____

Humanos: _____

_____

Materiales: _____

_____

Figura 5.1 Formato para puntualizar los riesgos factibles a materializarse.

3. Análisis de la protección actual que se les brinda a los recursos de información.

En base al esquema presentado anteriormente, se debe realizar un análisis de las protecciones actuales de la institución a los recursos de información, en base a los riesgos factibles.

Para lo cual se recomienda realizar las siguientes preguntas:

1) ¿ Qué tan probable es, que se presente cada contingencia factible detectada (nula, poca, mediana, alta) ?

2) ¿ Para las contingencias factibles detectadas, existen precauciones ?

3) ¿ Qué precauciones se toman ?

4) ¿ Cada cuánto tiempo las revisan ?

5) ¿ Quién es el responsable de revisar las precauciones tomadas ?

Se recomienda el uso del siguiente formato, para una mejor visión de las protecciones actuales a los riesgos factibles detectados.

Relación de las protecciones actuales a los riesgos factibles detectados

*Fecha:*_____

Riesgos Factibles	*Probabilidad de Presencia (nula, poca, mediana, alta)*	*¿Existen precauciones para prever la materialización de los riesgos?*	*¿Cuáles son?*	*¿Cada cuánto se revisan las precauciones tomadas?*	*¿Quién es el responsable de revisarlas?*

Figura 5.2 Protecciones actuales a los riesgos factibles detectados.

4. Clasificación de riesgos y de sistemas, determinación del lapso crítico de recuperación y análisis de la materialización de contingencias.

El propósito del plan de contingencias es tratar de evitar al máximo la presencia de contingencias en la institución, pero si éstas se presentaran, tratar de minimizar las consecuencias, y sobre todo, que el funcionamiento normal de la institución se reanude a la mayor brevedad posible. Es importante el tener una clasificación de los riesgos y su prioridad.

Clasificación de los riesgos (Valerio,94).

Críticos: Estos riesgos son los que al materializarse, detienen total o casi totalmente el funcionamiento normal de la institución, siendo éste muchas veces por un largo período de tiempo, y a su vez causando daños muy grandes a la institución.

Vitales: Estos riesgos son los que al materializarse, detienen por un período relativamente alto el funcionamiento normal de la institución. Estas contingencias deben ser solucionadas a la mayor brevedad posible.

Sensibles: Estos riesgos son los que al materializarse, detienen por un período muy breve el funcionamiento normal de la institución. Estas contingencias son solucionadas rápidamente.

No-Críticos: Estos riesgos son los que al materializarse, no afectan para nada el funcionamiento normal de la institución. Sin embargo es conveniente solucionar la contingencia, lo más pronto posible.

Un plan de contingencias siempre debe de poner especial cuidado en los sistemas de carácter crítico, ya que son los que tienen mayor importancia para la supervivencia de una institución. Muchos sistemas afectan a diferentes departamentos y éstos a su vez a otros, es decir, se forma una cadena, haciendo bastante difícil la determinación de todas las consecuencias de no contar con alguna de las aplicaciones. Es conveniente hacer una estimación de cada una de estas aplicaciones para determinar cuanto puede resistir el procesamiento normal de datos sin ellas, una hora, un día, una semana, un mes. De esta manera identificaremos los sistemas críticos y sucesivamente los demás.

Clasificación de los sistemas (Valerio,94).

Críticos: Estas funciones no se deben llevar a cabo, a menos que sean reemplazadas por capacidades idénticas. No se pueden reemplazar por métodos manuales. La tolerancia de la interrupción es muy baja por lo que el costo de la interrupción es muy alto.

Vitales: Estas funciones sí se pueden reemplazar manualmente pero sólo por un período breve. Existe una tolerancia mayor a la interrupción que con los sistemas críticos y por consecuencia costos de interrupción ligeramente menores, siempre y cuando se reanude el procesamiento de datos, dentro de un marco temporal determinado.

Sensibles: Estas funciones pueden realizarse en forma manual, con costos tolerables por un largo período. Si se van a realizar en forma manual, el proceso es difícil y es conveniente contar con mano de obra adicional.

No-críticos: Estas funciones pueden ser interrumpidas durante un largo período de tiempo, con poco o sin ningún costo para la institución y proporcionan poco o ningún esfuerzo de ponerse al corriente cuando se restauran.

Determinación del lapso crítico de recuperación

El "lapso crítico de recuperación", es el tiempo predeterminado en que debe reanudarse el funcionamiento normal de la institución, antes de arriesgarse a tener pérdidas. Estos marcos de tiempo siempre dependen de un desastre no-desastre, tomando en cuenta el giro de la institución. Por ejemplo, las instituciones financieras, siempre tendrán un lapso crítico de recuperación, mucho menor que una institución manufacturera. También influye mucho la época del año y el día de la semana en la recuperación del procesamiento normal de datos, ya que si a un banco se le presenta una contingencia menor un sábado a la medianoche tiene un lapso mayor para recuperarse que sí se le presentara un lunes a la medianoche (Valerio,94).

Se recomienda el uso de los siguientes formatos, para una mejor visión de las clasificaciones de los riesgos y sistemas.

CLASIFICACIÓN DE LOS RIESGOS

Fecha: _____

Críticos	*Lapso crítico de recuperación*	*Vitales*	*Lapso crítico de recuperación*	*Sensibles*	*Lapso crítico de recuperación*	*No Críticos*	*Lapso crítico de recuperación*

Figura 5.3 Clasificación de los riesgos.

CLASIFICACIÓN DE LOS SISTEMAS

Fecha: _____

Críticos	*Lapso crítico de recuperación*	*Vitales*	*Lapso crítico de recuperación*	*Sensibles*	*Lapso crítico de recuperación*	*No Críticos*	*Lapso crítico de recuperación*

Figura 5.4 Clasificación de los sistemas.

En base al análisis obtenido, se debe analizar el impacto de los riesgos en general, esto es, preguntarse:

1) ¿ Qué pasaría si se materializa alguno de los riesgos factibles detectados ?

2) ¿ Qué sistemas afectaría ?

3) ¿ Cuál sería la opción más factible para solucionarla ?

4) ¿ Cuál sería el costo de la recuperación ?

Esto es, se deben de determinar las hipótesis y las conclusiones.

5. Reporte general de contingencias factibles a presentarse y estimación de pérdidas.

En esta tarea, se debe de generar un reporte de los riesgos factibles que se pueden presentar, el reporte general que se obtiene es muy completo ya que determina los riesgos factibles por prioridades (críticos, vitales, sensibles, no-críticos), probabilidad de ocurrencia, sistemas que afecta, tiempo de recuperación, costo de recuperación y soluciones actuales.

Reporte general de los riesgos factibles a presentarse y estimación de pérdidas

Fecha: _____

Riesgo	*Clasificación (Crítico, vital, sensible, no-Crítico)*	*Probabilidad de ocurrencia (nula, poca, mediana, alta)*	*Sistemas afectados*	*Tiempo de recuperación*	*Costo de recuperación*	*Soluciones actuales*

Figura 5.5 Reporte general de los riesgos factibles a presentarse y estimación de pérdidas.

5.3 Segunda etapa.

5.3.1 Fase: Selección de estrategias.

Introducción

Estrategias factibles para protección a los recursos de información de la institución en cuestión.

Esta etapa es fácilmente cubierta cuando ya tenemos identificados los riesgos y sistemas críticos. Ya que son los de mayor importancia para la supervivencia de la institución en cuestión.

Esta fase consiste en determinar soluciones factibles para contrarrestar la materialización de riesgos identificados y el impacto de los mismos.

DESARROLLO DE TAREAS

1. Identificar estrategias que protejan contra riesgos que amenazan a los recursos de información.

a) Estrategias factibles para proteger la información.

- Respaldos internos y externos.

b) Estrategias factibles para proteger el software.

- Respaldos internos y externos.

c) Estrategias factibles para proteger el hardware.

- Seguro.
- Mantenimiento.

d) Estrategias factibles para proteger el personal.

- Seguro.

e) Estrategias factibles para proteger información, software y hardware.

- Instalaciones de recuperación.

La clasificación presentada corresponde a los principales recursos en cómputo y algunos ejemplos de estrategias factibles.

Estrategias factibles para proteger a los recursos de información de posibles riesgos a materializarse.

ESTRATEGIAS FACTIBLES PARA EL CUIDADO DE LOS RECURSOS DE INFORMACIÓN	
RIESGOS	*ESTRATEGIAS*
• *Temblores, tormentas, relámpagos, otros.*	• Seguro, alejarse de áreas de alta amenaza recurrente en riesgo, pararrayos.
• *Incendio.*	• Seguro, detectores y alarmas, ventiladores, extractores, sistemas rociadores, sistemas expansores de gas, uso de materiales inflamables en paredes y puertas, limpieza general continua, (particularmente de papel de impresión).
• *Inundación.*	• Seguro, situación cuidadosa de todos los conductos de agua cercanos al centro de cómputo, alejando éste de los pisos de abajo, lugares con mayor riesgo de ser susceptibles a inundaciones.
• *Robo, sabotaje, fraude, otros.*	• Seguro, áreas restringidas al centro de cómputo, respaldos, claves individuales, servicios de vigilancia, alarmas, registros sobre prestamos, fianza de fidelidad.
• *Pérdida de servicios.*	• Fuentes de poder ininterrumpidas, reguladores de voltaje, generadores propios, capacidad sobrada en equipo de aire acondicionado.
• *Destrucción (voluntaria e involuntaria) de: información, software, hardware.*	• Sistemas de antivirus residentes, capacitaciones, despido.
• *Descompostura de equipo.*	• Mantenimiento, equipo extra.
• *Personal clave.*	• Capacitaciones, documentación de apoyo.

Tabla 5.2 Estrategias factibles para el cuidado de los recursos de información.

Instalaciones de recuperación.

Cuando ocurre un desastre y éste a su vez trae consigo un largo lapso de recuperación, es necesario contar con alternativas de respaldo fuera de la institución, para continuar con el procesamiento normal de la institución y no tener pérdidas económicas.

A continuación se muestra un esquema con los tipos de centros de hardware de respaldo en otra sede disponible: (Valerio,94).

Instalación de Recuperación	Descripción	Costo de Instalación	Costo de Mantenimiento
Hot-Sites (Alternativas de emergencia) Clave: (HS)	Estos centros de emergencia están totalmente configurados y listos para operar dentro de pocas horas. El equipamiento y el software son compatibles con el centro de cómputo primario, del que ahora actúa como respaldo. Las únicas necesidades adicionales son las de personal, programas y archivos de datos.	Alto	Alto
Warm-Sites Clave: (WS)	Estos son centro de cómputo que están parcialmente configurados, generalmente con equipo seleccionado, como unidades de disco, cintas, controladores, pero sin el computador principal. Un warm-site, por lo general cuenta con un CPU menor, pero se puede conseguir un computador rápidamente para una instalación de emergencia (siempre que sea un modelo de uso común) y como el computador es la unidad más cara el arreglo es menos costoso que un hot-site. Después de instalar los componentes necesarios, el centro de cómputo puede ser considerado listo para usarse en cuestión de horas; ahora que sí se requiere de otro CPU su instalación puede llevar días o semanas.	Mediano	Mediano
Cold-Sites Clave: (CS)	Estos son centros de cómputo que están configurados básicamente, esto es con lo indispensable, para operar un centro de cómputo. El cold-site está listo para recibir el equipamiento pero no ofrece ningún componente instalado antes de que sea necesario. La activación del centro de cómputo puede llevar semanas.	Bajo	Bajo

Instalación de Recuperación	Descripción	Costo de Instalación	Costo de Mantenimiento
Centro duplicado de procesamiento de información Clave: (CDPI)	Estos centros pueden variar desde un hot-site en espera de utilización hasta acuerdos recíprocos con la instalación de otra institución. Por lo general existen menos dificultades para coordinar compatibilidad en el caso de centros duplicados de procesamiento de información.	Alto	Alto
Acuerdos Recíprocos Clave: (AR)	Los acuerdos recíprocos son contratos entre una o más organizaciones con equipos o aplicaciones similares. En un acuerdo típico, las partes se comprometen a brindar tiempo de procesamiento cuando surja una emergencia.	Bajo	Bajo
Centro de respaldo portátil Clave: (CRP)	Es semejante al servicio que presta un cold-site, pero basado en unidades modulares las cuales pueden ser localizadas en nuestra propiedad, usualmente en un estacionamiento. Tiene las mismas características que un servicio de respaldo en cold-site, excepto que no se tiene el problema de relocalización de los empleados. Con objeto de anticiparnos a un desastre, es recomendable instalar algunas líneas de comunicación al estacionamiento, para ser utilizados como base. El tener este servicio, nos permite reanudar el procesamiento de datos en un tiempo considerablemente corto, después de un desastre.	Alto	Alto
Servicio de respaldo de emergencia Clave: (SRE)	Es similar al uso de servicio de oficina y puede ser relativamente caro, regularmente los contratos son por un año y ofrecen la disponibilidad de prueba. Estos servicios funcionan de la forma de "El primero que llegue, el primero en ser atendido", debido a que otros suscriptores pueden ser aceptados por el mismo desastre al mismo tiempo. Como otros servicios, este servicio nos causa el problema de la transportación de nuestros empleados.	Alto	Alto
Acuerdo de respaldo mutuo Clave: (ARM)	A veces se refiere a "Acuerdos Recíprocos", son frecuentemente informales y poco funcionales. El equipo y los sistemas operativos deben ser compatibles y cada una de las partes debe contar con suficiente capacidad para correr sus sistemas y los del otro contratante. Es excepcionalmente difícil contar con esta capacidad; debido a que esta tiende a ser utilizada para desarrollos propios.	Bajo	Bajo

Instalación de Recuperación	Descripción	Costo de Instalación	Costo de Mantenimiento
Servicio privado de respaldo en cold Clave: (SPRC)	Es similar al servicio de respaldo en cold-site, pero exento de los conflictos con otros suscriptores y los inconvenientes derivados para los empleados. Claro que estas ventajas, incrementan costos, los cuales hay que analizar.	Alto	Alto
Servicio de respaldo en emergencia local Clave: (SREL)	Esta opción es la más cara, pero también la que ofrece una recuperación suficientemente rápida. Su localización, podría ser difícil o costoso mantenerlo y cuidar su compatibilidad con el equipo de producción. El centro de cómputo emergente puede ser utilizado para procesamiento de datos de sistemas no críticos. Es importante asegurarse que los sistemas críticos puedan ser respaldados dentro de un lapso de tiempo preestablecido. No debe de permitirse que los sistemas no-críticos se conviertan en críticos.	Alto	Alto
Combinación de opciones *Clave: (CO)*	Algunas de las desventajas de las diferentes opciones pueden dejarse atrás mediante la combinación de ellas; por ejemplo, una compañía que requiere recuperarse de un desastre en un corto periodo de tiempo, puede suscribirse a un servicio de respaldo de emergencia para cubrir las primeras dos o tres semanas y también puede hacerlo con un centro portátil de respaldo el cual puede ser instalado para su uso durante esas dos o tres semanas iniciales. No hay que olvidar que el objetivo es reanudar a la brevedad posible las operaciones normales, y a menudo esto llevará un tiempo considerable.	Alto	Alto

Tabla 5.3 Instalaciones de recuperación.

En base a las estrategias factibles presentadas anteriormente, es recomendable el uso de las siguientes matrices, para tener una mejor visión de las estrategias factibles que ayuden a minimizar riesgos predeterminados.

Matriz Riesgos - Estrategias	Estrategias Factibles para el Cuidado de los Recursos de Información								
Riesgos									

Figura 5.6 Matriz riesgos - estrategias factibles para el cuidado de los recursos de información.

Matriz Riesgos - Estrategias	Instalaciones de Recuperación								
Riesgos									

Figura 5.7 Matriz riesgos - estrategias respecto a instalaciones de recuperación.

A continuación se presenta un ejemplo de cómo llenar las matrices presentadas anteriormente, este caso es para el cuidado de los recursos de información:

Matriz Riesgos - Estrategias	**Estrategias Factibles para el Cuidado de los Recursos de Información**								
Riesgos	*Seguro*	*Alarmas*	*Respaldos Internos*	*Respaldos Externos*	*Capaci-taciones*	*otros,*			
Temblor, tormenta, etc.	*X*			*X*					
Incendio	*X*	*X*	*X*	*X*					
Robo	*X*	*X*	*X*	*X*					
Destrucción de: información, software, hardware.	*X*		*X*	*X*	*X*				
otros,...									

Como se puede apreciar en el ejemplo anterior, se escriben los riesgos predeterminados contra las estrategias factibles predeterminadas de la institución en cuestión, y en base a esto se seleccionan las estrategias factibles a implantarse en la misma.

Una vez seleccionadas las diversas estrategias factibles, es necesario clasificar a cada una de ellas como: ó*ptima, adecuada, aceptable.*

Siendo:

1. *Óptima:* La estrategia de costo razonable y que contrarreste un mayor número de riesgos en general.
2. *Adecuada:* La estrategia de costo mayor y que contrarreste en su mayoría riesgos críticos.
3. *Aceptable:* La estrategia de costo menor y que contrarreste riesgos vitales.

Una vez clasificadas las diversas estrategias seleccionadas, será muy fácil determinar soluciones factibles para la institución en cuestión.

5.4 Tercer etapa.

5.4.1 Fase: Presentación y mantenimiento del plan de contingencias.

Introducción

Documentación de resultados.

Una vez finalizadas las etapas anteriores se da paso a presentar resultados.

Esta fase consiste en presentar los riesgos factibles a materializarse en la institución en cuestión, estrategias factibles para implantarse y así contrarrestar la materialización de los mismos.

DESARROLLO DE TAREAS

1. Preparar el plan de contingencias.

El plan de contingencias deberá de estar formado por las siguientes secciones:

- Riesgos factibles.

  Se describen los riesgos actuales, la protección que se tiene sobre estos y reseñas de contingencias presentadas.

- Reporte de estrategias.

  Se presentan las estrategias de prevención propuestas.

- Selección de estrategias.

  En base a los reportes anteriores, se presenta como reporte final la determinación de estrategias factibles, acordes a los recursos y requerimientos de la institución.

2. Definición de planes de acción.

En base a las estrategias seleccionadas, se deberá definir la forma en que serán implantadas.

Determinando lo siguiente:

- Personal necesario.

  Se definirá cuantas personas serán necesarias para desarrollar la estrategia en cuestión.

- Apoyo externo.

  Se definirá si será necesario el contar con apoyo externo.

- Recursos requeridos.

  Se definirán los recursos requeridos de software, hardware, entre otros.

- Tiempo de implantación.

  Se definirá un marco de tiempo para finalizar la implantación de la estrategia en cuestión.

- Tareas a realizar.

  Se definirán las tareas a realizar para operar la estrategia.

- Implantación.

  Se definirán pasos a realizar para implantar la estrategia.

- Monitoreo.

  Se definirán formas de evaluación de la estrategia, cuando esté implantada.

3. Mantenimiento del plan de contingencias.

Se debe de responsabilizar a alguien del mantenimiento total del plan de contingencias. Ya que es fácil iniciarlo pero culminarlo y mantenerlo no. La persona responsable del mantenimiento debe asegurarse de que el plan de contingencias sea considerado en los cambios institucionales. Es decir, el plan de contingencias se debe de actualizar, conforme se realicen cambios en la institución.

CAPÍTULO VI

IMPLANTACIÓN DE LA GUÍA

6.1 Desarrollo del caso real.

En este capítulo se desarrollará paso a paso la implantación de la guía generalizada en Comisión Estatal de Servicios Públicos de Ensenada (C.E.S.P.E.).

- **Desarrollo de la primera etapa.**

1. Creación de un comité de contingencias y selección de un responsable del mismo.

Responsable del comité de contingencias:

P.L.C.C. Dalila Vazquez Romero

Tesista

Miembros del comité de contingencias:

Lic. Inf. Alfonso Talavera Hernández

Coordinador de Informática

L.C.C. Carlos Flores Campos

Analista programador

2. Identificar riesgos que amenazan los recursos de información.

Relación de riesgos factibles a materializarse en la institución

Fecha: 23/05/96

Externos:

Naturales: *Temblor, tormenta, incendio, inundación.*

Humanos: *Robo, sabotaje, fraude.*

Materiales: *Fallas de energía.*

Internos:

Naturales: *Incendio, inundación.*

Humanos: *Robo, destrucción (voluntaria e involuntaria), sabotaje, huelgas, fraude, personal clave.*

Materiales: *Descompostura de equipo, fallas de energía.*

3. Análisis de la protección actual que se les brinda a los recursos de información.

Relación de las protecciones actuales a los riesgos factibles detectados *Fecha:03/06/96*					
Riesgos Factibles	***Probabilidad de Presencia (nula, poca, mediana, alta)***	***¿Existen precauciones para prever la materialización de los riesgos?***	***¿Cuáles son?***	***¿Cada cuanto se revisan las precauciones tomadas?***	***¿Quién es el responsable de revisarlas?***
Temblor	Mediana	Si	Seguro	Según el contrato	Serv. Generales
Tormenta	Mediana	Si	Seguro	Según el contrato	Serv. Generales
Incendio	Mediana	Si	Seguro, extinguidores	Según el contrato	Serv. Generales
Inundación	Poca	Si	Seguro	Según el contrato	Serv. Generales
Robo	Alta	Si	Seguro, policía, alarmas	Diariamente	Serv. Generales
Sabotaje	Mediana	Si	Policía, registro de entradas	Diariamente	No definido
Fraude	Poca	Si	Uso de claves	Diariamente	Rodolfo Arballo
Fallas de energía	Alta	Parte	UPS global solo para las computadoras.	Esporádicamente	No definido
Destrucción Voluntaria e Involuntaria	Alta	Parte	Seguro, respaldos internos	Diariamente	Rodolfo Arballo

Relación de las protecciones actuales a los riesgos factibles detectados

Fecha:03/06/96

Riesgos Factibles	*Probabilidad de Presencia (nula, poca, mediana, alta)*	*¿Existen precauciones para prever la materialización de los riesgos?*	*¿Cuáles son?*	*¿Cada cuanto se revisan las precauciones tomadas?*	*¿Quién es el responsable de revisarlas?*
Huelga	Poca	Si	Seguro	Según el contrato	Serv. Generales
Descompostura de equipo	Alta	Si	Mantenimiento	Según el contrato	Serv. Generales
Personal Clave	Mediana	Parte	Guías de algunos sistemas	Cuando ocurre un problema	Carlos Flores

4. Clasificación de los riesgos y de sistemas, determinación del lapso crítico de recuperación y análisis de la materialización de contingencias.

CLASIFICACIÓN DE LOS RIESGOS

Fecha 17/06/96

Críticos	*Lapso crítico de recuperación*	*Vitales*	*Lapso crítico de recuperación*	*Sensibles*	*Lapso crítico de recuperación*	*No críticos*	*Lapso crítico de recuperación*
Temblor	Depende de los daños	Robo	Depende del tipo de robo	Personal clave	1 semana		
Tormenta	Depende de los daños	Sabotaje	Depende del tipo de sabotaje				
Incendio	Depende de los daños	Destrucción Voluntaria e Involuntaria	De 1 a 2 semanas				
Inundación	Depende de los daños	Fallas de energía	2 horas				
Huelga	Hasta que termine	Fraude	Depende del tipo de fraude				
Descompos-tura de equipo	De 1 a 2 semanas						

CLASIFICACIÓN DE LOS SISTEMAS

Fecha: 17/06/96

Criticos	*Lapso crítico de recuperación*	*Vitales*	*Lapso crítico de recuperación*	*Sensibles*	*Lapso crítico de recuperación*	*No críticos*	*Lapso crítico de recuperación*
S. O. del Servidor	2 días	Requerimien-tos	1 día a 2 sem.	Aclaraciones	1 día a 2 semana	Proobras	1 día
Corrupción de la B. D.	2 días	Cajas	1 día a 2 sem.	Tiraderos	1 día a 1 semana	Consulta rezago	1 día
Servicio medido	1 día a 1 semana	Padrón de usuarios	1 día a 2 sem.	Costos	1 día a 1 semana	Consulta microfilm	1 día
Nomina	1 día a 1 semana	Obras	1 día a 2 sem.	Activos fijos	1 día a 1 semana		
Cortes	1 día	Medidores	1 día a 2 sem.	Gasolina	1 día a 1 semana		
		Contabilidad	1 día a 2 sem.	137	1 día a 1 semana		
		Almacén	1 día a 2 sem.				
		Compras	1 día a 2 sem.				
		Egresos	1 día a 2 sem.				
		Presupuestos	1 día a 2 sem.				
		Caja ahorros	1 día a 2 sem.				
		Manteni-miento	1 día a 2 sem.				
		Facturación	1 día a 2 sem.				
		Sol. de Serv.	1 día a 2 sem.				
		Resguardos	1 día a 2 sem.				
		Comunal	1 día a 2 sem.				

5. Reporte general de contingencias factibles a presentarse y estimación de pérdidas.

Reporte general de los riesgos factibles a presentarse y estimación de pérdidas *Fecha:01/07/96*						
Riesgo	*Clasificación (crítico, vital, sensible, no-crítico)*	*Probabilidad de ocurrencia (nula, poca, mediana, alta)*	*Sistemas afectados*	*Tiempo de recuperación*	*Costo de recuperación*	*Soluciones actuales*
Temblor	Crítico	Mediana	Todos	Depende de los daños	Depende de los daños	Seguro
Tormenta	Crítico	Mediana	Todos	Depende de los daños	Depende de los daños	Seguro
Incendio	Crítico	Mediana	Todos	Depende de los daños	Depende de los daños	Seguro, extinguidores
Inundación	Crítico	Poca	Todos	Depende de los daños	Depende de los daños	Seguro
Huelga	Crítico	Poca	Todos	Duración de la huelga	Depende de lo que se solucione	Seguro
Descompostura de equipo	Crítico	Alta	Todos los del equipo	Más de 2 días	Alto	Mantenimiento
Robo	Vital	Alta	Depende del robo	1 día a 8 semanas	Alto	Seguro, policía, alarmas sólo en 2 deptos.
Sabotaje	Vital	Mediana	Depende del tipo de sabotaje	1 día a 8 semanas	Alto	Policía, registro de entradas

Reporte general de los riesgos factibles a presentarse y estimación de pérdidas

Fecha 01/07/96

Riesgo	*Clasificación (crítico, vital, sensible, no-crítico)*	*Probabilidad de ocurrencia (nula, poca, mediana, alta)*	*Sistemas afectados*	*Tiempo de recuperación*	*Costo de recuperación*	*Soluciones actuales*
Destrucción Voluntaria e Involuntaria	Vital	Alta	Depende del sistema en que ocurra	1 día a 8 sem.	Alto	Seguro, respaldos internos
Fallas de energía	Vital	Alta	Todos	Lo que dure	Bajo	UPS global solo para las computadoras.
Fraude	Vital	Poca	Depende del fraude	1 día a 8 sem.	Alto	Uso de claves
Personal clave	Sensible	Mediana	Los del responsable (personal clave)	1 día a 2 sem.	Bajo	Guías de algunos sistemas

- **Desarrollo de la segunda etapa.**

1. Identificar estrategias que protejan contra riesgos que amenazan a los recursos de información.

Matriz Riesgos - Estrategias	Estrategias Factibles para el Cuidado de los Recursos de Información					
Riesgos	Respaldos Externos	Alarmas	Capacitaciones	Equipo extra	Generador de energía eléctrica	Documentación de apoyo
Temblor	X					
Tormenta	X					
Incendio	X	X				
Inundación	X	X				
Robo	X	X				
Destrucción Voluntaria e Involuntaria	X		X			
Descompostura de equipo				X		
Personal clave			X			X
Fallas de energía					X	

Instalaciones de recuperación

No se cuentan con instalaciones de recuperación en esta ciudad, pero en este caso C.E.S.P.E. cuenta con una sucursal la cual puede ser utilizada como sede alternativa. Siempre y cuando se adquiera un servidor adecuado, se instale el software necesario y se bajen los respaldos.

Es una gran ventaja el tener esta sucursal, ya que si se llegara a presentar una contingencia en cualquiera de las dos sedes, se tendría acceso inmediato en la otra.

- **Desarrollo de la tercera etapa.**

1. Preparar el plan de contingencias.

PLAN DE CONTINGENCIAS

- ***Riesgos factibles***

Riesgos Actuales	Protecciones Actuales	Contingencias Vividas
Temblor	*Seguro*	*No*
Tormenta	*Seguro*	*No*
Incendio	*Seguro, extinguidores*	*Si, leve*
Inundación	*Seguro*	*No*
Huelga	*Seguro*	*No*
Descompostura de equipo	*Mantenimiento*	*Si, grave*
Robo	*Seguro, dos alarmas en deptos: claves, policía*	*Si, leves*
Sabotaje	*Policía 24 horas, registro de entradas*	*No*
Destrucción (voluntaria e involuntaria) de: Software, Hardware e Información	*Seguro, respaldos internos*	*Si, leves*
Fallas de energía	*Suministrador de energía eléctrica*	*Si, leves*
Fraude	*Uso de claves*	*No*
Personal clave	*Gulas de algunos sistemas*	*Si, grave*

- *Reporte de Estrategias*

Matriz Riesgos - Estrategias	Estrategias Factibles para el Cuidado de los Recursos de Información					
Riesgos	Respaldos Externos	Alarmas	Capacitaciones	Equipo extra	Generador de energía eléctrica	Documentación de apoyo
Temblor	X					
Tormenta	X					
Incendio	X	X				
Inundación	X	X				
Robo	X	X				
Destrucción Voluntaria e Involuntaria	X		X			
Descompostura de equipo				X		
Personal clave			X			X
Fallas de energía					X	

Instalaciones de recuperación

No se cuentan con instalaciones de recuperación en esta ciudad, pero en este caso C.E.S.P.E. cuenta con una sucursal la cual puede ser utilizada como sede alternativa. Siempre y cuando se adquiera un servidor adecuado, se instale el software necesario y se bajen los respaldos.

Es una gran ventaja el tener esta sucursal, ya que si se llegara a presentar una contingencia en cualquiera de las dos sedes, se tendría acceso inmediato en la otra.

- ***Selección de estrategias***

Riesgos	Estrategias Propuestas	Estrategias Factibles
Temblor	Respaldos externos.	Respaldos externos.
Tormenta	Respaldos externos.	Respaldos externos.
Incendio	Respaldos externos, alarmas.	Respaldos externos, alarmas.
Inundación	Respaldos externos, alarmas.	Respaldos externos, alarmas.
Robo	Respaldos externos, alarmas.	Respaldos externos, alarmas.
Fallas de energía	Generador de energía eléctrica.	Generador de energía eléctrica.
Destrucción (voluntaria e involuntaria) de: Software, Hardware e Información	Respaldos externos, capacitaciones.	Respaldos externos, capacitaciones.
Descompostura de equipo	Equipo extra.	Equipo extra.
Personal clave	Capacitaciones, documentación de apoyo.	Capacitaciones, documentación de apoyo.

PLAN DE ACCIÓN

Estrategias seleccionadas	*Personal necesario*	*Apoyo externo*	*Recursos requeridos*	*Tiempo de implantación*	*Tareas a realizar*	*Monitoreo*
Respaldos externos	*Una persona*		*Cintas de respaldo*	*Inmediato*	*Respaldar diariamente*	*Revisión diaria*
Alarmas		*Necesario (para instalación)*	*Económicos*	*Inmediato*		*Revisión del mantenimiento por parte del proveedor*
Capacitaciones	*Depende del problema*	*Depende del problema*	*Económicos y/o personal adecuado para impartir las mismas*	*Inmediato*		*Realización de pruebas*
Equipo extra			*Económicos*	*En tiempo razonable*		
Generador de energía eléctrica			*Económicos*	*En tiempo razonable*		*Revisión del mantenimiento por parte del proveedor*
Documentación de apoyo	*Depende del problema*			*Inmediato*	*Elaborar documentación de apoyo*	*Revisión de la elaboración de la documentación de apoyo*

Implantación

A continuación se describen una serie de pasos a seguir, para la implantación de las estrategias seleccionadas:

- Respaldos Externos:
  - Determinar qué se va a respaldar (información, software).
  - Quién va a respaldar.
  - Quién va a monitorear que se realicen los respaldos.
  - Determinar la institución adecuada, en donde se van a guardar los respaldos.
  - Realizar el contrato.
- Alarmas:
  - Realizar cotizaciones de diversas alarmas.
  - Determinar las alarmas y el precio adecuado.
  - Realizar la adquisición de las alarmas.
- Equipo extra:
  - Determinar el equipo extra necesario.
  - Realizar cotizaciones del mismo.
  - Determinar los precios adecuados y adquirir el equipo.
- Generador de energía eléctrica:
  - Realizar cotizaciones de diversos generadores de energía eléctrica.
  - Determinar el generador de energía eléctrica y el precio adecuado.
  - Realizar su adquisición.

- Mantenimiento:

  - Realizar cotizaciones de diversas instituciones que presten el servicio.

  - Determinar la institución adecuada.

  - Realizar el contrato.

- Capacitaciones:

  - Determinar sobre qué es necesario capacitar.

  - A quiénes se va a capacitar.

  - Quiénes van a impartir las capacitaciones.

  - Cuánto tiempo van a durar las capacitaciones.

  - Quién va a monitorear que se lleven a cabo las capacitaciones, que sean las adecuadas y con resultados favorables.

- Documentación de apoyo:

  - Determinar sobre qué es necesario realizar documentación de apoyo.

  - Quiénes van a realizar la documentación.

  - Quién va a monitorear que se realice la documentación.

MANTENIMIENTO DEL PLAN DE CONTINGENCIAS

La persona responsable del mantenimiento del plan de contingencias es:

XOCHITL QUEZADA ACOSTA

6.2 Conclusiones generales.

La guía generalizada se presentó en C.E.S.P.E., con el fin de implantarse para probar su eficiencia y fue aceptada, ya que el encargado del departamento de informática mostró interés en esta investigación desde el momento en que contestó la encuesta, por estar consiente de la necesidad de contar con un plan de ésta índole implantado. Mientras avanzaba la implantación de la guía, se mostró interés en la investigación, por parte de los demás miembros del departamento de informática, lo cual es muy satisfactorio.

C.E.S.P.E. cuenta con vulnerabilidad sobre la protección a sus recursos de información. Algunas de las fallas detectadas no requieren de mucho esfuerzo ni trámite para solucionarse.

Los miembros del comité de contingencias, son competentes en su trabajo y están consientes de las fallas con las que cuentan, por lo tanto desarrollan proyectos a futuro, ya que los mismos solo pueden implantarse mediante la aprobación de los altos niveles.

Los proyectos que se desarrollan son para mejorar la eficiencia en el procesamiento de información, y para lograr esto, hay que actualizarse en el software y hardware, y todo este cambio trae consigo la gran ventaja y beneficio de minimizar el riesgo de presencias de contingencias.

CAPÍTULO VII

CONCLUSIONES

Como se ha podido apreciar por lo presentado anteriormente, es muy importante el uso de este tipo de planes y por lo tanto ha sido decepcionante el haber confirmado que muchas instituciones no tenían una idea clara y concisa de lo que es un plan de contingencias óptimo.

Todas las instituciones que cuentan con recursos de información deben y tienen que protegerse de la presencia de contingencias, esto es, minimizar el riesgo de vivir malas experiencias.

En base al estudio de campo realizado, se puede concluir que algunos de los profesionistas en cómputo, no tienen una idea clara de lo que es un plar de contingencias. Es importante mencionar que los profesionistas en cómputo son los responsables directos de promover el uso de este tipo de planes, pero por lo mencionado anteriormente no es común que lo hagan.

Se deduce con un gran porcentaje de seguridad la aceptación y necesidad de este trabajo, ya que todas las instituciones encuestadas, aceptaron tener fallas en sus medidas de protección a sus recursos de información, y también aceptaron la gran necesidad de contar con un plan de esta índole.

Se recomienda siempre que se realice una investigación, apoyarse en datos reales y actuales, para tener la seguridad de aceptación y veracidad en los resultados.

ANEXOS

Anexo 1:

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE CIENCIAS

Investigación para el Desarrollo de Tesis:

Metodología generalizada para implantar un plan de contingencias óptimo para redes de área local (LAN's)

Cuestionario para el Desarrollo de Tesis

La información solicitada en la siguiente encuesta, es con el fin de identificar las diversas medidas de seguridad que toman las instituciones de la localidad en cuestión, para proteger sus recursos de información (hardware, software, personal, información). La veracidad de los datos que usted proporcione serán críticos para el éxito de nuestra investigación.

DATOS GENERALES

1) Nombre de la institución:_____

2) Nombre del encuestado:_____

3) Puesto:_____

4) Tiempo en la institución:_____

5) Tiempo en el puesto:_____

6) Teléfono y/o Fax:_____

7) Giro de la institución:

a.() Banca b.() Manufactura c.() Educativa y Serv.

d.() Gobierno e.() Comercio f.() Otro:_____

8) Puestos desempeñados en el centro de cómputo:

a.() Director b.() Análisis c.() Diseño

d.() Programación e.() Administrador de la Red f.() Captura

g.() Auditor de Informática h.() Admor. de la Base de Datos

i.() Soporte Técnico

j.() Otro:_____

9) Número aproximado de usuarios del sistema de información:

_____

10) Protegen sus recursos de información con un plan de contingencia bien definido (estructurado):

Sí_____ No_____

11) Porqué:

_____

_____

_____

12) Cuáles son las precauciones que toman para evitar contingencias.

Ocasionadas por:

Riesgos externos:

Naturales: temblor, incendio, inundación, tormenta, otros.

Humanos: robo, sabotaje, fraude, otros.

Materiales: pérdida de información, fallas de energía, otros.

Riesgos internos:

Naturales: incendio, inundación, otros.

Humanos: robo, destrucción (voluntaria e involuntaria), sabotaje, huelgas, fraude, otros.

Materiales: descompostura de equipo, fallas de energía, otros.

13) Que tan frecuentemente revisan las precauciones tomadas para evitar contingencias :

_____

_____

_____

14) A pesar de las precauciones tomadas, se les han presentado contingencias (enumérelas):

1.-_____

2.-_____

3.-_____

4.-_____

5.-_____

15) Cómo las han solucionado:

1.-_____

2.-_____

3.-_____

4.-_____

5.-_____

16) Qué pérdidas les han causado:

a.() Tiempo b.() Dinero c.()Información

d.() Otros:_____

17) Qué tan importante es el contar con un plan de contingencias para su institución y/o usted:

_____

_____

_____

LITERATURA CITADA

1. Libros

(Andrea,91) Andrea, Rafael; Ricart, Joan E.; Valor, Josep. 1991. Estrategias y Sistemas de Información. McGraw-Hill.

(Babbie,88) Earl R. Babbie. 1988. Métodos de Investigación por Encuesta. FOTOEDISA. México, D.F.

(Fine,90) Fine Leonard H. 1990. Seguridad en Centros de Cómputo. Ed. Trillas. México, D.F.

(González,93) González Sainz Nestor. 1993. Comunicaciones y Redes de Procesamiento de Datos. De. Panamericana. Colombia.

(Heldman,94) Heldman Robert K. 1994. Information telecommunications : networks, products, and services. McGraw-Hill Inc. E.U.A.

(Hopper,89) Hopper;Temple;Williamson. 1989. Diseño de Redes Locales. Ed. Addison-Wesley Iberoamericana. Wilmington, Delaware, E.U.A.

(Mair,80) Mair, William C. 1980. Control y Auditoría del Computador.

(Murdick,93) Robert G. Murdick con John C. Munson. 1993. Sistemas de Información Administrativa. Segunda edición. Prentice-Hall Hispanoamericana, S.A. E.U.A.

(Murdick,94) Robert G. Murdick y Joel E. Ross. 1994. Sistemas de Información basados en Computadoras para la Administración Moderna. Editorial Diana, S.A. E.U.A.

(Pearty,82) Pearty F. Carlos E. 1982. Sistemas de Comunicación de Datos. Ed. Limusa, S.A. México, D.F.

(Perry,88) Perry, William E. 1988. Sistemas de Computación. Limusa.

(Scheaffer,87) Scheaffer Richard L.; Mendenhall William; Ott Lyman. 1987. Elementos de Muestreo. Grupo Editorial Iberoamérica, S.A. de C.V. México, D.F.

2. Diplomado

(Valerio,94) Valerio Ma. Angélica. 1994. Grupo Kernel, Módulo 9, Plan de Contingencias. Monterrey, Nuevo León, México.