UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

DESARROLLO DE UN PLAN DE SEGURIDAD EN CASO DE DESASTRE PARA UN CENTRO COMERCIAL

T E S I S

QUE PARA OBTENER EL TITULO DE

INGENIERO EN COMPUTACION

P R E S E N T A N

JOSEFINA ACEVEDO HERRERA

GEORGINA ACUÑA RIVERA

RUTH GAMEZ GUTIERREZ

MARIA ELENA RIVERA ORTEGA

DIRECTOR DE TESIS:

M.I. LAURO SANTIAGO CRUZ

MEXICO, D. F.

JULIO, 1995

No me importa, si para empezar de nuevo meter marcha atrás y retroceder, ni dar con la cabeza en el suelo siempre que pueda ponerme de pie.

J.M. SERRAT

Siempre he pensado que las estrellas conceden deseos, y es por eso que hoy quiero dar las gracias a Dios por la gracia de vivir, ya que este trabajo, es uno de los objetivos más significativos alcanzados en mi vida.

Con todo mi Amor dedico este trabajo principalmente, a las dos personas más importantes que siempre me acompañan dentro de mi corazón e inspiran todo lo que yo realizo, y a quienes debo gran parte de lo que hoy soy, mis padres:

Lidia Herrera Martínez
Rogelio Acevedo Vázquez

Pocas personas expresan siempre un amor y apoyo incondicional, y entre ellas he tenido la dicha de contar con mi familia, por lo que quiero dedicarla con el mismo amor a mis hermanos(as): **Guadalupe, Jorge Martín, Ana Laura, Rogelio, José Antonio, Carlitos Israel**, y de la misma forma a **mis Abuelitos y a mis tías.**

Si te acercas a alguien y permite que tú lo aprendas a amar puedes llamarlo tu amigo; es por eso que también quero dedicar este trabajo a todos mis amigos por su cariño y apoyo que me han brindado; y en especial a las siguientes personas:

Sandra Ruiz Barragán
Juan Antonio Caldera Trujillo
Jorge Luis Espinoza Filares
María Sara González Torres
Gloria Díaz Velasco
Ruth Martínez Ramírez
Octavio Farfán
Manuel Casanova

De igual forma quiero agradecer a mis amigas y compañeras de tesis: Georgina Acuña, María Elena Rivera, Ruth Gámez, toda su dedicación y paciencia para la elaboración de este trabajo.

Por último quiero dar las gracias a través del nombre del director de tesis ING. Lauro Santiago a la Universidad y a todas aquellas personas que me brindaron su apoyo en el transcurso de mi carrera, así como en la realización de la tesis.

Solo con el Corazón se puede ver bien, lo esencial es invisible a los ojos.

Josefina Acevedo Herrera.

Dedico esta tesis :

A tí madre, por ser una mujer tan maravillosa y bondadosa. Te agradezco tus enseñanzas porque sin ellas no sería lo que soy, gracias.

A tí padre, por tu manera tan especial de enseñarme a luchar para alcanzar lo qua quiero.

A mis hermanos: Raymundo, Francisco, Laura Guadalupe, Alejandro, Marcela, Gerardo y Ricardo, por su amor y apoyo que siempre he sentido.

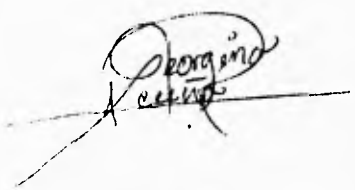
A mi tía Dolores, porque representa alguien especial en mi corazón.

A todos mis familiares, por que cerca y/o lejos he aprendido de ellos.

A mi novio Sergio, por ser el complemento de mi vida, que me ha enseñado lo que es el verdadero amor.

A todos mis maestros y amigos que me han enseñado tantas cosas a lo largo de mí vida.

A mí perra Fraika, por todo el cariño y ternura que me brinda.



Georgina Acuña Rivera

Agradezco primeramente a DIOS, por la vida que es tan hermosa. Porque no estamos solos y cada día que comienza es una nueva oportunidad para ser mejores.

Quiero agradecer a mis Padres y a mi abuelita, que con todo su amor me dieron su apoyo y comprensión, siempre estimulándome a seguir adelante en todas mis metas, no importando que tan grandes fueran los obstáculos para lograrlas.

A mis hermanos por su apoyo y entusiasmo que me mostraron en todo momento.

A mis amigos por su amistad sincera e incondicional, por sus palabras de aliento y su compañía, en los momentos difíciles.

También quiero agradecer a todas aquellas personas que intervinieron en mi formación, no sólo como profesionista sino como persona. Porque cada etapa de mi vida que ha pasado, tuve buenas y malas experiencias; palabras sinceras, de cariño y aliento; porque siempre hubo alguién en todo momento que me apoyaba, sobre todo en los momentos difíciles, ayudándome de cualquier forma para que yo siguiera adelante, llenándome siempre de valor para cambiar lo que puede cambiarse, teniendo la paciencia de aceptar lo que no se puede cambiar, y sobre todo, tener la sabiduría para distinguir lo uno de lo otro.

A todos esas personas que forman parte de mi vida y de mis recuerdos, sinceramente: gracias.

RUTH GAMEZ GUTIERREZ.

Caminante no hay camino,
se hace camino al andar.

Porque ha llegado el momento de obtener una de las cosas que más he soñado en la vida y porque esto es el reflejo de todo el entusiasmo que trato de poner a cada instante de mi vida.

Por lo cual dedico esta tesis :

A mis padres por haberme dado la vida, a mis hermanos Mary, Irma, Silvia y Toño por su amor y apoyo invaluable.

A mis maestros y amigos que conocí a lo largo de mi vida como estudiante, en especial a Gloria, Ana Luisa y Alicia por haber estado siempre en los momentos difíciles y felices de mi vida.

A Enrique por impulsarme a terminar mis estudios.

Pero en forma muy especial a mis amigas y compañeras de tesis Ruth, Georgina y Josefina por haberme soportado durante todo este tiempo.

MARIA ELENA

INDICE

Páginas

INTRODUCCION

El uso cada vez más extendido de los sistemas de cómputo en empresas e instituciones, ha simplificado las cargas de trabajo en las diversas áreas donde se aplican, por lo que los sistemas de archivos contienen información que es muy valiosa para su operación, en consecuencia, incrementa los riesgos de sufrir abusos en el manejo de las computadoras o bien desastres a causa de robo, fraude, sabotaje o interrupción en las actividades de cómputo. Tales riesgos organizacionales se deben en gran medida al aumento en la cantidad de aplicaciones, concentrado de información y el procesamiento que conlleva a incorporar sistemas más complejos, como las bases de datos y la dependencia de personas claves en los sistemas de cómputo. Por lo que, la protección de esta información debe ser un interés fundamental.

Algunos problemas que se deben tomar en cuenta para llevar un buen control sobre todos los procedimientos generales de la empresa y, por ende, de su información son:

1. La pérdida de información.

Que puede darse a causa de errores de hardware o de software debido a un mal funcionamiento de la unidad central de procesamiento, discos o cintas ilegibles; errores de telecomunicación; errores ocultos en los programas; errores humanos, a causa de captura incorrecta de datos, corrida deficiente del programa, discos o cintas extraviadas o bien por guerras, motines, huelgas, terremotos, etc.

2. Intrusos al sistema.

Esto se refiere a los usuarios internos o externos de la empresa, que violan los reglamentos de seguridad, al hacer mal uso de los sistemas para realizar modificaciones no autorizadas en los datos, leer archivos o ejecutar procesos a los que no tienen acceso.

3. Privacía en la información.

El objetivo debe ser proteger el buen uso de todos los equipos e información, aunque existen ciertos mecanismos de seguridad en los centros de cómputo, por lo general, sólo se dirigen los enfoques a las áreas de seguridad física y contra incendios, mientras el nivel real de seguridad sobre los equipos y de la información es muy bajo o superficial.

Es notorio que la mayoría de las compañías piensen que cuentan con planes adecuados de recuperación en caso de desastre, y que cubren todas las categorías para éste, sin embargo la realidad es que la mayor parte de esos planes son superficiales, no estructurados e inadecuados para afrontar las complicaciones que surgen en un desastre real; por lo tanto, la pérdida de poder de cómputo debido a fallas eléctricas, terremotos, incendios, inundaciones

o cualquier otra causa, puede amenazar la supervivencia de cualquier negocio. Ignorar estos riesgos puede ser muy peligroso.

Los desastres suceden y no estamos exentos de ellos. Sin una buena estrategia de recuperación, la empresa puede paralizarse por completo, por lo que contar con un Plan de Seguridad se puede confiar de que cuando ocurra un desastre, las aplicaciones criticas seguirán operando.

El motivo de este trabajo es presentar un plan de seguridad en la información en caso de desastre para un Centro Comercial. Su importancia se debe a diversos problemas que han ocurrido a lo largo del tiempo de diferentes empresas, al no tomar en cuenta aspectos de seguridad, ya que la gente se confía mucho y piensa que ciertos acontecimientos no les podrían ocurrir o que se toman medidas de seguridad una vez que ya pasó una catástrofe. Muchas veces no se quiere prevenir porque piensan que puede ser un gasto innecesario. Se debe dar la importancia y hacerle ver a los directivos para que se den cuenta de cuánto se puede perder por tomar o no, una acción sin valorar las consecuencias.

Por lo anterior, este trabajo tiene como objetivos, en primer lugar, presentar una metodología para realizar el plan de seguridad de una organización que cuente con el área de informática, en donde una organización es una agrupación de áreas, en las que se cuenta con el personal que lleva a cabo las actividades para realizar el negocio de la misma.

En segundo lugar, indicar la importancia de contar con el plan de seguridad de la información para dar continuidad al Centro Comercial en caso de que suceda algún desastre; y en tercer lugar, porqué es el departamento de informática el coordinador principal del plan de seguridad de la información.

En cuanto a la forma en que está organizado el presente trabajo de tesis tenemos:

En el primer capítulo se dan antecedentes en cuanto a las generalidades de pérdida de la información, así como la importancia de la seguridad en la misma.

En el segundo capítulo se definen las bases de un sistema integral de seguridad, cuya finalidad es garantizar la prevención y detección de un accidente de cualquier índole que sufra la información.

En el tercer capítulo se explican los requerimientos del Centro Comercial en general, como el factor humano, el factor organizacional, las instalaciones del Centro Comercial y el departamento de informática.

En el cuarto capítulo se presentan los dos tipos de encuestas realizadas una para los departamentos administrativos, identificando sus aplicaciones criticas, y la otra para el

departamento de informática, realizando un inventario de estándares y procesos, los cuales tienen asignados un número de trabajo ó proceso (job) que depende del nivel de riesgo.

En el quinto capítulo se desarrollan e implantan las ocho fases del plan de seguridad: clasificación de la información, identificación del personal, seguridad física, seguridad lógica y seguridad de comunicación, evaluación de riesgos, plan de contingencias y plan de recuperación.

En el sexto capítulo se evalúan los resultados de los simulacros de recuperación de información efectuados al Centro Comercial.

Finalmente se presentan la bibliografía y los anexos.

1. ANTECEDENTES

En el mundo de hoy, las organizaciones sofisticadas dependen del procesamiento de datos para el flujo de información esencial. Imaginemos qué pasaría si se prescindiera del procesamiento de datos durante dos días, una o dos semanas, las operaciones comerciales podrían limitarse de tal forma que afectarían los activos corporativos, los movimientos comerciales, el servicio a clientes, el flujo de dinero, las oportunidades de inversión y el margen de competencia. Toda la organización es vulnerable en caso de que las operaciones de cómputo no funcionen.

1.1. Generalidades de pérdida de información.

La información dentro de una empresa es de vital importancia para su operación, por lo que se debe prestar atención a las causas que puedan ocasionar la pérdida de la misma, esto da lugar a la siguiente clasificación:

- Causas naturales
- Causas circunstanciales
- Fallas de equipo

1.1.1. Causas naturales.

Estas causas se pueden dar por fenómenos naturales, tales como: sismos, huracanes, inundaciones, incendios, explosiones y derrumbes en las instalaciones, que pueden tener efectos de mayor intensidad y duración. Tales problemas pueden ser consecuencia de errores de diseño, de construcción o de fabricación, o bien si no se cuenta con medidas preventivas o hay exceso de confianza al no efectuar un mantenimiento constante.

1.1.2. Causas circunstanciales.

Dentro de este punto intervienen los daños intencionales y los no intencionales, los primeros son provocados por personal propio y/o ajeno a la empresa al efectuar acciones de sabotaje, espionaje o fraude; mientras que los segundos se presentan cuando existen errores de captura, reproceso equivocado de programas de producción, operación inadecuado del equipo, diseño deficiente de los sistemas de información, falta de preparación o de actualización del personal, ausencia de un sistema de prevención de fallas y resguardo o mantenimiento deficiente de los archivos.

1.1.3. Fallas de equipo

Estas causas se pueden generar tanto en Hardware como en Software, originándose de la siguiente forma:

Hardware

Este tipo de causas se presentan cuando cualquier equipo de cómputo ya sean mainframes, minicomputadoras, laptops, computadoras personales o incluso equipo para redes , ya sean de tipo LAN, vía satélite o vía microondas, sufren daños en sus discos internos y/o externos, unidades de cinta, unidades de respaldo, dispositivos periféricos, cableado y en cualquier tipo de tarjetas.

Software

Estas causas se pueden presentar por fallas en herramientas utilizadas para monitoreo de equipo, bases de datos, seguridad en el acceso, paquetería, lenguajes de programación, programas de aplicación e incluso en el sistema operativo.

1.2 Importancia de la seguridad en la información

La mayoría de las empresas en los últimos años han sufrido pérdidas de información, debido a que nunca le han dado importancia al desarrollo de un plan de contingencias, para no interrumpir su operación, tal es el caso de la empresa que trataremos a continuación:

Comencemos por señalar que **Nacional Financiera** es una institución enfocada al desarrollo del país, sirviendo de aval en préstamos extranjeros, a través de una participación mayoritaria o minoritaria en conjunto con diversas empresas de diferentes sectores. Debido a la gran cantidad de información que maneja, se tiene una dependencia básica del soporte de cómputo, ya que si ésta desapareciera se presentaría "una gran catástrofe Nacional". Esta institución tuvo su primera experiencia de desastre y pérdida de información en 1979, durante un incendio, cuando en los pisos 9 y 10 al tratar de apagar las llamas, el agua lanzada por los bomberos escurrió hasta el tercer piso, donde se encontraba el centro de cómputo, el cual se vio afectado por ésta al dañarse los equipos, las unidades de cintas, el procesador central y las líneas de comunicación.

Pero el problema no termina ahí, ya que el temblor de 1985 afectó nuevamente a la institución. La situación antes del sismo era la siguiente: su centro de cómputo estaba instalado en el tercer piso, y en el sótano se había acondicionado una bóveda en donde se guardaban los respaldos en cintas y cartuchos , además se estaba construyendo un centro de cómputo alterno en las oficinas de Alpina, con la finalidad de descentralizar su operación, pero debido a que estaba en obras negras, se contaba con pocas líneas de comunicación, por lo que parte de la operación de esta institución se apoyaba en una sucursal en Guadalajara. Cada sucursal contaba con dos equipos mainframe, uno para desarrollo y otro para producción, los equipos tenían un sistema de respaldo que interactuaba entre ellos, ya que si uno fallaba el otro podía entrar eventualmente en operación; a cada mainframe estaban conectadas en red 500 terminales aproximadamente, donde se contaba con un Master Control System (MSC), el cual mantenía la seguridad del usuario, ya que los sistemas en producción

tenían su propia seguridad integrada, además la red se combinaba vía telefónica y microondas para la emisión y recepción de datos. Debido a que el principio de esta institución era proporcionar un buen servicio, se ajustaba al lema " Nunca dejar de operar", por lo que de cierta manera se contaban con estrategias que pudieran funcionar como un plan de contingencias de operaciones diarias, con el objetivo de mantener sus actividades durante el día o la noche, por lo que existía una rotación de personal cada cuatro meses, con la finalidad de que cualquier persona de este grupo conociera los procedimientos a seguir en caso de falla. Después del temblor, el edificio quedó enterrado hasta su tercer nivel, destruyéndose parte del centro de cómputo; la información se vio afectada y, los únicos respaldos existentes eran de la noche anterior que estaban en la bóveda, y los que se mandaron a las oficinas de Alpina, dos días antes. Al enterarse de lo ocurrido, el personal del centro de cómputo acudió voluntariamente a colaborar en el rescate de documentos, cartuchos y cintas, las cuales fueron trasladadas a las oficinas de Alpina y con esta información se comenzó a operar el mismo día en sus instalaciones, quedando restablecido el sistema al día siguiente a las 7:00 hrs, para el D.F., y tres días después para toda la República Mexicana. Se controló de manera rápida el desastre, debido a que se contaba con las estrategias mencionadas. Además se había firmado un convenio con otras instituciones como BANAMEX y U.N.A.M. previendo la necesidad de hacer uso de equipo e instalaciones externas, en caso de que se presentara una situación similar.

Aunque se tenía como proyecto un plan de contingencias, nunca se pensó que realmente se llegaría a utilizar, y de hecho como tal nunca se aplicó. Lo anterior demuestra que un plan de seguridad no es una inversión a largo plazo, es una inversión redituable día a día ya que una simple interrupción del sistema y pérdida de información, pueden ser el factor decisivo en la vida de una empresa, sin que se tengan que esperar a que ocurran grandes desastres.

2. BASES DE UN SISTEMA INTEGRAL DE SEGURIDAD

La seguridad efectiva de un centro de cómputo para garantizar la prevención, detección de un accidente o ataque de cualquier índole, se debe basar en medidas bien definidas, que le permitan afrontar cualquier interrupción con la finalidad de restablecerlo, por lo que tiene gran importancia establecer sistemas de seguridad para la información, en los cuales se muestren los factores necesarios de todas las áreas funcionales para lograr un ambiente seguro e integro de trabajo, que ayude al fortalecimiento de la estructura organizacional de la empresa y defina una relación costo/beneficio razonable.

Lo anterior da lugar al surgimiento de un nuevo concepto de seguridad manejado actualmente que es el de "seguridad total", el cual se constituye de los siguientes elementos:

2.1. Elementos Administrativos.

Los elementos administrativos son aquellos que definen las políticas de seguridad hacia el personal y el centro de cómputo, a través de una organización y división de responsabilidades, con el objetivo de disminuir el incremento en los riesgos que cada día se generan debido a la cantidad de aplicaciones que se tienen, por la gran concentración de información y procesamiento de datos. Por lo que la cuantificación de riesgos para establecer la seguridad buscada, implica clasificar a las instalaciones de acuerdo a su nivel de riesgo, que puede ser alto, medio o bajo.

Las instalaciones de alto riesgo son aquellas que manejan datos o programas que contienen información confidencial, de interés nacional o para mantener un nivel competitivo dentro de su mercado de acción, generando como consecuencia una pérdida financiera considerable si se presentara algún desastre; mientras que las instalaciones de riesgo medio son aquellas cuya interrupción prolongada causa grandes inconvenientes y posiblemente el incremento de los costos, pero sin embargo se obtiene poca pérdida de material.

Contrariamente a las anteriores, en las instituciones de bajo riesgo el procesamiento retardado tiene poco impacto material, en términos de costo o de reposición del servicio interrumpido.

Después de clasificar las instalaciones en términos de riesgo, se procederá a definir una estrategia global que se debe seguir para afrontar los niveles de riesgo señalados. Dentro de esta estrategia se deben incluir las aplicaciones, programas, archivos específicos, planes de detección y métodos para prevenir desastres, agregando detalladamente las prioridades o acciones que se requieran a corto, mediano o largo plazo, por lo que la responsabilidad de la seguridad total en éstas se debe dividir en dos áreas: una que trate todos los asuntos de riesgo comercial y otra que sólo involucre asuntos técnicos del centro de cómputo, manteniendo la coordinación en ambas áreas para garantizar un intercambio productivo entre las funciones comerciales y técnicas, para asignar responsabilidades de participación en la determinación de una política de seguridad y hacer el seguimiento de los logros alcanzados.

2.1.1. Definición de una política de seguridad.

Para desarrollar un plan de seguridad completo, se debe tomar en cuenta la organización del equipo de planeación, identificación de actividades críticas, la forma en que deben de realizarse las pruebas, simulacros de recuperación y revisiones para que éste funcione y se mantenga al día con las necesidades de la Empresa. Se pueden mencionar varios modelos a seguir para el desarrollo de un plan de seguridad.

Leonard H. Fine, nos menciona en su libro Seguridad en Centros de Cómputo, que los objetivos a seguir son:

1. Planear en forma anticipada, las necesidades en la recuperación de aplicaciones críticas, asegurando la continuidad en la operación de la Empresa.
2. Contar con una estrategia que permita reactivar la operación del procesamiento de datos, en caso de siniestros o por cualquier tipo de interrupción, minimizando la desorganización y pérdida de información, a un nivel que sea observado por la Empresa.
3. Tener una metodología a seguir para dar continuidad al procesamiento de los datos más importantes, determinando las áreas involucradas.
4. Fijar el valor crítico del proceso.

Por otro lado, Kenneth N. Myers, considera tres etapas .

- **Primera Etapa**

Comprende la revisión de las prácticas operacionales de información gerencial y de procesamiento requerido con las organizaciones de procedimientos de datos y de usuarios claves.

Sus objetivos son el desarrollar un conocimiento de las funciones de los usuarios y dependencia en el procesamiento computarizado, evaluar inicialmente el impacto y el riesgo de situaciones críticas de desastre, e identificar operaciones de procesamiento de datos internas.

- **Segunda Etapa**

En ésta se desarrolla una estrategia interna de procesamiento de datos, en la cual es muy importante contar con el apoyo gerencial, ya que el error más peligroso es tener un plan de seguridad en caso de desastre que sólo exista en papel. La metodología para su realización consiste en la participación del personal, donde ésta proporcionará la información acerca del procesamiento de datos de la empresa, identificando los niveles mínimos en los que la

empresa puede operar, así como al personal responsable de la toma de decisiones ante alguna emergencia.

- **Tercera Etapa**

Se elabora la documentación de las normas de procedimiento, a partir de la metodología desarrollada en la segunda etapa que cubran los siguientes períodos de tiempo:

- operaciones normales,
- respuesta de emergencia,
- procesamiento y
- restauración.

En el desarrollo de estas normas de procedimiento se asignan responsabilidades a cada una de las diferentes áreas, con la finalidad de realizar auditorías e identificar las responsabilidades individuales.

Por otro lado, Michael Dobbertein, en un artículo para Computer Decisions, menciona que uno de los factores más importantes de la seguridad consiste en realizar simulacros, incluso en las empresas donde los auditores exigen revisión periódica de los planes para situaciones de emergencia, debido a que pocas veces se observa algún simulacro para comprobar la validez de dichos planes, él establece dos normas de tipo general:

1. Hacer el simulacro en partes, comprobando la validez sistema por sistema, y evitando abarcar todas las aplicaciones a la vez.
2. Aprovechar lo que el simulacro pueda enseñar, ya que, sea cual sea el resultado del mismo, permite determinar el grado de validez y de utilidad del plan en situaciones de emergencia.

Si bien muchos especialistas consideran que los simulacros son indispensables, se oponen a las pruebas sorpresivas por el hecho de que ponen en peligro los datos "reales". Sin embargo, al menos desde un punto de vista teórico, entre más imprevista sea una prueba, más efectiva resultará ésta. Quizá lo mejor consista en realizar varios simulacros y en comprobar la validez de los planes para situaciones de emergencia en diversas ocasiones antes de pensar en un simulacro sorpresa.

2.1.2. Organización y división de responsabilidades.

Los sistemas de control interno de una organización constituyen un elemento importante para la seguridad en computación. Los factores principales de este elemento son la división de responsabilidades y los sistemas de verificación interna, ya que estos permiten lograr la revisión y obtener un balance sobre la calidad del trabajo, a través de restricciones firmes,

tanto físicas como de procedimiento. Los elementos clave de este criterio lo constituyen las siguientes funciones:

- Desarrollo de los sistemas
- Programación
- Mantenimiento de programas
- Apoyo en el uso de los programas
- Preparación de los datos
- Operaciones centrales y remotas
- Control
- Preservación de los archivos

Los dos elementos clave que sirven de base para las divisiones subsecuentes de responsabilidad, son las funciones de control y de archivo; resulta conveniente que estas funciones sean autónomas y se adscriban a la autoridad más alta que se pueda, de preferencia al gerente del departamento de procesamiento de datos. En algunas instalaciones, la función de control es reducida y se limita sólo a los controles del procesamiento, en otras, tiene un alcance amplio y abarca las funciones de archivo, la responsabilidad del seguimiento de otras funciones como la documentación de los sistemas, la programación y las operaciones, los puntos de enlace clave de diferentes funciones y el mantenimiento de los sistemas existentes. El grado de división entre las diferentes funciones depende del nivel de seguridad que la instalación requiera. La consideración prioritaria es la independencia de la función de control y el manejo de esta actividad por parte del personal preparado para afrontar las exigencias que se le harán.

La división de responsabilidades y los sistemas de verificación interna se combinan para formar el sistema de control de una institución. Estos sistemas se pueden definir como, aquellos que prueban la realización de recolección de datos en forma completa, precisa y que además se trabaja de acuerdo con las divisiones de responsabilidades y de jerarquía establecida a medida que desciende la jerarquía, las responsabilidades son más operativas y detalladas.

Un elemento que es esencial para la seguridad en computación, consiste en garantizar que todo el personal clave tenga una sustitución adecuada, por lo cual se debe poner especial atención al evaluar la importancia del personal relacionado con la programación de las aplicaciones o de los sistemas de carácter avanzado y los niveles de gasto, así como también del presupuesto destinado para este fin.

2.1.3. Seguridad física y contra catástrofes.

Al evaluar la seguridad física y contra catástrofes de las instalaciones, se debe tomar en cuenta de manera especial la seguridad del Centro de cómputo. Las áreas clave que se deben verificar son:

- **Ubicación y construcción del centro de cómputo**

El área del Centro de cómputo debe estar en un edificio o habitación que no esté situada encima, debajo o adyacente a un área donde se procesen, fabriquen o almacenen materiales inflamables o explosivos. Deberá contar con puertas de emergencia y las paredes deben ser de material incombustible. Si el centro de cómputo tiene una o más paredes exteriores, adyacentes a un edificio que sea susceptible de incendio, se deben construir ventanas irrompibles para mejorar la seguridad del personal y del equipo contra los robos, agua y residuos materiales.

Se recomienda que el techo falso y sus canalizaciones sean de material resistente al fuego y al polvo; al igual el piso falso deberá ser del mismo material, instalándose sobre el piso real. Además de las consideraciones anteriores, el techo del centro de cómputo y el área de almacenamiento de cintas, discos y dispositivos de respaldo deben ser impermeables, debiéndose prever un sistema de drenaje en el piso firme.

El área de recepción y distribución de datos es considerada la de más alto riesgo y la más susceptible de sufrir ataques externos, por lo tanto, debe estar aislada, hasta donde sea posible. Por lo general, este requisito interfiere con la eficiencia del flujo de trabajo pero es indispensable en las instalaciones de alta seguridad.

- **Ubicación del sistema de aire acondicionado**

Para evaluar la capacidad del aire acondicionado se deberá tomar en cuenta: la disipación térmica de las máquinas, cargas latentes, aire de renovación, pérdidas por puertas y ventanas, infiltración en paredes, techos, suelos y disipación de otros aparatos.

Las cargas caloríficas del equipo de cómputo y sus periféricos serán proporcionadas en BTU/hora o en Kcal/hora. Se propone que el aire acondicionado deberá ser independiente, esto es, no debe formar parte del aire acondicionado del edificio, su distribución en el centro de cómputo es importante, ya que los componentes de las máquinas se refrigeran normalmente mediante la circulación rápida de aire por medio de ventiladores, al igual se debe tomar en cuenta su ubicación dependiendo de la forma en que se distribuya, que puede ser por techo (tratándose de menores volúmenes de aire) y por piso falso con controles de temperatura.

- **Suministro de energía**

El suministro de energía para el aire acondicionado y del equipo de cómputo es importante, especialmente cuando se cuenta con procesamiento en línea o de tiempo real; se debe contar con un respaldo(planta de energía) para afrontar una falla eléctrica, así como también con reguladores de voltaje, para soportar posibles variaciones de éste, que podrían dañar los datos almacenados, los programas o el equipo.

- **Riesgo de inundación**

Los riesgos de inundación se tienen cuando las computadoras se colocan en sótanos o en las áreas de planta baja, por lo cual se debe evitar instalarlas cerca de cañerías o donde el riesgo de inundación sea evidente.

- **Acceso físico**

Se debe considerar el control de acceso a la empresa, durante todo el día y la noche, incluyendo descansos y cambios de turno mediante dispositivos electrónicos como: alarmas contra robos y tarjetas de acceso para el personal.

- **Incendios**

Se deben contar con detectores de humo, de vapor y calor, que se deben instalar en el centro de cómputo junto a las áreas de oficinas, cerca del perímetro físico de las instalaciones; así como también, en los pisos falsos y en los ductos del aire acondicionado, ubicando los extinguidores apropiados en lugares de acceso inmediato. Por otro lado, es necesario definir los procedimiento en caso de incendios y entrenar al personal para su uso. En caso de incendio se deberá indicar a los bomberos los procedimientos a seguir para el centro de cómputo.

Otro aspecto importante y que, generalmente se descuidada, es la limpieza y mantenimiento de las instalaciones del centro de cómputo.

2.1.4. Prácticas de seguridad en el personal.

La mayoría de las instituciones han tomado conciencia de la creciente dependencia en la integridad, estabilidad y lealtad del personal, ya que una contratación inapropiada puede poner en riesgo su seguridad, por lo que es importante contar con políticas como las siguientes:

- Verificación de referencias y antecedentes de una manera detallada y profunda de acuerdo al puesto solicitado.
- Realizar pruebas psicológicas para evaluar habilidades, actitudes, valores sociales, opiniones políticas y estabilidad general.
- Efectuar exámenes médicos, que permitan evaluar no sólo el estado físico de un individuo, sino también las actitudes y la estabilidad potencial del recién contratado.

En particular, se debe analizar la habilidad para laborar en situaciones de estrés, especialmente cuando éste es parte de las exigencias del puesto.

Al mismo tiempo, se deben tener procedimientos para la evaluación del desempeño, que pueden servir también para establecer las actitudes hacia el trabajo y los sentimientos generales hacia la institución, al igual, para asegurar que el personal expuesto al estrés por el trabajo excesivo, descanse periódicamente de manera apropiada.

2.1.5. Pólizas de Seguros.

Las áreas de riesgo que se deben asegurar comprenden: el medio donde se encuentra la empresa y la instalación de cómputo, tomándose en cuenta el equipo, los programas, los datos, la interrupción de la actividad comercial y el personal. Entre los riesgos a cubrir se tienen los siguientes:

- Riesgos ambientales. Provienen tanto de fuentes externas como de problemas dentro de la instalación del centro de cómputo. Estos surgen de fuentes cercanas a cualquier instalación de cómputo, por ejemplo: fábricas de explosivos, de material o procesos inflamables, atmósferas tóxicas (con gas, polvo o abrasivos), riesgos de inundación, incendios, terremotos, daño por impacto, disturbios y tumultos civiles, entre otras.

- Riesgos internos: Surgen del mal funcionamiento de los servicios de los cuales depende la computadora, como fuentes de energía, equipos de aire acondicionado y de calefacción, detectores de calor o humo, extinguidores y el sistema de drenaje. Existen otros riesgos, como los errores del sistema o de los procedimientos de seguridad.

Las pólizas de seguro para el equipo abarcan la totalidad de la instalación de cómputo, es decir, edificio, mobiliario, planta de aire acondicionado, equipo auxiliar, fuentes de energía, cintas, papelería y la computadora en sí. Esta última incluye todo tipo de equipo de procesamiento centralizado, sistemas, terminales y redes.

En muchas instalaciones existe equipo tanto comprado como rentado; el rentado debe considerarse en forma separada, ya que el contrato con el arrendador por lo general establece previsiones específicas. En muchos casos, el vendedor posee su propio contrato de seguros y no se requiere duplicación, sin embargo, en general esta cobertura no incluye los daños causados por la negligencia del personal, donde se instala el equipo y se requiere especificación al respecto. Es importante que en todos los casos estos recursos se aseguren por el valor de su reposición y no de su costo.

Dentro de las pólizas de seguros se incluyen sistemas operativos, programas de utilización u otras aplicaciones de software que provee el fabricante de la computadora, los programas de aplicación que se obtienen de terceros, programas que se han desarrollado en la institución, así como también elementos tales como los archivos maestros y de transacciones; por lo tanto, los registros (programa y datos) de los sistemas de cómputo se

deben asegurar: contra la pérdida o el daño causado al medio, según el costo de reposición de la información registrada en ellos.

La determinación del valor para asegurar se puede calcular en base al costo de producción del equipo, los costos de reproducción del programa y el valor comercial del mismo, por lo que cualquier daño trae como consecuencia una reducción de su valor.

La función de las pólizas por daños materiales consiste en restituir el valor por medio de la provisión de fondos para su reparación o reposición. Tal daño también puede dar lugar a la incapacidad para realizar ciertas operaciones, lo que puede significar pérdidas financieras en el negocio. Estos riesgos se deben cubrir por medio de una póliza de interrupción comercial o pérdida de ganancias, a fin de proporcionar la compensación financiera por pérdidas o incrementos de costos del trabajo.

Los daños causados se relacionan con los departamentos de la empresa, como el equipo auxiliar y los sistemas de comunicación. La evaluación de sus consecuencias debe abarcar: los costos que permanecen constantes, aunque el negocio funcione a un nivel reducido de actividad; los costos adicionales de trabajo para minimizar los efectos de la pérdida en los ingresos, la depreciación del valor de los artículos perecederos, las multas por la entrega retardada, la interrupción en los sistemas de control, que puede causar un desequilibrio en la producción o en los niveles de inventario; la incapacidad de cobrar o recolectar las deudas importantes, las demoras en la aplicación de los nuevos sistemas, lo que podría retardar la producción de nuevas mercancías o servicios y la desorganización administrativa general con repercusión en las áreas de comercio de la empresa.

Por lo que se debe identificar cada riesgo material, revisando los planes de contingencia y determinando el nivel requerido de riesgo asegurable.

Dentro de los riesgos que puede sufrir el personal existen varios tipos: eléctricos o mecánicos, que pueden provenir de los dispositivos de protección como extinguidores de bióxido de carbono y por trabajo de tipo excepcional, entre otros.

Finalmente, se puede mencionar que los objetivos ha cumplir por parte de estas pólizas son:

- Identificar y cuantificar los riesgos directos y consecuentes de la instalación de cómputo en la empresa.
- Garantizar que la cobertura se revise para tomar nota de los incrementos en los costos o en los precios de reposición.
- Garantizar la existencia de los planes de contingencia adecuados, en especial cuando no se puede obtener la cobertura del seguro.
- Asegurar que la pérdida consecuente se excluya de las responsabilidades de la institución hacia terceras personas.

- Obtener asesoría y orientación especializadas cuando se requiera.

2.2. Elementos técnicos y procedimientos.

Conforme fue creciendo la demanda del uso de equipo de cómputo, empezaron a surgir las necesidades que consistían en guardar estos datos de una manera confidencial y en cantidades de un tamaño considerable, para lo cual fue necesario comenzar a establecer niveles de seguridad y protección de información.

2.2.1. Seguridad de los sistemas.

Es importante hacer mención que el hecho de hablar de seguridad informática se refiere al equipo, los programas, las redes, las líneas y sistemas de comunicación de datos, las terminales y los programas generales directamente asociados. Cada uno de estos aspectos se presentan ahora por separado:

- **Programas**

La seguridad de la información es el cumplimiento de las actividades y mantenimiento de las condiciones en que se maneja la información que garantiza la seguridad, respaldo y confidencialidad de la misma. A través de la identificación de los elementos que intervienen en el proceso automatizado, estableciendo controles de acceso, medidas detectivas y de vigilancia. La seguridad de la programación pretende restringir el acceso para garantizar que los operadores puedan trabajar utilizando los archivos, datos y programas autorizados, evitando cualquier modificación a estos.

- **Equipo**

La seguridad de los equipos consiste principalmente en dispositivos externos que se ajustan a las computadoras de una forma opcional y que evitan el acceso a la información en una manera directa. La mayoría de las computadoras tienen una gran variedad de controles automáticos para asegurar su operación apropiada y por último, existen malos manejos en la operación del equipo que crean riesgos. Estos se deben definir e incluir en un manual práctico de operaciones para el personal. Hasta donde sea posible, estas prácticas se deben vigilar en todo el equipo por medio de pruebas.

- **Redes**

La seguridad en comunicaciones se enfoca a proteger la información transmitida a través de redes de comunicación, mediante el control de acceso y criptografía en los enlaces, para lo cual requiere medidas de autentificación de usuarios y recursos. El almacenamiento y el análisis de información ha sido uno de los grandes problemas a los que se ha enfrentado el

hombre, pero las tendencias actuales se dirigen hacia la conectividad de datos. No sólo en la transferencia de información de una computadora a otra sino, sobre todo, en la distribución del procesamiento a lo largo de grandes redes.

- **Terminales**

En la actualidad, muchas terminales equivalen por sí solas a poderosas computadoras que utilizan programas muy complicados. Por ello al revisar la seguridad de las terminales éstas se deben tratar como pequeñas computadoras.

La parte esencial en la seguridad de la terminal es el uso indebido que se le pueda dar a ésta; entre los aspectos a revisar tenemos, la ubicación, el acceso físico, el control sobre la operación a través de claves y códigos u otro método de identificación. Para disminuir este problema hay que realizar verificaciones físicas e informes acerca del uso de la terminal y de la vigilancia sobre los intentos de acceso no autorizado, efectuar un cambio sorpresa de los códigos del usuario, así como pruebas sorpresa para auditoría y prácticas de operación.

- **Seguimiento del desempeño**

El seguimiento del desempeño del computador central, las redes y las terminales es una función administrativa y de seguridad importante. Se deben considerar cuidadosamente los recursos disponibles de los programas existentes o sus modificaciones. Además, se requiere seguimiento en informes de todo intento de acceso indebido a los programas o archivos.

2.2.2. Seguridad de las aplicaciones.

El alcance de la seguridad de los datos y los archivos de una aplicación incluye tanto el trabajo de la computadora como otras labores. Se necesita considerar en forma cuidadosa la relación de las actividades de cómputo con las que no lo son. Por parte de la computadora comprende datos, programas y archivos que se procesan en el sistema. Los elementos que no son de la computadora incluyen recolección y entrega de datos e información así como su control para garantizar que se procese en forma correcta.

- **Controles del usuario**

El usuario tiene la responsabilidad primaria de asegurar que los datos recolectados para el procesamiento estén completos y sean precisos; también se debe asegurar de que todos los datos se procesen y se incluyan en los informes que le regresan. En el análisis final de los resultados, no es aceptable culpar a la computadora por las decisiones que se basen en datos imprecisos, ya que las responsabilidades de los usuarios no se pueden delegar al departamento de informática.

- **Controles de procesamiento de la computadora y seguridad de los archivos**

El control que se mantiene en el centro de cómputo es, en general, con respecto a los archivos y programas.

Los controles que se mantienen dentro del departamento de cómputo son de procedimiento y aritméticos. Los de procedimiento incluyen división de la responsabilidad entre captura de datos, operaciones y archivos, seguimiento de evidencias en la transferencia de registros y datos entre las diferentes funciones, control sobre la precisión y distribución de los resultados. Los controles aritméticos son los que garantizan el proceso completo y preciso de todos los registros de datos durante y al final del procesamiento.

Un elemento importante en el control del procesamiento es mantener la seguridad de los archivos, la cual abarca el almacenamiento secundario (cintas, cartuchos, discos magnéticos) en un lugar distante del centro de cómputo, tales como: cintotecas y bóvedas para su resguardo, considerando medidas de seguridad para su transportación.

Otro aspecto ha considerar es la precisión de los archivos con los estándares de la instalación que se deben incorporar en los programas, controles detallados de principio a fin y conteos de registros. Se debe de integrar el balance detallado registro por registro y/o los conteos binarios. La verificación e igualación de estos conteos aritméticos se deben comparar con los controles manuales de cada proceso, por otra parte los operadores de cómputo deben tener acceso físico restringido a los archivos de cintas, el cual debe de estar bajo control de otras personas, quienes, de preferencia, se encuentren adscritas a alguien que no realice funciones de operación. Se deben poner los datos y los archivos a la disposición de quien los necesite para cada proceso de producción, aunque esto resulte difícil de realizar.

2.2.3. Estándares para programación y operación de sistemas.

Los estándares de sistemas, programación y operación, así como la documentación, tienen efectos de suma importancia en la seguridad en computación. Existen dos razones para revisar los estándares como parte de la seguridad de computación, como son la necesidad de poner atención en la seguridad durante todas las etapas preliminares y subsiguientes, del análisis y del diseño, la exigencia de arreglos de respaldo adecuados, como la duplicación de los sistemas, programación y documentación de operaciones.

- **Sistemas y estándares de programación**

La seguridad se debe considerar en dos niveles, para la instalación como un todo y para las aplicaciones específicas. Las primeras requieren una planificación a largo plazo para garantizar que se tome en cuenta la seguridad en la realización de las aplicaciones progresivas, los puntos claves que se deben considerar son el impacto de la seguridad en computación sobre la estrategia del equipo y los programas, la seguridad de las terminales

respecto a los controles de la aplicación, los requisitos físicos , el respaldo, la ubicación, y la estrategia de redes, los estándares de control de la aplicación, en especial los de reinicio y de respaldo, los estándares de los datos y del diseño de archivos y la función de las auditorías.

Por otro lado, las segundas tienen un significado a corto plazo, donde los elementos principales que se deben revisar son: la seguridad de los equipos, los programas, controles de aplicación, supervisión, métodos de trabajo y documentación.

- **Operaciones**

Así como la documentación de los sistemas y de los programas, la instalación de los mismos puede estar expuesta a un riesgo considerable, debido a la ausencia de estándares adecuados para las actividades de operación. Estos estándares deben incluir prácticas de mantenimiento, evitar la mala operación del equipo, de los programas y los procedimientos para el uso de las copias de seguridad.

2.2.4. Funciones de los auditores tanto internos como externos.

Las funciones de auditoría tanto externa como interna cumplen un papel importante en la seguridad en computación. La primera se refiere de manera fundamental a estatus legales. Por lo general la legislación clave es la relativa a la operación de las empresas o su equivalente; mientras que la segunda no tiene responsabilidades legales, el alcance de sus actividades varía de una institución a otra, ya que algunas veces, desempeña funciones de alto nivel, que consisten en informar sobre la efectividad de los sistemas y procedimientos, con la finalidad de reportarlos.

Las actividades del auditor interno abarcan por lo general la participación activa en el proceso de desarrollo, al garantizar la incorporación de las medidas adecuadas de seguridad y auditoría, colaborando también con las revisiones de los puntos de verificación del proceso; la revisión de sistemas y controles de la aplicación, tanto en los departamentos de usuarios como en los centros de procesamiento computacional; la revisión de la política y los procedimientos de seguridad en computación y participación activa en las pruebas contra desastres, por último la introducción de técnicas avanzadas para la auditoría de los sistemas computacionales complejos. Para lograr una contribución efectiva de la función de auditoría a la seguridad computacional se deben considerar ciertos aspectos importantes:

- El alcance de la auditoría interna en la seguridad computacional.
- Una relación entre los auditores externos y los internos.
- El papel interno en la sociedad.
- El papel de la auditoría interna en los sistemas en operación.
- La instrucción y capacitación para la auditoría interna y efectiva.

Durante mucho tiempo se ha reconocido la necesidad de contar con la participación extensa de la auditoría interna en los sistemas y seguridad computacionales. En la práctica, muy pocas instituciones han logrado éxito. Probablemente el obstáculo mayor en este sentido es el logro de un compromiso real de la gerencia de línea, el personal de cómputo y los auditores para aplicar los procedimientos.

2.2.5. Planes y simulacros para la recuperación en caso de desastre.

La prueba real de la efectividad de la seguridad es la respuesta que se produce en el caso de un desastre real. La respuesta efectiva sólo puede proceder de los planes efectivos contra estos, así como también del personal bien adiestrado.

Por lo tanto, la buena planeación contra desastres debe abarcar:

- Las aplicaciones en proceso de desarrollo.
- Las aplicaciones terminadas.
- Los procedimientos para los distintos tipos de desastre.

Tipos de desastres

Al considerar los planes y los simulacros de desastre, se necesita delinear cuidadosamente, primero, los distintos tipos que pueden ocurrir:

1. Destrucción completa o parcial de los recursos centralizados y descentralizados (equipo de cómputo y periféricos) utilizados en el procesamiento de datos.
2. Destrucción o mal funcionamiento de los recursos ambientales (aire acondicionado, planta de emergencia) destinados al procesamiento centralizado de datos.
3. Destrucción total o parcial de los procesos manuales del usuario, utilizados para la captura de la información de entrada de los sistemas de cómputo, por ejemplo sus archivos de facturas, recibos o voucher o la pérdida de las aplicaciones de captura.
4. Pérdida del personal de cómputo clave.
5. Interrupción por huelga.

Los procedimientos de planeación contra desastres tiene que considerar cuidadosamente los tipos de desastre expuestos anteriormente. Para cada suceso se requiere efectuar planes específicos. En cada caso se necesita, además, considerar la posible causa del desastre, por ejemplo, un accidente o un ataque deliberado. Esta información será útil para la aplicación de los procedimientos de recuperación necesarios.

Planeación contra desastres

La planeación contra desastres debe abarcar tanto las aplicaciones en procesos de desarrollo como las operativas.

En el caso de las últimas, existen ciertas áreas que necesitan protección o ciertos recursos que deben estar disponibles para la recuperación:

1. Documentación de los sistemas, la programación y las operaciones.
2. Recursos de procesamiento que incluyen:
   - Todo tipo de equipo.
   - Ambiente para el equipo.
   - Datos y archivos.
   - Programas.
   - Papelería.

Los procedimientos de planificación contra desastres tendrán que definir en forma detallada, un plan de trabajo para la iniciación y la aplicación paso por paso de los procedimientos de recuperación. A continuación se describen con mayor detalle estos aspectos.

Aplicaciones en proceso de desarrollo

El análisis mal estructurado puede dar como resultado el incremento de los costos respecto al personal de sistemas, la pérdida de programas y para el tiempo de prueba del equipo, el costo de las aplicaciones crecen en forma acelerada. Puede ocurrir un desastre en alguna fase avanzada y será necesario tomar medidas para garantizar que no se pierda la inversión. Además, otra pérdida potencial para la empresa, es la demora en las operaciones comerciales de la aplicación de servicios de cómputo o de información.

En términos teóricos, un desastre se puede presentar en cualquier etapa del desarrollo de una aplicación. No obstante, según la Ley de Murphy, el desastre tiende a suceder cuando la aplicación está casi terminada pero la documentación no está completa.

En cada punto de verificación o pausa del proyecto, es importante que se lleve a cabo una revisión cuidadosa a fin de asegurar que existe una adecuada protección contra desastres. Aunque pudiera parecer exagerado, los beneficios pueden ser significativos en el caso de que suceda un accidente. De esta manera, las consideraciones sobre seguridad y desastres se deben incorporar como asuntos estándar en la verificación al final de cada fase del trabajo.

Cuando se cuente con una excelente planeación contra desastres, es aconsejable tener en mente que siempre se incurrirá en algunos gastos en caso de que suceda alguno. La verificación de las pérdidas siempre es un proceso laborioso y éste se agudiza con la

ausencia de los datos de costo del proyecto, los cuales también deben estar almacenados en un lugar seguro.

Aplicaciones terminadas

Dentro de la aplicaciones terminadas podemos señalar:

1. Sistemas y programación

Las operaciones se encuentran en cambio constante todo el tiempo y, en muchos casos, la documentación no se modifica para reflejar lo que realmente sucede en la práctica. Por lo tanto, los planes contra desastre no sólo deben considerar la existencia de la documentación sino también, las consecuencias que puede traer ésta.

2. Operaciones de procesamiento

Las operaciones de procesamiento comprenden el sistema completo, desde el momento que se presta el servicio solicitado o se produce el informe. En consecuencia, la planeación contra desastres debe incluir las actividades y los procedimientos del usuario; si el caso lo amerita los recursos de transmisión y redes, el procesamiento centralizado y la redistribución de los resultados a los puntos de usuarios. Esta planeación se debe considerar en cada uno de estos puntos como una entidad separada y como un todo, cubriendo lo que se utiliza en cada etapa del proceso, por ejemplo:

- Equipo de terminales o de entrada de datos.
- Equipo de procesamiento.
- Equipo ambiental, es decir, aire acondicionado, energía, etc.
- Recursos de distribución y arreglos incluyendo red y terminales.

Cada aplicación se debe revisar con mucho cuidado y también se deben realizar los arreglos necesarios para datos y archivos. Un aspecto que con frecuencia se descuida consiste en que muchas veces existe una cantidad considerable de datos para transacciones. Debido a que la recaptura de estos puede requerir mucho tiempo, es importante guardarlos en forma legible en el computador. Por lo cual se requiere que cada aplicación cuente con los procedimientos por escrito. En ellos, se deben diferenciar claramente los diversos tipos de desastres expuestos. Los procedimientos deben especificar con claridad:

- Las responsabilidades en caso de desastre y la organización que entra en vigencia.
- La acción inmediata que se debe seguir.
- Los planes contra desastres deben ser lo más detallados que sea posible. Las personas tienden a olvidar que cuando sucede éste no hay tiempo para pensar en qué se hará. Es posible anticiparse a la mayoría de situaciones y éstas deben estar cubiertas en el plan contra desastre.
- Todo el personal requiere adiestramiento regular en el plan contra desastres. Muchas veces se pasa por alto el hecho de que en muchas instituciones de procesamiento de datos, el número de empleados es alto.

- La aplicación de las prácticas convenientes para aumentar la seguridad se debe hacer como rutina, por ejemplo, cerrar las cajas de seguridad para datos en medios magnéticos después de que los archivos se hayan recuperado.

Los planes y documentación contra desastres, los debe conocer un grupo pequeño del personal, pero suficientemente grande como para garantizar la diversificación. La información excesiva acerca de los planes contra desastres también constituye una amenaza para la seguridad.

Simulacros de desastres

Aunque muchas empresas cuentan con planes contra desastres, muy pocas han intentado las pruebas de simulacros de esos planes. Los simulacros de desastres son importantes por las siguientes razones:

- Se prueban la conciencia y preparación del personal para afrontarlo.
- Se identifican las omisiones en los planes.
- El elemento sorpresa de los simulacros constituye una buena verificación moral para garantizar que se encuentren vigentes, en forma rutinaria, buenas prácticas de seguridad.

Son muchas las razones aludidas para no probar los planes para situaciones de emergencia, pero, en el fondo, los factores más importantes a considerar para la realización o no de simulacros son el tiempo y el dinero.

Frecuencia de los simulacros de desastre

Los simulacros se deben realizar de manera esporádica. Así como la contabilidad de caja y las circulares que se envían a los deudores se inician en forma sorpresiva, los simulacros no se deben anunciar. La planeación de estos requiere que una o dos personas sepan de su realización y guarden el secreto, de otra forma el elemento sorpresa se pierde.

Además se necesita de la experiencia y se sugiere que se realicen en un momento relativamente conveniente. No obstante, los desastres reales rara vez ocurren en estos momentos, por lo que después de una o dos pruebas, se debe realizar el simulacro durante un momento de gran inconveniencia, por ejemplo cuando hay exceso de trabajo. Esta situación no será grata, pero probará con gran realismo los procedimientos de recuperación.

A pesar de que el realismo es importante, es necesario reconocer que existe un riesgo en los simulacros. A menos que se establezcan planes muy cuidadosos, existe la posibilidad de que se cause daño. Si no se instruye a los empleados para que sigan los procedimientos establecidos.

3. INVESTIGACION DE LA SITUACION ACTUAL DEL CENTRO COMERCIAL

3.1. Antecedentes.

El Centro Comercial se creó en el año de 1982. En la actualidad éste ha tenido un crecimiento bastante acelerado, tanto a nivel de sucursales como de sistemas y de tecnología. Actualmente dicho centro cuenta con una oficina central y 29 sucursales.

La oficina central está integrada por 350 empleados distribuidos en los siguientes departamentos:

- Recursos Humanos
- Mercaderías
- Compras
- Finanzas y Contabilidad
- Informática

En el departamento de Informática se encuentra el centro de cómputo, dicho centro cuenta con el siguiente equipo:

- 4 minicomputadoras HP-3000 modelos 992, 980, 967 y 932
- Una red de comunicaciones vía satélite (VSAT) , que utiliza el protocolo de transmisión X.25.
- Un servidor para la red LAN.

Dentro de cada sucursal se cuenta con el siguiente equipo de cómputo:

AREA	EQUIPO
Gerencia	1 PC
Oficina Administrativa	1 PC, *MASTER
Personal	1 PC
Recibo	1 PC
Pedido de mercancía	1 PC

*MASTER : Controlador maestro de las cajas registradoras.

Actualmente el éxito de cualquier empresa depende en gran medida de su departamento de Informática, ya que por una interrupción prolongada de los servicios de cómputo puede ocasionar pérdidas de información considerables y en consecuencia, perder un lugar de competitividad en el mercado.

3.2. Organización.

En la figura 3.1 se presenta el organigrama del Centro Comercial.

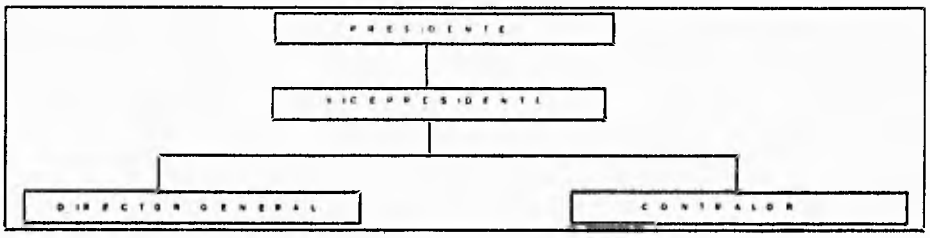


Figura 3.1. Organigrama del Centro Comercial

Como se puede observar en el organigrama existen un presidente, un vicepresidente, un director general y un contralor. Las funciones de cada uno de estos son:

Presidente: Junto con algunos socios es el dueño de la empresa. Estos toman decisiones que tendrán impacto para la vida de la empresa.

Vicepresidente: Toma las decisiones con respecto al buen funcionamiento de la empresa.

Director General: Encargado del funcionamiento de las Oficinas Centrales.

Contralor: Encargado de todas las tiendas departamentales.

Además del organigrama general existen organigramas por división:

La Dirección General está integrada por la Gerencia administrativa, la cual a su vez está dividida en los departamentos de Finanzas y Contabilidad, Recursos Humanos, Informática, Mercaderías y Compras. Figura 3.2.

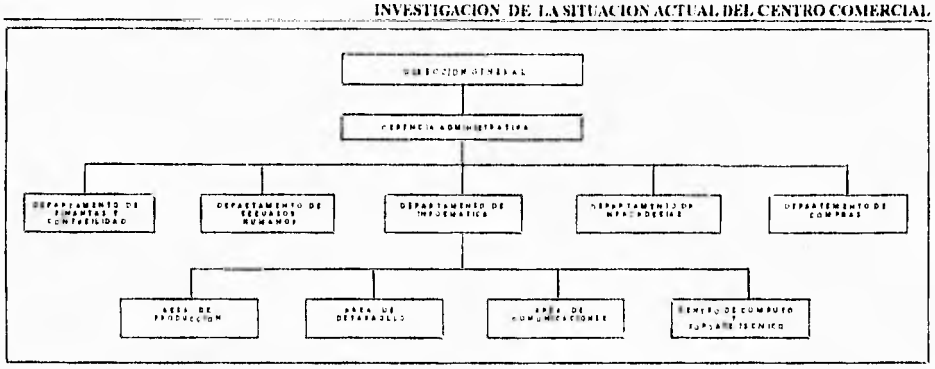


Figura 3.2. Organigrama por división.

Gerencia Administrativa: Se encarga de coordinar las actividades de los departamentos de Finanzas y Contabilidad, Recursos Humanos, Informática, Mercaderías y Compras. A continuación se dará una breve explicación de las actividades efectuadas en cada uno de ellos:

- **Departamento de Finanzas y Contabilidad**

Para muchos las funciones financieras y contables dentro de un negocio es casi la misma, no obstante lo anterior y aunque existe una relación estrecha entre éstas, cada una de ellas tiene una función bien especifica. La función contable se preocupa de registrar con exactitud los eventos o transacciones, de acuerdo con las reglas contables que se estén utilizando, y manteniendo el registro del estado de los recursos físicos y financieros, mientras que la función financiera se ocupa de la solvencia del Centro Comercial, obteniendo los flujos de caja necesarios para satisfacer las obligaciones y adquirir los activos fijos y circulantes necesarios para lograr los objetivos de éste.

- **Departamento de Recursos Humanos**

Este departamento controla el presupuesto para la capacitación, reclutamiento y selección de personal, así como todo lo relacionado con la nómina, tanto de las sucursales como oficinas generales del Centro Comercial.

- **Departamento de Informática**

Es la responsable de coordinar las actividades realizadas en las áreas de producción, desarrollo, comunicaciones, y centro de cómputo y soporte técnico. (Ver figura 3.2.).

A continuación se dará una breve explicación de las actividades realizadas en cada una de las áreas:

Producción

Se encarga de correr todos los procesos que se requieran en fechas y horarios establecidos, así como de generar todos los reportes que se necesiten para todas las áreas del Centro Comercial, además tiene la obligación de revisar que cada proceso que se ejecute esté documentado por el área de desarrollo, para darle seguimiento.

Desarrollo

Se encarga del análisis, diseño, desarrollo, implantación y mantenimiento de los sistemas, por otro lado, indica los estándares a utilizar por cada uno de los sistemas desarrollados y, documenta en forma clara y concisa todos ellos.

Comunicaciones

Tiene como finalidad el transferir e intercambiar información entre equipos de punto de venta, teléfonos, computadoras y terminales "tontas", entre otros. Por otro lado, debe controlar el tráfico de información a ciertas horas del día, ya que la transferencia de archivos de las diferentes sucursales hacia el computador central, se realiza durante la mañana y la tarde.

Centro de Cómputo y Soporte Técnico

Existe una relación estrecha entre estas dos áreas, pero cada una tiene objetivos específicos, el administrador del centro de cómputo es el que se encarga del buen funcionamiento y coordinación de los equipos existentes, esto es, lleva todo el control del centro de cómputo. Esta área conoce de manera global la operación completa del Centro Comercial, ya que sabe qué procesos batch (jobs) se corren diariamente, horarios de ejecución y los reportes generados, etc. Su responsabilidad principal es mantener la integridad y consistencia de toda la información.

El área de Soporte Técnico se encarga de la evaluación e instalación del software en los equipos del centro de cómputo, así como de la capacitación del mismo, de la administración de las bases de datos, de la asignación de claves para accesar a los sistemas y de evaluar las estrategias de respaldo o recuperación.

- **Departamento de Mercaderías**

En compañías que manejan un gran número de productos, las ventas son muy importantes, por lo que la función primordial de este departamento es proporcionar información útil del desplazamiento que tengan los productos, actualizando directa o indirectamente la información de ventas, inventario, compras, finanzas y contabilidad.

- **Departamento de Compras**

Este departamento tiene relación directa con el proveedor, el cual negocia cantidades y precios sobre los mismos, además los fija sobre la demanda del producto, dependiendo de: la zona comercial, la reacción de la competencia, el costo del producto, así como también los descuentos, concesiones, tasas de interés y fletes.

En general, debe anticipar las demandas cambiantes con relación a los productos, aumentar la productividad en las ventas y mantener un control estrecho sobre los gastos de ventas y distribución.

Contralor (Sucursales). En la figura 3.3 se presenta el organigrama de Sucursales, representadas por el contralor. La función del contralor, es tener productividad efectiva en cada una de las 21 sucursales a su cargo, divididas en 7 distritos, dependiendo de su ubicación por zona.

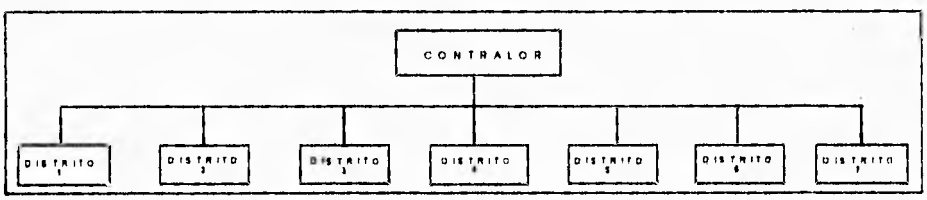


Figura 3.3 Organigrama por División (Sucursales)

Cada distrito está compuesto por 3 sucursales, cada sucursal cuenta con una organización, en la cual existe un gerente, un subgerente de operaciones, un subgerente de mercaderías, un encargado de personal, auditoría y jefes de departamento. Las funciones que desempeñan son las siguientes:

Gerente: Es el encargado de controlar y vigilar la buena administración de la sucursal.

Subgerente de Operaciones: Es el responsable de controlar todos los procedimientos que se llevan a cabo en la sucursal, además de llevar a cabo la planeación y realización de los inventarios.

Subgerente de mercaderías: Es el responsable de que todos los sistemas instalados por el departamento de informática en la sucursal funcionen correctamente y también verifica que la información que se envía a las oficinas generales sea la correcta.

Subgerente de personal: Se encarga de llevar el control y capacitación del personal, donde incluye la nómina que envía a las oficinas generales para que sea integrada en la nómina general del Centro Comercial.

Auditor Interno: Es el que realiza la auditoría dentro de la Sucursal con el objetivo de mejorar la integridad y confiabilidad de la información.

Jefes de departamento: Se encargan de mantener funcionando de manera eficiente cada departamento que conforma a la sucursal.

3.3. Información Operativa.

Para una mejor comprensión de como opera la empresa, resulta evidente que se debe tener un conocimiento básico de las funciones principales de todos los departamentos que constituyen al Centro Comercial, por lo que es necesario explicar en forma detallada los procesos de trabajo así como el flujo y procesamiento de la información.

3.3.1. Gerencia Administrativa.

La Gerencia Administrativa se encarga de coordinar, asesorar y analizar toda la información que proporcionan los departamentos de finanzas y contabilidad, mediante todos sus movimientos registrados en las aplicaciones desarrolladas por el departamento de informática, para establecer el nivel de competencia y solvencia económica.

El funcionamiento de esta gerencia tiene una relación directa con los principales ejecutivos de las siguientes instituciones y personas:

a) Bancos y compañías de fianzas
b) Asesores en previsión de riesgos (seguros)
c) Sindicato
d) Clientes
e) Proveedores nacionales

Por esto, requiere información actualizada y confiable, para que sus operaciones sean oportunas y pueda prever problemas futuros de cualquier índole. En base a esta información también evalúa las autorizaciones de tipo financiero y controla movimientos que podrían

repercutir en el funcionamiento del Centro Comercial, estas funciones se engloban de la siguiente manera:

- Control de seguros de todos los activos de la compañía, como son: vehículos, planta e instalaciones, asi como seguros que cubran robo con violencia e incendios y seguros de vida para el personal.
- Revisión y autorización para pago de facturas de compra, notas de gastos, tiempo extra y préstamos al personal.
- Control y pago de la nómina de compensación mensual.
- Atención a inspectores y notificadores de dependencias oficiales.
- Revisión del reporte semanal del flujo de caja.

3.3.2. Departamento de Finanzas y Contabilidad

La función de finanzas se encuentra en uno de los niveles más altos de la estructura organizacional de la empresa, ya que las decisiones financieras óptimas son absolutamente indispensables para su sobrevivencia y éxito. Tales aspectos comportan la adición de nuevas líneas de productos o la reducción de las antiguas, expandir o añadir plantas, cambiar su ubicación y retener las utilidades u obtener capital externo para dar apoyo a la expansión. Estas decisiones tienen un efecto a largo plazo sobre la rentabilidad de la empresa.

La responsabilidad de finanzas se relaciona con aquellas decisiones que tengan que ver con las inversiones que la empresa hace y la manera en que financia los proyectos.

Las funciones especificas son efectuadas por dos funcionarios: el tesorero y el contralor. El tesorero se encarga de la adquisición y de la custodia de los fondos, incluyendo la administración del fondo corporativo para pensiones. Mantiene relaciones con los bancos comerciales y con los accionistas, prepara informes sobre la posición diaria del efectivo de la empresa, efectúa de la formulación de los presupuestos de efectivo y la administración del crédito de los seguros y fondos de pensión.

Las áreas de responsabilidad del contralor incluyen el establecimiento y el mantenimiento del catálogo de cuentas, la preparación de reportes internos y extemos, y el control presupuestal. La función central del contralor incluye el registro y la preparación de presupuestos y de los estados financieros, para los cuales requiere información que ya fue capturada previamente por los departamentos responsables de la nómina, los impuestos y la auditoría interna. Las actividades de finanzas son correlativas con la de los departamentos de carácter administrativo y productivo, como se muestra en la figura 3.4.

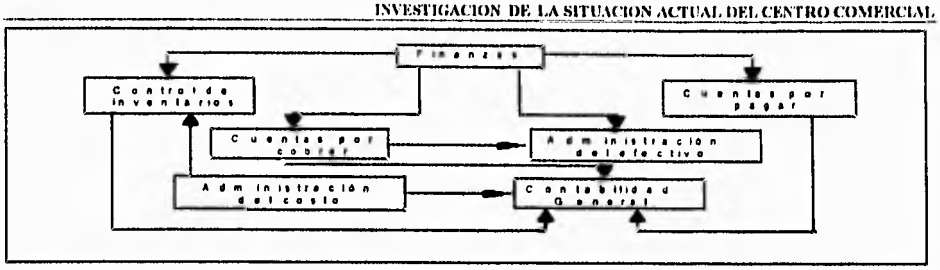


Figura 3.4 *Se observa el flujo de información que proporciona el departamento de Finanzas y como se relaciona con los diferentes departamentos de carácter productivo (Control de inventarios y de costo) y de carácter administrativo (todo lo relacionado con el activo circulante).*

Para el análisis de los antecedentes financieros del Centro Comercial, de su posición actual y de su probable trayectoria futura, es necesario relacionar los puntos fuertes y débiles que existen en la empresa, los puntos fuertes deben ser entendidos si han de ser usados para obtener una ventaja adecuada, y los puntos débiles deben ser reconocidos si se ha de tomar una acción correctiva. Dentro del departamento de finanzas se emplean datos cuantitativos provenientes del balance general y del estado de resultados.

Contabilidad se encarga de registrar las operaciones de carácter financiero, estas operaciones se basan en la información capturada y procesada, en las aplicaciones desarrolladas por el departamento de informática. Cuando hay un nuevo concepto contable (impuesto o prestación), que sea agregado a la aplicación, se le pide al departamento de informática que lo modifique o desarrolle. En la siguiente figura se muestran los sistemas de información que dan apoyo a la función de contabilidad.

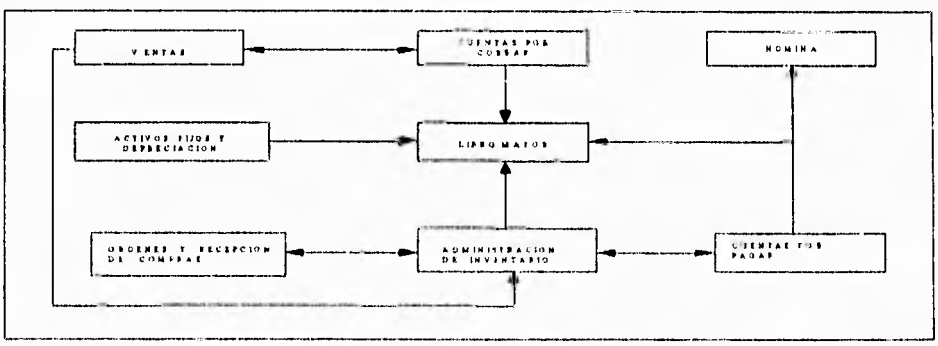


Figura 3.5 *Se muestra un esquema de la información que es soporte para función del Departamento de Contabilidad, aquí toda la información se refleja en el Libro Mayor.*

Las actividades que desarrolladas por Contabilidad son:

- Se supervisan las operaciones diarias que realiza la empresa, como la facturación diaria, el control de las compras de materias primas y materiales para fabricación.
- Se revisan y autorizan todas las declaraciones y envíos que se presentan ante las dependencias oficiales.
- Cada mes se revisan y se analizan las cifras de los estados financieros que se presenta a la Dirección General.
- Se coordina con el Contador General, la elaboración de todo tipo de trabajos especiales, como son: arqueos de caja, revisión de cartera, solicitudes de devolución de productos.
- Se depuran las cuentas de: proveedores, acreedores diversos, deudores diversos, para la Integración de los costos.
- Se elaboran las formas de pago de impuestos: Infonavit, pago del uso o goce temporal de inmuebles, por la prestación de servicios personales independientes, apoyándose en la consulta de los auxiliares contables(cuentas, proveedores, departamento de ventas, por mencionar algunos).
- Se elabora la cédula para el pago de IVA, checando las cuentas de productos diversos, productos financieros, ventas de activo fijo, rebajas sobre ventas y devoluciones sobre ventas.
- Se efectúa la recopilación de inventarios cada mes:
  a) Productos terminados.
  b) Materia prima (para panadería, tortillería)
  c) Productos en Proceso
  d) Materiales varios (mantenimiento y papelería).
- Se hace una recopilación de precios y cálculos para determinar el gran total de cada inventario.
- Se verifican todos los movimientos contables (mayor auxiliar), para hacer las aplicaciones, correspondientes de cada cuenta.
- Se codifican los cortes de caja y se investigan ciertos movimientos para proceder a contabilizarse(póliza de ingresos) y se genera el reporte de cobranzas(diario).
- Se codifican las pólizas de egresos, y los documentos que vienen anexados a la póliza de reposición de caja chica.
- Se verifican manualmente las operaciones bancarias.
- Se verifica la codificación y elaboración de las notas de entrada de productos para fabricación y de materia prima.
- Se verifica la póliza de ventas.
- Se analiza el corte previo, mensualmente para la elaboración de los estados financieros.
- Se hacen las pólizas de gastos por amortizar, así como también las provisiones de intereses de los préstamos.
- Cuando todos los movimientos estén codificados o contabilizados en su totalidad, son capturados en los sistemas contables para generar sus diversos reportes.
- Se actualizan los papeles de trabajo para la determinación del componente inflacionario y conciliaciones bancarias.
- Se determinan los Saldos promedios mensuales de las siguientes cuentas:
  1. Clientes
  2. Documentos por cobrar
  3. Cuentas en trámite judicial
  4. Anticipo a proveedores
  5. Deudores diversos

- Se determinan los intereses y comisiones cobradas del mes.
- Se determinan los saldos promedios mensuales de las deudas (Cuentas):
  a) Proveedores
  b) Préstamos
  c) Determinación de los intereses pagados.
- Se hace el ajuste a las pólizas de la provisión de impuestos y servicios.
- Se determina el impuesto a pagar I.S.R., Infonavit, I.S.P.T. y honorarios, calculados en base a:
  1) Sueldos
  2) Vacaciones pagadas
  3) Prima vacacional
  4) Prima de antigüedad
  5) Honorarios
- Se revisa la validación de cartera contra:
  a) Pólizas de diario
  b) Pólizas de egresos
  c) Pólizas de ingresos
  d) Reporte de clientes de crédito y cobranza
- Se verifica el Mayor Auxiliar y relaciones cada mes:
  1) La cuenta de materia prima recibida
  2) La cuenta de funcionarios y empleados
  3) El concepto de la cuenta de reparación de equipo
- Se archiva:
  a) Situaciones bancarias
  b) Correspondencia
  c) Notas de crédito y cargo
  d) Retenciones de honorarios
  e) Control del minutario.

En este departamento también se determina las normas, políticas, procedimientos y bases de aplicación obligatoria para el ejercicio presupuestal. Para la elaboración del presupuesto por sucursal, se consideran los siguientes factores:

1. Ingresos.
2. Costos de ventas o producción de mercancía.
3. Gastos controlables e incontrolables.

La base para el cálculo presupuestal es el cálculo de ventas, el cual determinará el costo de la venta o de la producción de sus propios productos y los gastos controlables. Su operación comprende :

1) Iniciación del análisis presupuestal. Prepara los formatos para el ejercicio presupuestal por cada sucursal.
2) Cálculo presupuestal a nivel sucursal.
   a) El área de presupuestos recibe los formatos para su análisis.
   b) Realizan su presupuesto considerando los ingresos y el costo de venta de mercancía, considerando al volumen total de ventas.

c) La sucursal matriz calculará el presupuesto considerando también el número total de unidades que se producirán probablemente el próximo año, el costo de la mano de obra directa y la materia prima utilizada por unidad. Así como los gastos por publicidad.
d) Cada sucursal debe elaborar su presupuesto tomando en cuenta, el número de personal de ventas, viajes, entrenamientos, así como aquellos gastos inherentes a la operación como, seguros, depreciaciones, gastos de oficina, correo, teléfono, impuesto sobre la nómina.

Una vez que cada área ha revisado, analizado y determinado sus necesidades, realizan su presupuesto considerando el gasto administrativo al mes corriente, proyectado a diciembre. Esta área también realiza las siguientes actividades:

- Revisa y captura la información recibida.
- Evalúa cifras y justificaciones presupuestales.
- Se consulta telefónicamente a cada sucursal para aclarar dudas, omisiones y/o desviaciones.
- Se realiza la integración y consolidación presupuestal a nivel Centro Comercial.
- Finalmente se aprueba o rechaza, mandando a cada área de la aprobación o rechazo de su ejercicio presupuestal.

3.3.3. Departamento de Recursos Humanos

El departamento de recursos humanos se maneja a través de un sistema de cómputo, el cual interactúa con los departamentos de informática y finanzas; este departamento está dividido en dos áreas relacionadas entre sí, que son la de personal y la de nómina.

Los diferentes departamento existentes en la empresa realizan las requisiciones de personal a través del área de personal, la cual se encarga de entregar las solicitudes a los posibles candidatos para su asignación dentro de la plantilla de puestos y plazas, también lleva el control de las reasignaciones de las mismas, ya que considera los índices de rotación de puestos, por motivos de promoción, bajas, antigüedad, y otras políticas que establezca el Centro Comercial; para ello se realizan pruebas y test psicológicos que determinan si el empleado cumple con el perfil solicitado.

- A través del sistema de cómputo se puede registrar la trayectoria laboral, así como la información personal del empleado, también efectúa el mantenimiento del tabulador del personal, que consiste en registrar la puntuación obtenida por el desempeño del empleado, para establecer rangos de salarios dentro de la misma; al mismo tiempo realiza presupuestos para la capacitación y seguridad física de los empleados, generando una plantilla de presupuesto a través del sistema, que se pasa al departamento de finanzas y contabilidad, esto se maneja a nivel corporativo o por departamento. Esta área tiene control de los porcentajes de pagos y gastos de los servicios médicos por empleado.

El área de nómina captura los datos generales del empleado, referentes a su sueldo actual, así como el histórico de su salario integrado, esto se hace para todos los departamentos del Centro Comercial. También, ejecuta un proceso que realiza el cálculo de la nómina quincenal, que considera período vacacional, faltas, adeudos del empleado, los estados de cuenta y de los pagos fuera de nómina que se puedan realizar. Efectúa las percepciones y deducciones de los empleados, así como, los totales de la nómina calculada, emitiendo recibos o cheque de pago de la misma, así como reportes de desglose de efectivo, al igual realiza el cálculo de la póliza contable para todos los movimientos registrados dentro del periodo de nómina.

En el área de nómina se manejan también procesos mensuales, anuales y especiales. Los procesos mensuales corresponden a las declaraciones del IMSS, SAR, INFONAVIT, fondo de ahorro, vales de despensa, vales para uniformes del empleado, impuestos estatales variables o por porcentaje y mantenimiento a instrumentos/bancos de la compañía. Los procesos anuales incluyen la declaración del impuesto sobre el producto del trabajo (ISPT), el cálculo del aguinaldo, reparto de utilidades (PTU) y la actualización a los días de trabajo. Los procesos especiales se definen como aquellos que se efectúan en cualquier tiempo, tal como la generación, mantenimiento y cálculo de los finiquitos, la actualización y emisión de tarjetas de reloj, así como en determinado momento el aumento masivo de sueldo dentro de la compañía, para una determinada área.

3.3.4. Departamento de Informática

Como se vio anteriormente, informática se divide en cuatro áreas: Centro de cómputo y Soporte Técnico, Desarrollo, Producción y Comunicaciones. Cada una de éstas se involucra de manera directa o indirectamente con los demás departamentos.

El área de desarrollo recibe las requisiciones justificadas de nuevas aplicaciones o sistemas solicitados por los diferentes departamentos del Centro Comercial, para que posteriormente se efectúe el análisis, diseño, desarrollo, implantación y pruebas de las mismas.

Si el resultado de las pruebas realizadas a las aplicaciones satisfacen las necesidades del usuario, éstas se liberan en el área de producción, la cual se responsabiliza de que los datos capturados para la aplicación estén completos y sean precisos, llevando un registro de control, en él que se incluyen los siguientes puntos:

- Número de proceso (job)
- Si genera reportes
- Tipo de papel a utilizar
- Firma de usuario

En caso de que algún proceso falle o que se interrumpa se reportará de inmediato al área de desarrollo, con la persona encargada de dicho proceso, la cual revisará a detalle hasta localizar el problema. Estas fallas se pueden presentar por varias causas:

- La información no está completa, tiene algún carácter especial o secuencia de escape.
- Por una inadecuada interface de comunicación entre las sucursales y oficinas generales y, por lo tanto, no se pudo integrar la información de éstas en el computador central.
- Se presentaron fallas eléctricas o de algún equipo.

Para evitar estas posibles causas, se debe llevar un control estricto de cada una de ellas.

El área de comunicaciones ha diseñado una red satelital para el mejor control en las transferencias de datos entre las sucursales y oficinas. Si estas transferencias no han sido realizadas debido a fallas en la red, el área debe resolver de inmediato el problema. Si éste no se soluciona, puede causar fallas en los procesos diarios dentro de las áreas importantes de las sucursales, las cuales son:

- Recibo
- Oficina Administrativa
- Transferencia Electrónica de Datos (TEF)

Recibo: Transfiere archivos, teniendo estos como datos las entradas de mercancía para la sucursal, esta información se debe integrar diariamente al computador central de oficinas generales, y se corren procesos para generar los pagos a proveedores.

Oficina Administrativa: Envía las ventas diarias, que también se deben integrar diariamente, generando estadísticas de desplazamiento por artículo/sucursal, de gran utilidad para el área de compras.

TEF: Es una aplicación interactiva, donde se solicita el crédito en línea mediante el conmutador que tiene conectado varios puertos a las Instituciones de crédito, las cuales autorizan o rechazan el crédito solicitado.

Como se puede observar el área de Centro de cómputo y Soporte Técnico tienen una gran responsabilidad, ya que es la encargada de administrar los equipos, e interfaces que intervienen en todo el proceso de comunicaciones, en caso que se presentara una falla o algún desperfecto, se deberá restablecer lo más pronto posible, debido a que la operación de la empresa depende, en gran parte, de las aplicaciones que en estos reside, por lo que no se puede permitir una interrupción prolongada.

3.3.5. Departamento de Mercaderías.

La función principal de este departamento es realizar reportes estadísticos del desplazamiento del producto, llevando un registro histórico del análisis de ventas, el cual proporciona una visión sobre las ventas por producto o artículo, así como su margen de utilidad y cantidad vendida, también mantiene un flujo constante de información con los departamentos de informática, compras, finanzas y contabilidad, contando con un sistema automatizado, el cual le permite tener un control estricto de su información. Ver figura 3.6.

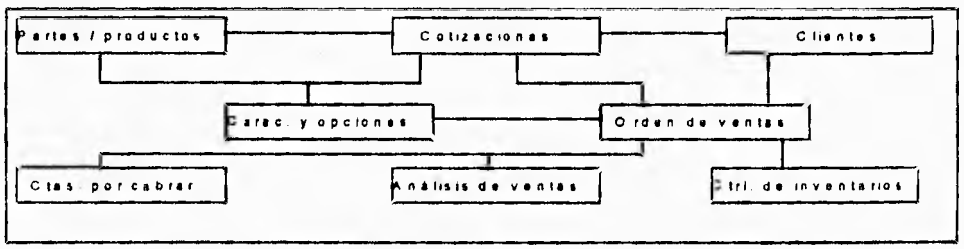


Figura 3.6 Control de información del departamento de mercaderías

Todas las sucursales del Centro Comercial cuentan con un Master, el cual controla las cajas registradoras, almacenando toda la información de las ventas diarias y las transfiere vía red a la minicomputadora HP-3000/992, que se encuentra en oficinas generales. Con estas ventas se realizan las estadísticas por artículo, información que es útil para el departamento de compras.

Por otro lado, el área de recibo cuenta con un sistema de captura para las entradas de mercancía, las cuales son transferidas al host central (HP-3000/992) y así, el departamento de mercaderías, con esta información, puede generar el pago a proveedores.

3.3.6. Departamento de Compras.

El objetivo de este departamento es lograr una operación de mercadeo eficiente del Centro Comercial. Por esto siempre está en busca de los mejores procedimientos de compras para su permanencia en el mercado y su continuo crecimiento.

El departamento de Compras mantiene un flujo constante de información con el departamento de mercaderías, informática, finanzas y contabilidad. Este cuenta con un sistema automatizado, desarrollado por el departamento de informática, el cual le permite tener un control en el manejo de su información. Este sistema está instalado en una PC conectada a una HP-3000. Además recibe requisiciones para validar y/o aclarar dudas de

acuerdo a lo solicitado por cada sucursal, y posteriormente verificar su existencia, y enviar las autorizadas al área de administración de inventarios.

Para la adquisición de nuevos productos o artículos, éste se encarga de costear, autorizar y evaluar la mejor opción, la cual consiste en contactar al proveedor que ofrezca el mejor precio y buena calidad, una vez seleccionado se genera la orden de compra enviando una copia al almacén, el cual se encarga de recibir los productos solicitados y de verificar su buen estado. Una vez que el almacén le comunica que el producto fue recibido, compras procede a generar el registro de pasivos por la recepción de orden de compra, que son anticipos a cuentas de gastos, pagos normales (recibidos, comprobantes, notas), los cuales son utilizados por el departamento de finanzas y contabilidad.

3.4. Recursos y materiales técnicos.

Dentro de este punto sólo se hará referencia al edificio donde se ubican las oficinas generales, así como su distribución interna, rutas de evacuación y salidas de emergencia, instalaciones y cableados del equipo de cómputo y comunicaciones.

3.4.1 Instalaciones.

El edificio de oficinas generales consta de sótano, planta baja y primer piso.

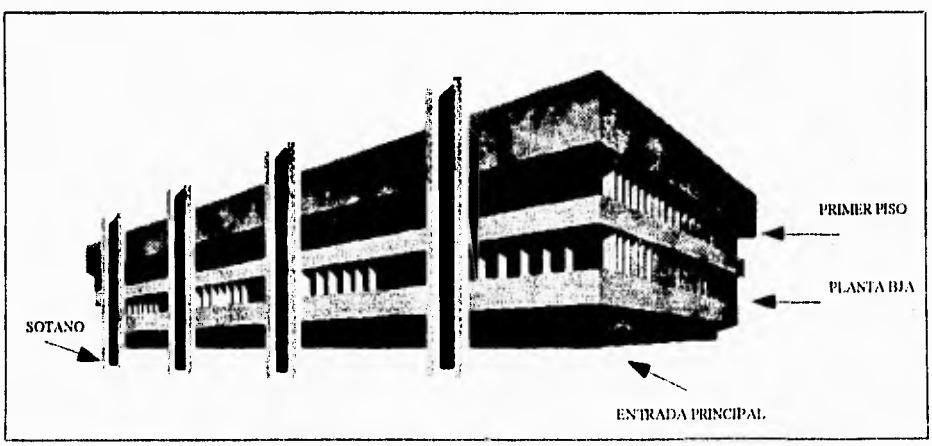


Figura 3.7 Edificio de oficinas generales.

En el 1er. piso se encuentra el área de Informática, Centro de cómputo y comedor. Dentro de esta área solamente se tiene un extinguidor y la ruta de evacuación es señalada con flechas rojas en la pared, indicando la salida de emergencia, la cual está ubicada a un costado del Centro de cómputo como lo muestra la siguiente figura:

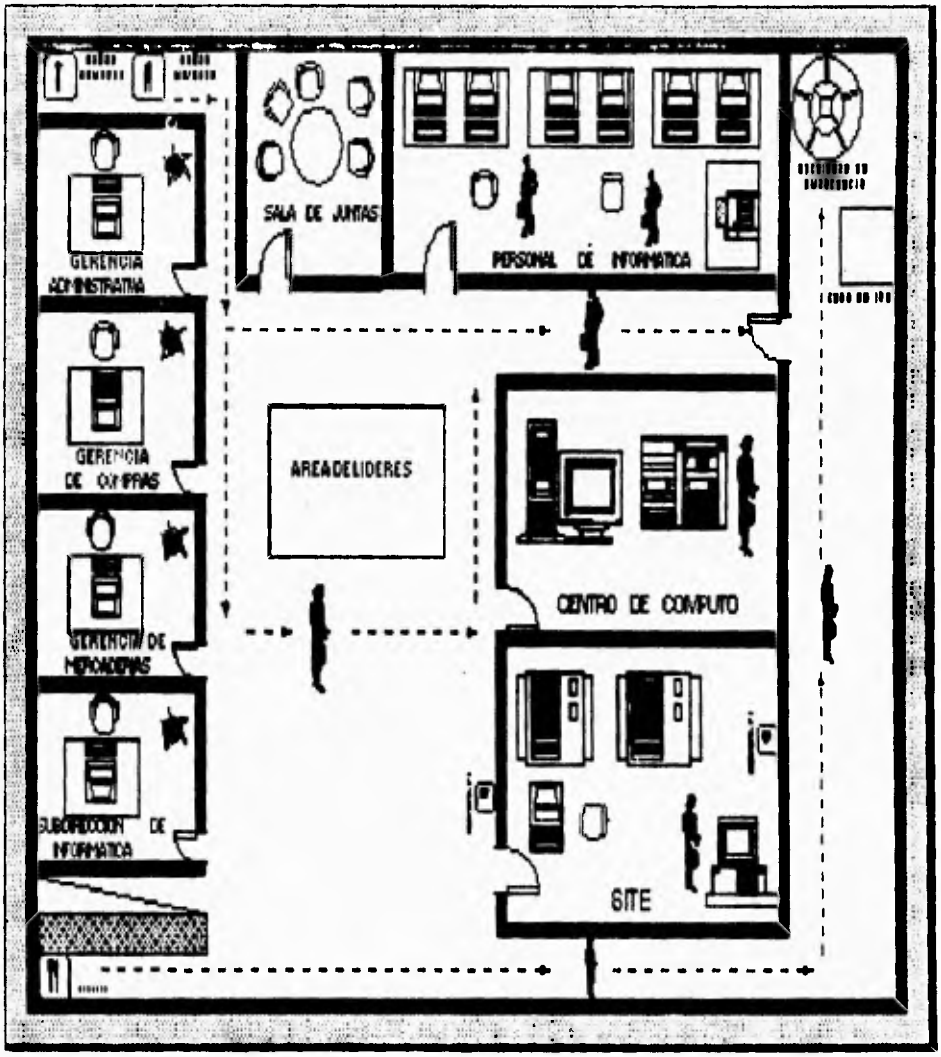


Figura 3.8 Primer Piso de las oficinas generales en el cual se encuentra el área de informática, Centro de Cómputo y Comedor.

En la planta baja se encuentran los Departamentos Administrativos: Finanzas, Contabilidad, Compras, Mercaderías y Recursos Humanos, las cuales están distribuidas de la siguiente forma :

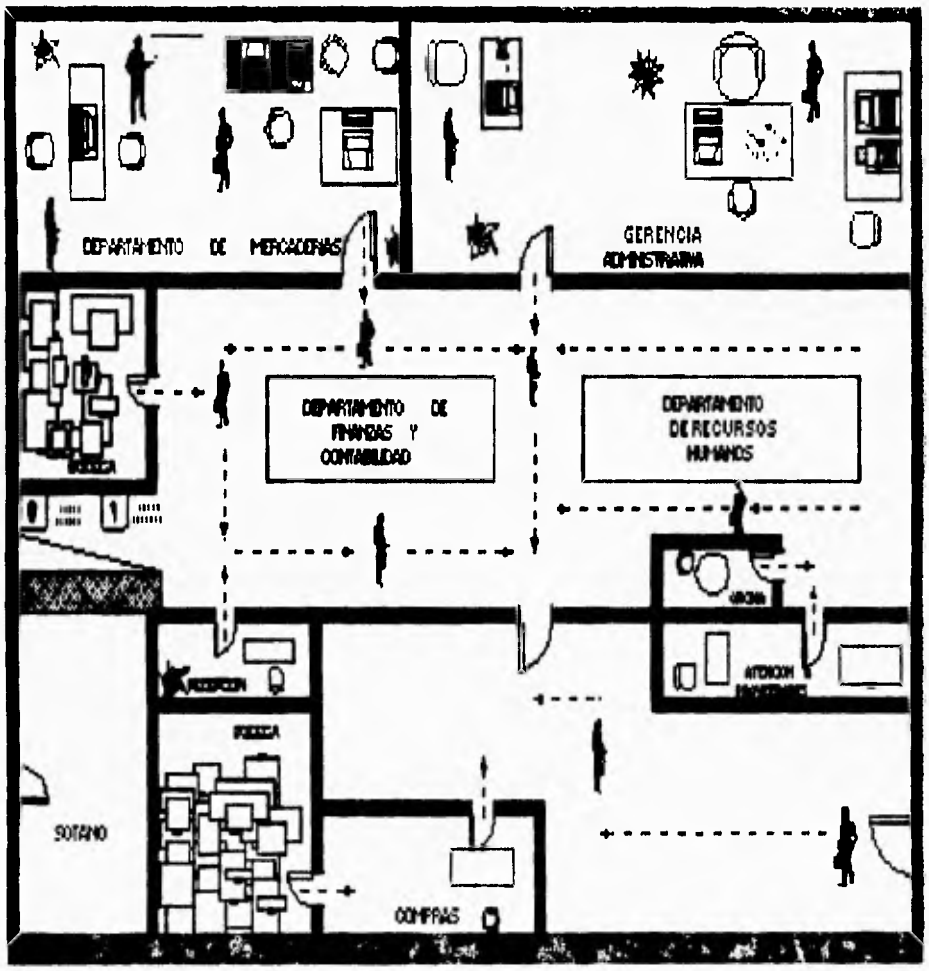


Figura 3.9 Planta baja, en la cual se encuentran los departamentos administrativos.

La ruta de evacuación, la cual se indica con flechas rojas, llega a la puerta principal del edificio, que a su vez, es la salida de emergencia.

En el sótano se encuentra la planta de emergencia para las instalaciones eléctricas de todo el edificio, Centro de cómputo y equipo en general. La ruta de evacuación también es indicada con flechas rojas, llegando a la salida de emergencia, como lo muestra la figura 3.10.

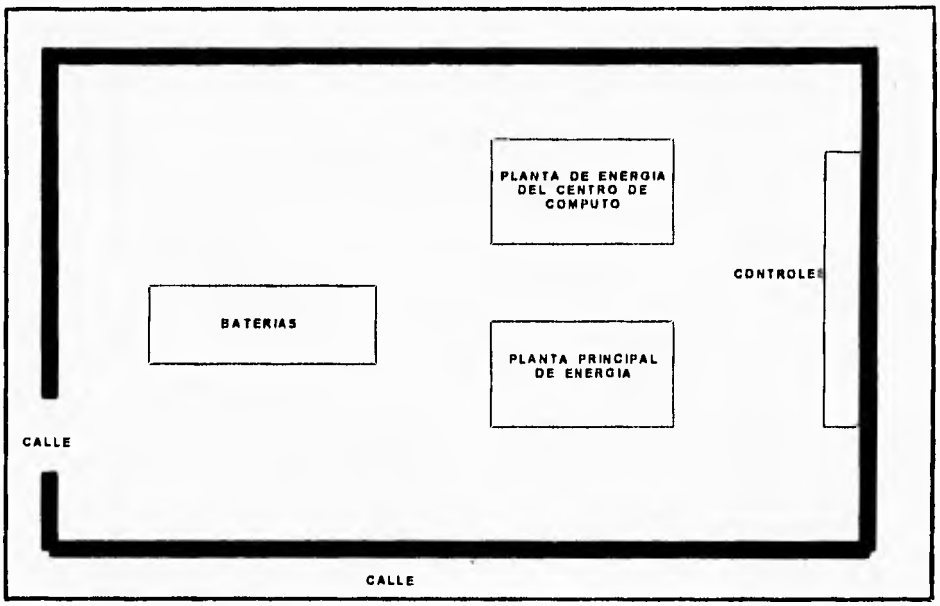


Figura 3.10 Sótano, en el se encuentran la planta de emergencia de suministro de energía eléctrica.

3.4.2 Hardware y Software de equipos.

En el siguiente apartado se revisará los equipos utilizados en:

a) Oficinas Generales y Sucursales
b) Centro de cómputo.
c) Comunicaciones
   - Red Satelital
   - Red LAN

A) Oficinas Generales y Sucursales

Dentro de las oficinas generales y las sucursales se tiene el siguiente equipo:

1. El equipo que se utiliza en oficinas son PC´s, donde éstas incluyen:
   - Conector de teclado mini- DIN

- Conector de mouse mini-DIN.
- Conectores en serie y paralelo para conectar impresoras y graficadores u otros dispositivos.
- Placas del sistema con dos bases de conexión para dos módulos de memoria principal y cuatro de conexión para 128 KB de memoria rápida (caché) de segundo nivel.
- Base de conexión de procesador disponible para una mejora fácil a un microprocesador más rápido.
- Interface de video Ultra VGA integrada con 512 KB de memoria de video, ampliable a 1024 KB (1 MB)
- Interface de disco integrado para sus unidades de disco flexible y unidad de disco duro IDE.
- Cuatro ranuras de arquitectura estándar de industria (ISA) de 16 bits para placas accesorias.
- Dos aberturas para unidades de disco: una de 3.5 y 5 1/4 pulgadas.
- SETUP basado en ROM con ayuda sensible al contexto para configurar la PC.
- El microprocesador utilizado puede ser : 486SX/25, 486DX/33 o 486DX2/66.
- Memoria RAM de 4MB, ampliable hasta 32MB, sin paridad.

2. El software utilizado en los departamentos administrativos es:

- Sistema Operativo DOS V. 5.0
- Hoja de cálculo.
- Procesador de palabras.
- Emuladores para terminal HP-792 o HP-796.
- Sistema de nómina integral (NOI) y Sistema de contabilidad integral (COI).

3. Para el departamento de informática :

- Sistema Operativo DOS V. 5.0
- Paquete de programación Clipper 5.0.
- Windows 3.1.
- Paquete para diagramas de flujo.
- Emuladores para terminales HP-792 o HP-796.

B) Centro de cómputo.

Las minicomputadoras que se utilizan en el centro de cómputo son HP-3000 series 900: modelos 992, 980, 967 y 932. Las cuales son de dos tipos:

- Series Midrange
- Series High-End

Como lo muestra la figura 3.11.

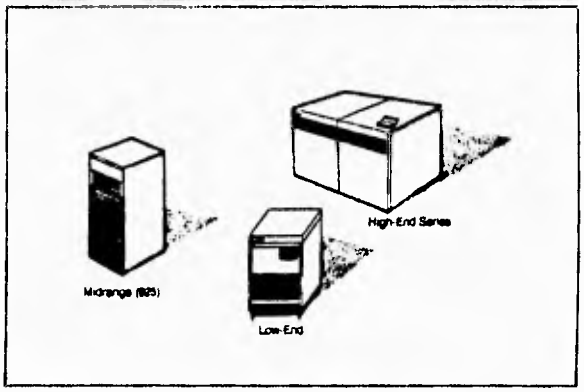


Figura 3.11 Gabinetes de las Series HP-3000/900

Dentro del centro de cómputo, las minicomputadoras HP-3000/992, 980 y 967 son series high-end; en tanto la HP3000/932 es serie Midrange. Las diferencias entre estas series son: el tipo de microprocesador, la capacidad en disco, velocidad de respuesta y el tamaño del gabinete, entre otras (como se muestra en la figura 3.12). Todas estas especificaciones son establecidas por los fabricantes de estos equipos.

En seguida se mencionarán algunas características de los gabinetes mencionados anteriormente:

1. Series Midrange

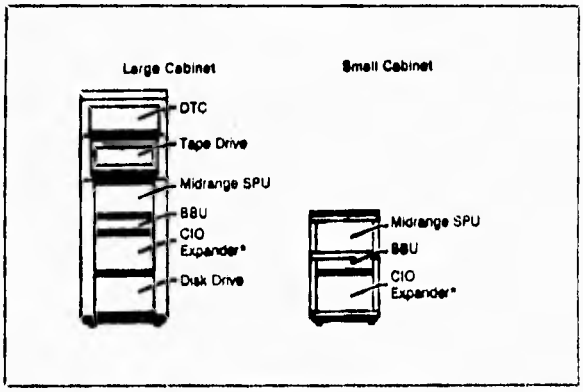


Figura 3.12 Gabinete de Series Midranges

DTC : Datacommunications y Terminal Controller(DTC), éste es utilizado para conexión de dispositivos en forma serial (terminales, modems, impresoras seriales) al CPU como una red de área local (LAN).

La figura 3.13, muestra los diferentes tipos de conectores que se utilizan para la conexión a un DTC.

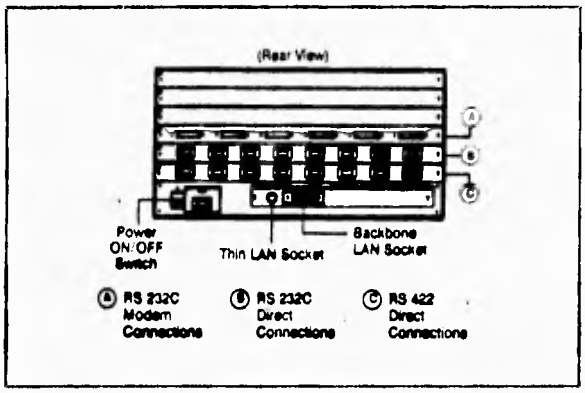


Figura 3.13 Controlador de terminales y comunicación de datos (DTC)

RS-232C: Se usa para conectar dispositivos de tipo serial (terminales, PC's, impresoras), con el SPU(System Processor Unit) via modem o conexiones directas arriba de 50 pies fuera del DTC.(Conector de 3 pin).

RS-422 : Conecta en forma directa los dispositivos seriales con el SPU, que distan a más de los 4000 pies fuera del DTC(Conector de 5 pin).

ON/OFF: Es el interruptor de encendido/apagado.

LAN socket: Es para conectar la red LAN con cable delgado.

Backbone LAN: Es para conectar la red LAN con el estándar 802.3 de IEEE.

Tape Drive: Es un dispositivo que se activa en forma automática ("auto-loading") para respaldos en unidades de cinta tipo riel o manual.

En el gabinete System Process Unit (SPU) residen las tarjetas de: memoria, periféricos, procesador y una fuente de poder, como se muestra en la figura 3.14.

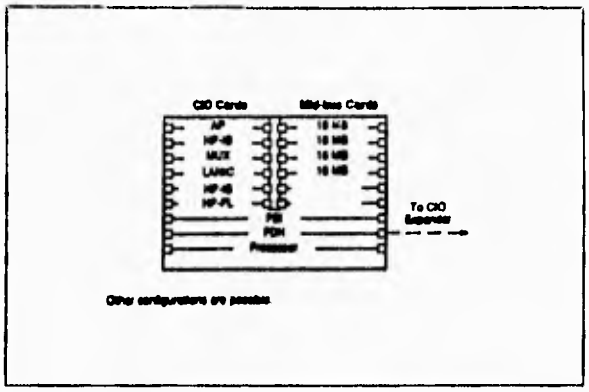


Figura 3.14 Configuración de SPU.

La batería de respaldo (BBU: Battery Backup Unit) pasa corriente a la tarjeta de memoria cuando ocurre alguna falla eléctrica.

El canal de expansión de I/O (CIO expander) provee de 8 slots adicionales de tarjetas para periféricos conectados al SPU (PSI, HP-IB, HP-FL, LANIC).

SI se ve la computadora de frente, vemos que tiene un panel de control con el cual nos muestra, por medio de led's, el estado del equipo. La figura 3.15 nos lo muestra:

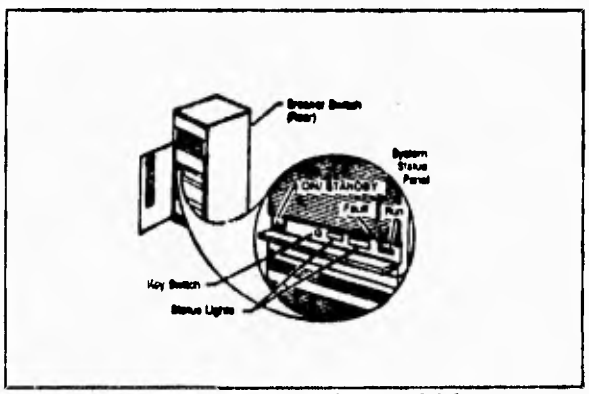


Figura 3.15 Interruptores y configuración de led's

La posición del interruptor habilita el acceso remoto, es decir para inicializar el sistema operativo e identificación de periféricos. Mientras que los led's, dependiendo del color nos indican el estado en que encuentra el equipo.

2) Series High-End

En la figura 3.16 se muestra el gabinete de las Series High-End.

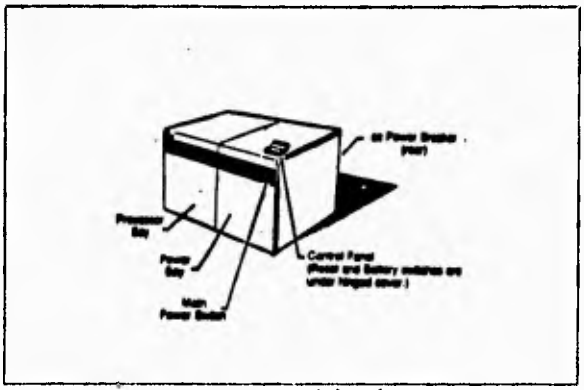


Figura 3.16 Series High-End

En el gabinete del Processor Bay se encuentran las tarjetas del System Process Unit (SPU) y "Cooling Fans".

En el gabinete del Power Bay se encuentran las unidades de corriente alterna , el cargador de batería, la batería y los transformadores.

El Main Power es el interruptor principal de encendido y/o apagado del equipo.

El Control Panel proporciona información completa del estado del equipo, donde éste se muestra en la figura 3.17.

Figura 3.17 Control Panel

También en este tipo de series se conectan DTC's y periféricos como los mencionados **para las series Midrange.**

Por lo anterior, nos podemos dar cuenta de la diversidad de especificaciones que existen en este tipo de minicomputadoras por lo que, la mala interpretación de los mensajes desplegados en la consola, relacionados con el estado de los led's del panel de control, puede ocasionar la demora en el restablecimiento del sistema en caso de una interrupción.

SOFTWARE

En sus cuatro equipos, cuenta con el siguiente software:

Sistema operativo:	MPE/iX v. 4.0
Lenguaje para desarrollo de sistemas:	POWER HOUSE v. 7.09 Cobol v. 8.05
Software para monitoreo de equipo:	GLANCE XL
Editor:	FULL SCREEN:QEDIT v. 3.9.1
Administrador de base de datos:	DBGENERAL v. 6.1
Servicios de Comunicaciones:	NS SERVICES v.B.0005 FTP/ARPA
Sistema de seguridad para acceso:	SECURITY
Monitoreador de seguridades:	VEAUDIT
Monitoreador de red con DTC's:	OPEN VIEW

C) Comunicaciones

C.1. Red Satelital

1) Conmutador TP4

Es una red tipo malla-estrella, como lo muestra la figura 3.18.

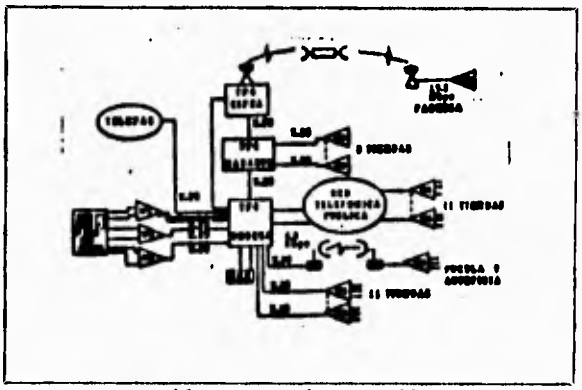


Figura 3.18 Red de conmutación de paquetes del Centro Comercial

Esta tiene un nodo principal un conmutador de paquetes TP4/II-4255, instalado en las oficinas centrales. Este conmutador puede soportar hasta 224 puertos X.25 (ver anexo B), sin embargo, solamente tiene instalados 48 de estos puertos.

Tiene una capacidad máxima de manejo de información hasta de 820 paquetes por segundo. Conjuntamente con los concentradores TP3 y los conmutadores TP4 de la sucursal Masaryk, al que está conectado con troncales de 9.6 Kbps, y de la sucursal Cuajimalpa, con troncales de 64 Kbps, forman una malla-estrella a través de la cual recibe y envía comunicaciones a las demás sucursales.

2) Concentradores TP3

A los puertos X.25 del conmutador TP4/II-4255 se conectan 31 concentradores TP3325E (ver anexo A). De estos, 28 se encuentran instalados en igual número de sucursales y tres se conectan localmente a la computadora huésped HP-3000. Estos equipos TP3325E están instalados como se muestra en la figura anterior y se subdividen de la siguiente forma:

- 11 concentradores utilizan líneas privadas.
- 3 concentradores entran por el TP4 de la sucursal Masaryk y usan línea privada.

- 11 concentradores utilizan líneas telefónicas conmutadas.
- 2 concentradores utilizan enlaces de microondas.
- 1 concentrador utiliza un enlace satelital.
- 3 concentradores utilizan líneas locales para conectar el TP4 al computador central HP-3000 de oficinas generales.

En general, cada TP3 cuenta con 8 puertos disponibles, cinco de los cuales están asignados a las aplicaciones siguientes :

- TEF (Transferencia Electrónica de Datos)
- TPI con protocolo BSC (Control Sincrono Binario).
- Recibo, con protocolo asincrono.

TEF

En cada sucursal, se cuenta con una red local de cajas NCR, donde cada una de ellas tiene un lector electromagnético de tarjetas de crédito. Estas cajas están conectadas a una maestra que tiene acceso a la red mediante el protocolo BSC3270.

TPI

Esta utiliza un conmutador de Banamex (Conmutador TANDEM de la sucursal Masaryk) y en las demás se utilizan terminales de punto de venta con lectora electromagnética de tarjetas marca ICOT modelo TPI.

RECIBO

El modo de transmisión es asíncrono, carácter por carácter, usando PC´s (HP) instaladas en las sucursales conectadas al computador central HP-3000.

OFICINA ADMINISTRATIVA

Realiza la transferencia de información de cada tienda en forma asíncrona, por bloques de datos, y utiliza el protocolo ENQ/ACK de Hewlett Packard.

3) Centro de control TP5

Este consiste en un computador de propósito general con un software especializado para administrar la red. Las caracteristicas del centro de control TP5 se pueden ver en el anexo C.

Para el caso del Centro Comercial en cuestión, se trata de un computador PRIME modelo 2450 con 8 MB de memoria principal, dos unidades de disco duro con 360 Mb cada uno, una

unidad de cinta streamer de 40 MB por cartucho, una impresora, su consola y un monitor a color .

Software

1.Centro de Control de la Red.

El centro de control está basado en un computador PRIME modelo 2450 cuyo software se compone del sistema operativo PRIMOS, los programas utilizados para el manejo de la red PRIMENET y los programas especializados de SPRINT INTERNATIONAL, que sirven para la configuración de los componentes de la red.

En cuanto a los archivos de configuración del computador PRIME, a continuación se describen brevemente los principales:

a) CONFIG.OFICIN

Este archivo proporciona la información de tipo estadístico, que define :

- Capacidad de equipo
- Número de Usuarios
- Identificación del sistema
- Disco del Sistema operativo al hacer un Boot
- Cantidad de Memoria Virtual
- Memoria asignada a procesos y usuarios
- Número de puertos físicos y protocolos que manejan
- Eventos que se habilitan o deshabilitan.

Cabe mencionar que al modificar algunos de estos parámetros será necesario realizar un hard-reset o boot al sistema para que tome los cambios.

b) PRIMOS.COMI

Este archivo radica en el directorio CMDNC0 y se utiliza para la configuración dinámica del sistema, es leído cuando se inicializa el sistema.

c) PRIMENT*>CONFIG.OFICIN.X.25

Este archivo es el que configura en la tarjeta de comunicaciones, los parámetros de operación de los puertos X.25 y direcciones de la red a las que se tiene acceso desde la red. Los puertos de red del PRIMENET se inicializan automáticamente en el momento en que se efectúa el boot.

2. Archivos SPRINT INTERNATIONAL .

a) CONFIG (NETWORK DATA BASE EDITOR)

Es un editor que establece la estructura física de los equipos TP´s y su conectividad en la red. El programa CONFIG afecta dos bases de datos, NETWRK y PSECON.

b) PGP (PROFILE GENERATION PROGRAM)

Es un programa que se utiliza para asignación de atributos de configuración para establecer los perfiles del puerto, de acuerdo a los requerimientos y protocolos utilizados por la aplicación. Este lo utilizan para asignar los perfiles de los puertos de los TP4/II y TP3/II.

c) SNAPP (SYSTEM NODE AND PORT PROFILER)

Este programa asigna los atributos de la configuración al puerto en forma similar al programa PGP, sólo que es utilizado para los equipos TP4/III y TP8000.

d) CODE EDITOR

Define la combinación de códigos de software que un TP requiere para operar, además efectúa la asociación de un grupo de códigos de software con un nombre de módulo de códigos.

e) CODVR (CODE OVERRIDE PROGRAM)

Se utiliza para cambiar o modificar el módulo de códigos de software para una máquina (TP) específica.

f) DBUILD (DYNAMIC TABLE BUILDER)

Este ensambla y procesa los datos de las bases generadas por los programas de configuración (proceso de compilación), para generar las tablas actuales que serán cargadas en las máquinas y TP´s dentro de la red.

g) AUTOROUTER

Genera las tablas de enrutamiento que habilitan el establecimiento de las llamadas virtuales a través de la red. También identifica las rutas que van a cada dispositivo destino dentro de la red.

h) SAVE-TABLES

Este, en conjunto con los programas que se definieron anteriormente, forman el grupo de programas de construcción de tablas de configuración fuera de línea. Por otro lado, SAVE-TABLES almacena las tablas de disco o cinta para ser usadas por los programas de construcción de tablas de línea.

i) RESTORE-TABLAS

Recupera las tablas de configuración, previamente almacenadas por SAVE-TABLES, y las deja disponibles para que se utilicen por el programa TPLOAD, quien a su vez se encarga del proceso de software de configuración para los equipos TP's de la red.

j) CONTROL (COLOR MONITOR SYSTEM)

Da el acceso de comando para el sistema de monitor a color. Con estos comandos se monitorea el total de la red, con la facilidad de monitorear la red global o bien un puerto en particular del TP. Con este sistema se visualiza el estado actual de los TP's, tarjetas, puertos, enlaces, buffers, entre otros.

4. ANALISIS DE LAS NECESIDADES DE LA EMPRESA

En la recopilación de la información operativa de cada departamento del Centro Comercial, realizada en el capítulo anterior, se obtuvo una descripción lo más detallada y exacta posible de la forma como se desarrollan las operaciones más importantes, identificando dos puntos principales para su funcionamiento continuo:

- Algunos procesos son indispensables, ya que si se prescindiera de ello paralizarían el funcionamiento de las áreas involucradas, ocasionando una cuantiosa pérdida financiera.

- En el Departamento de Informática, el área del Centro de cómputo y Soporte Técnico juegan un papel de vital importancia en la vida del Centro Comercial, ya que ésta se encarga del procesamiento, integración y seguridad de la información del mismo.

Por lo que, sin una buena estrategia de recuperación, la pérdida de información puede causar la quiebra de la empresa. Es por ello que se han diseñado dos encuestas que engloban las necesidades primordiales de todos los departamentos.

La primera encuesta está dirigida a los departamentos administrativos para recabar información de sus aplicaciones críticas. Mientras que la segunda, está dirigida al departamento de informática que se encargará de identificar todos los procesos para la ejecución de la aplicación mencionada en la encuesta anterior.

Antes de comenzar a detallar los procesos de las diferentes áreas involucradas, se dará una breve definición de los términos utilizados en las encuesta diseñadas.

Encuesta para los Departamentos Administrativos.

Estas encuestas incluyen:

- Aplicación :Es el nombre del proceso a ejecutar.

- Definición :Es una explicación concisa de la función del proceso.

- Prioridad :Es el nivel crítico en que se ubica un proceso dependiendo de la importancia que tiene para las diferentes áreas de la empresa. Estos niveles se identifican como :

  a) Alto (A): Procesos de mayor impacto que amenazan la subsistencia de la empresa.

  b) Medio(M): Procesos cuya interrupción prolongada causa grandes inconvenientes, siendo relativamente fácil realizar procedimientos de apoyo.

c) Bajo (B): Procesos de poco impacto en términos de reposición del servicio interrumpido.

- Frecuencia: Es el ciclo normal de ejecución del proceso, que puede ser diario, semanal, quincenal, mensual o anual.

- Horario: Es el turno asignado para la realización del proceso. Dividiéndose en:

  a) Matutino (M): de 6:00 a 14:00 hrs.
  b) Vespertino(V): de 14:00 a 22:00 hrs.
  c) Nocturno (N): de 22:00 a 6:00 hrs.

- Meses y Días Críticos: Es el tiempo preestablecido para el procesamiento de la información más importante.

- Necesidad : Son herramientas solicitadas por el usuario, como pueden ser: papel, equipo de cómputo, entre otros.

- Tiempo Máximo: Es el tiempo en el cual el proceso puede dejar de funcionar sin causar efecto importante en la operación de la empresa.

- Area de la que depende : Es el área que transfiere información necesaria para que el proceso cumpla su objetivo.

- Información requerida: Son datos y/o documentos que se necesitan para llevar a cabo el proceso.

- Ejecución: Forma en que el proceso genera resultados, donde éstos pueden ser: Procesos batch (jobs), en línea.

- Información Generada: Es el almacenamiento o salida de reportes de los resultados obtenidos del proceso.

- Usuarios Finales : Son aquellos que utilizan la información generada.

- Procesos Opcionales: Aquellos procesos que se corran adicionales a la aplicación.

Encuesta para el Departamento de Informática.

Estas encuestas incluyen:

- Nombre: Es el nombre del proceso Batch donde las dos primeras letras identifican al sistema las dos siguientes son JB (Job) y posteriormente el número del job.

c) Bajo (B): Procesos de poco impacto en términos de reposición del servicio interrumpido.

- Frecuencia: Es el ciclo normal de ejecución del proceso, que puede ser diario, semanal, quincenal, mensual o anual.

- Horario: Es el turno asignado para la realización del proceso. Dividiéndose en:

  a) Matutino (M): de 6:00 a 14:00 hrs.
  b) Vespertino(V): de 14:00 a 22:00 hrs.
  c) Nocturno (N): de 22:00 a 6:00 hrs.

- Meses y Días Criticos: Es el tiempo preestablecido para el procesamiento de la información más importante.

- Necesidad : Son herramientas solicitadas por el usuario, como pueden ser: papel, equipo de cómputo, entre otros.

- Tiempo Máximo: Es el tiempo en el cual el proceso puede dejar de funcionar sin causar efecto importante en la operación de la empresa.

- Área de la que depende : Es el área que transfiere información necesaria para que el proceso cumpla su objetivo.

- Información requerida: Son datos y/o documentos que se necesitan para llevar a cabo el proceso.

- Ejecución: Forma en que el proceso genera resultados, donde éstos pueden ser: Procesos batch (jobs), en línea.

- Información Generada: Es el almacenamiento o salida de reportes de los resultados obtenidos del proceso.

- Usuarios Finales : Son aquellos que utilizan la información generada.

- Procesos Opcionales: Aquellos procesos que se corran adicionales a la aplicación.

Encuesta para el Departamento de Informática.

Estas encuestas incluyen:

- Nombre: Es el nombre del proceso Batch donde las dos primeras letras identifican al sistema las dos siguientes son JB (Job) y posteriormente el número del job.

- Descripción: Es una breve explicación de la aplicación.

- Periodo: Es el ciclo normal de ejecución del job. Este puede ser:

  a) Diario (D).
  b) Eventual (E).
  c) Mensual (M).
  d) Anual (A).

- Prioridad: Nivel crítico en el que se ubica el job. Estos niveles se definen como :

  a) Alto (A): Procesos de mayor impacto que amenazan la subsistencia de la empresa.

  b) Medio(M): Procesos cuya interrupción prolongada causa grandes inconvenientes, siendo relativamente fácil realizar procedimientos de apoyo.

  c) Bajo (B): Procesos de poco impacto en términos de reposición del servicio interrumpido.

- Responsable de Ejecución: Es el personal encargado de llevar a cabo la ejecución del job.

- Proceso Previo: Se determina si es necesario ejecutar un proceso anterior.

- Reproceso: Indica si este job puede ser ejecutado dos veces dentro del mismo período.

Para la aplicación de estas encuestas se trabajó conjuntamente con las áreas administrativas, asesorando, recabando y depurando la información, con la finalidad de identificar las aplicaciones críticas. Posteriormente, con los resultados obtenidos, en colaboración con el departamento de informática, se procedió a establecer la relación proceso/aplicación, que consiste en asignar el número de proceso correspondiente a la aplicación, de acuerdo a su nivel de riesgo dentro de los diferentes sistemas.

Una vez definidos los términos, se presentan a continuación los resultados de las encuestas con la información requerida, de todas las áreas de los departamentos que componen al Centro Comercial.

CENTRO COMERCIAL S.A. DE C.V.

ENCUESTA PARA DEPARTAMENTOS ADMINISTRATIVOS

DEPARTAMENTO: CONTABILIDAD

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	1 día						
	[illegible]					1 PC LOTUS							
	[illegible]												
	[illegible]												
	[illegible]												
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]		[illegible] batch			
[illegible]	[illegible]					[illegible]		[illegible]					
	[illegible]												
	[illegible]												
[illegible]	[illegible]												
	[illegible]												
	[illegible]												
	[illegible]												
	[illegible]												
	[illegible]												
	[illegible]												
[illegible]	[illegible]		Diario [illegible]			[illegible]		[illegible]					
						[illegible]							
						[illegible]							
[illegible]	[illegible]		Diario			PC/[illegible]		[illegible]					

NOTA: Adicionalmente se requiere impresora para el equipo Hp3000 y la PC
El papel utilizado es tamaño carta (blanco) y caramelo

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]			[illegible]			
[illegible]	[illegible]					[illegible]							
[illegible]	[illegible]												
	[illegible]												
	[illegible]												
	[illegible]												
	[illegible]												
	[illegible]												
	[illegible]												
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]			[illegible] batch			
[illegible]	[illegible]					[illegible]							
	[illegible]												
	[illegible]												
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]			
[illegible]	[illegible]					[illegible]			[illegible]				
[illegible]	[illegible]								[illegible]				
	[illegible]												
	[illegible]												
	[illegible]												
	[illegible]												

NOTA: Adicionalmente se requiere impresora para el equipo Hp3000 y la PC
El papel utilizado es tamaño carta (blanco) y caramelo

CENTRO COMERCIAL S.A. DE C.V.

ENCUESTA PARA DEPARTAMENTOS ADMINISTRATIVOS

DEPARTAMENTO: CONTABILIDAD

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
Depreciación	El valor del importe	Importante	Mensual	Trabajo			Depende de la	Informática y finanzas		PC		Contabilidad	
	que afecta resultados						información						
	que sean computo						Importe						
Depreciación fiscal	El valor del importe	Importante	Semestral	Trabajo			Depende de la	Nomina		HP 3000 y personal		Fiscal	
	que afecta el resultado						declaración anual			de PC			
	de fiscal												
Amortización fiscal	Informes con saldos en los	Importante	Semestral	Trabajo			Depende de la	Nomina		PC		Fiscal	
	cuentas de activo						declaración anual						
	de capital diferido												
	perdidas						Depende de la	Nomina		PC		Fiscal	
Base 2%	El valor del importe	Importante	Semestral	Trabajo			declaración anual						
	de impuesto que se												
	toma para calcular												
	el impuesto												
Inventarios fiscal	Reportes Fiscal de	Opcional	Una hoja por	Trabajo			1 día	Informática	Reportes	HP 3000 y personal		Auditoria de Sucursal	
	los saldos (Kardex)		semana							auditor			
	de la contpaq												
El impuesto de activo	Listado de los saldos	Opcional	Semestral	Trabajo			1 Trimestre	Auditoria	Reportes			Subsidiarias	
	siguientes que												
	integran los saldos												
	contables												

Nota: Para todas las aplicaciones se necesitan de: 3 Personas, PC (LOTUS 123), 3 Escritorios, Sillas, 2 Calculadoras
3 Blocks Tabulares de 8 columnas, 1 Caja de Papel Caramelo, 1 Caja de papel carta, 1 caja de diskettes de 3.5 y 5 1/4.
Impresoras.

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
Pagos de nomina	Proceso que requiere	Diariamente	Mensual	Nocturno						Personal			
	el saldo diario de cada					1 Terminal		Contadores internos					
	una de las cuentas												
	bancarias												
Utilerías varias banco	Procesos que efectua	Medio	Mensual	Nocturno		1 Persona	3 a 5 días	Bancos	Estados de cuenta	Personal			
	Cuadre de partidas de					1 Terminal							
	la empresa con las del												
	banco y reporte final												
	las que quedan por												
	cierre												
Captura de polizas	Captura de polizas	Medio	Diario	Matutino		2 Personas	1 Semana	Contpaq	Cuadre Mensual	1 Hora			
	de diario, ingreso,												
	egresos diferentes												
	en el periodo anterior												
ALTAS	Captura en el sistema	Importante	Diario	Trabajo						HP 3000		Auditoria fiscal	
	Equipos adquiridos												
	por la Compañia												
BAJAS	Cambios varios de			Trabajo		1 Mes		Nomina				Auditoria fiscal	
	los Equipos a cambio												
	o Desechados												

NOTA: Adicionalmente se requiere impresora para el equipo Hp3000 y la PC
El papel utilizado es tamaño carta (blanco) y caramelo

CENTRO COMERCIAL S.A. DE C.V.

ENCUESTA PARA DEPARTAMENTOS ADMINISTRATIVOS

DEPARTAMENTO: CONTABILIDAD

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX. SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]			[illegible]	[illegible]		PC			
[illegible]	[illegible]	[illegible]	[illegible]				[illegible]	[illegible]		PC			
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]			[illegible]	[illegible]		[illegible]		[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]			[illegible]	[illegible]	[illegible]	HP 3000		[illegible]	

Nota: Para todas las aplicaciones se necesitan de: 3 Personas, PC (LOTUS 123), 3 Escritorios, Sillas, 2 Calculadoras
3 Blocks Tabulares de 8 columnas, 1 Caja de Papel Caramelo, 1 Caja de papel carta 1 caja de diskettes de 3.5 y 5 1/4 — [illegible]

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX. SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]			
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]			
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]			[illegible]			
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]			[illegible]			
[illegible]	[illegible]		[illegible]		[illegible]		[illegible]						
[illegible]	[illegible]		[illegible]		[illegible]		[illegible]						

NOTA: Adicionalmente se requiere Impresora para el equipo Hp3000 y la PC
El papel utilizado es tamaño carta (blanco) y caramelo

CENTRO COMERCIAL S.A. DE C.V.

ENCUESTA PARA DEPARTAMENTOS ADMINISTRATIVOS

DEPARTAMENTO : FINANZAS

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX. SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
Mantenimiento de Bancos	Actualizacion Maestro de Bancos	Alta	Diario	De 7 a 7 hrs		Respaldo de movimientos diario hasta las diez pm Escritorio Suministro PC (Excel) y conexion Impresora de red HP 3000 Facilidad de Terminal de consulta mainframe Correo Electronico	4 hrs	Tesoreria Bancos Contabilidad Caja Informatica					
Reporte de saldos	Reporte de los saldos generados por los movimientos de cada una de las cuentas		Diario	Todo el Dia			8 hrs	Mantenimiento de bancos Las diferentes					
Depuracion de bancos	Depuracion de Partidas viejas pendientes de conciliar referente a cuentas bancarias		Diario	Todo el Dia			8 hrs	Mantenimiento de bancos Contraloria Control de ingresos					
Conciliacion Contable	Conciliacion de Cuentas Los diagramas o tablas		Diario	Todo el Dia			8 hrs	[redacted] personal [redacted] externos Algo similar al siguiente los siguientes procesos					

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX. SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
Pagos a Proveedores	Pago diario de los pagos a proveedores y acreedores	Alta	Diario	Todo el Dia		Respaldo de movimientos diario hasta las [redacted] 1 Persona 1 Terminal	1 hrs	[redacted] Consumos Internos Personal Mercancias	Listado de bancos	Proceso batch	Integracion Diaria efectivo con Merca varios Datos Pagados Bancos Datos Vigentes por proveedor Datos Pagados por proveedores Recompras Datos Recomprados por vencimiento Pagos en [redacted] los recompras	Finanzas Contraloria	Diario / semanal Mensual
Control de ventas en consignacion	Control de ventas de mercancias propiedad de proveedores	Media	Semanal (Viernes)	Horario Vespertino		1 Persona 1 Terminal	15 Dias	Mercancias Generales [redacted] Cuentas a la vista Pagos varios	Facilidad de Cuenta Transferencias	Proceso batch Interactivo	Estados de cuenta Reportes por tipo	Proveedores externos	

CENTRO COMERCIAL S.A. DE C.V.

ENCUESTA PARA DEPARTAMENTOS ADMINISTRATIVOS

DEPARTAMENTO : FINANZAS

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX. SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
Cuentas de acreedores	Proceso de liquidacion	Media	Anual (Diciembre)	1 Hr									
	pago de acreedores			Dia									
Pagos a Proveedores	Cuentas de proveedores	Media	Mensual	Variable y Irregular		1 Persona	8 Hrs	Compras Ingresos	Cheques de pagos a	Ver Supervisor de Cen	Reporte de cuentas		
	y pagos a Proveedores					PC (Excel)			proveedores	por via electronica	de acreedores y pagos		
	Local												
Prestamos Programados	Aplicacion de los	Alta (Acumulacion	Diario	Nocturno			2 hrs	Tarjetas(Informacion	Cuentas por pagar	Ingresos Sueldos		Mismo Area	
	cuentas por pagar	ingresos)						por division por linea)		cuentas vendor			
	de cada una de las	Media (Movimientos											
	sucursales en el HP												
	3000. Cada una												
	con su clave y IP						4 hrs		Liquidacion de la cuenta	Ver en terminal		Ventas programadas	
	de 4 dias								pagos de prestamo	Ingresar en pantalla		al sistema de manera	
	la aplicacion en el											Mismo area, informe	
	sistema de Cuentas											de movimientos de	
	por Pagar Opcion											cuentas	
	Pagos mensuales y												
	reporte de pagos												
Lectura de cheques	De acuerdo a la cuenta	Alta	Diario	Durante el dia	Meses criticos, enero		48 hrs	Cuentas	Facturas pagadas	Pantalla CRT	Alta liquidacion cuentas	Proveedor y Caja	Se realizara de acuerdo
con cuentas de Caja	bajas de cheques que				julio, agosto				Listados y Computos		de gastos por centros	Chofer	a las cuentas pagadas
	se emiten se verá		Semanal	Nocturno	Meses de fin y diciembre		48 hrs		Lista de pagos		Cuenta bancaria por		con cheques en forma
	con el de banco a fecha				Dias 15 y 30				Cheques diarios y fijos		Sucursales y Cheques		manual
	para su entrega				Los 3 ultimos y previo				Notas				
					a fin de cada mes				Con fuente de Info				

NOTA Para todas las aplicaciones se necesario una terminal conectada a la HP-3000/992

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX. SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
Pagos	Recepcion y Lectura		Diario	1 Hr (Matutino)		1 Persona							
	de cheques												
	Impresion de Informe		Semanal	30 Hrs (Matutino)				Bancos externos					
	mensual (Sabados)												
	Captura		Diario	02 Hrs (Matutino)		PC con puerto para		Pagos					
						la HP 3000							
	Envio de información		Diario	1:00 Hrs (Matutino)		Papel blanco							
	a sucursales y bancos												
	Gestion telefonica a		Diario	2:00 Hrs (Matutino)									
	sucursales y bancos												
	Tramites de los mas		Diario	4:30 Hrs (Matutino)		Papel blanco							
	polizas de sucursales												
	y bancos												
	Arqueo externo		Mensual	4:30 Hrs (Vespertino)		Papel blanco		Personal y bancos					
	Corte general		Semanal	2:00 Hrs (Vespertino)		Papel blanco		Abogado externo					
	Corte mensual		Mensual	18:00 Hrs (Vespertino)		Papel blanco		Sucursales					
	Arqueo interno		Mensual	3:30 Hrs (Matutino)		Papel blanco		Contadores					

Nota: Se requere guardar en otro edificio 1 PC (Excel y puerto para la HP3000). Diskettes con programas

En caso de pérdida total de valores, no son recuperables a la fecha hs 4:00 00

Para todas las aplicaciones se necesita 1 Persona

CENTRO COMERCIAL S.A. DE C.V.

ENCUESTA PARA DEPARTAMENTOS ADMINISTRATIVOS

DEPARTAMENTO: FINANZAS.

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX. SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
[illegible]	Depósito Diario [illegible]		Diario	[illegible] hrs (Matutino)		PC (Excel)		[illegible]					
	[illegible] a Bancos		Semanal	[illegible] hrs (Vespertino)									
Cheques Devueltos	Recepción y clasifica-		Diario	10:[illegible] hrs (Matutino)				Bancos externos					
	ción de documentos												
	Captura		Diario	[illegible] hrs (Matutino)		PC y puerto para		Informática					
						la HP 3000							
	[illegible] de cheques		Diario	10:[illegible] hrs (Matutino)		Papel blanco		[illegible]					
	con [illegible]												
	Envío de informes de		Diario	11:30 hrs (Matutino)		Papel blanco		Sucursales, [illegible]					
	[illegible] y [illegible]							[illegible]					
	Trámite de [illegible]		Diario	[illegible] hrs (Matutino)		Papel blanco		[illegible]					
	[illegible]												
	[illegible]		Mensual	[illegible] hrs (Vespertino)		Papel blanco		[illegible] externo					
	[illegible]												
	[illegible]		Mensual	12:00 hrs (Vespertino)		Papel blanco		Informática					
	[illegible]												

Nota: Se requiere guardar en otro edificio. 1 PC (Excel y puerto para la HP-3000), Discos con programas

Para todas las aplicaciones se necesita: 1 Persona

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX. SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
Cheques devueltos	[illegible] de cobranza		Diario	[illegible] hrs (Matutino)				Sucursales y clientes					
	[illegible]												
	[illegible]		Mensual	6:00 hrs (Matutino)		Papel blanco		Contraloría					
	Depósitos de pagarés		Semanal	1:30 hrs (Matutino)		Papel blanco		[illegible]					
	[illegible] con cheques		Diario	10:15 hrs (Matutino)		Papel blanco		[illegible]					
	[illegible]		Diario	[illegible] hrs (Matutino)		Papel blanco		[illegible]					
	[illegible] con cheques		[illegible]	1:30 hrs (Vespertino)		Papel blanco		[illegible]					
	[illegible] Con-		Mensual	[illegible] hrs (Vespertino)		Papel blanco		[illegible] externo					
	[illegible] con cheques												
	[illegible]		Diario	[illegible] hrs (Vespertino)				Bancos [illegible]					
	[illegible]												

Nota: Se requiere guardar en otro edificio. 1 PC (Excel y puerto para la HP3000), Diskettes con programas

Para todas las aplicaciones se necesita: 1 Persona

CENTRO COMERCIAL S.A. DE C.V.

ENCUESTA PARA DEPARTAMENTOS ADMINISTRATIVOS

DEPARTAMENTO: COMPRAS.

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX. SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
Recepción de	Automatizar el proce	Media	Diario Mensual	Mañana y tarde		1 Persona	El requerido por las	Compras	Reporte Hojas de	Recepción FLETE	Preparación de facturas	Compras	Poder realizar un fax
Base de datos	Que mantenga de						áreas de compras		para el proceso	Personal	para su captura		en cierto horario para
	las áreas de compras								de facturación con	Programa de impresión de			recibir los formularios
										facturas			
El departamento de	Verifique en el sistema	Alta	Diario	Mañana y tarde		1 Terminal (Internet)	El requerido por las	Compras	Hojas de pedidos con	Consulta en línea	A las áreas de Compras	Sucursales compras	
Recepción	de mercadotecnia que					Formatos pre impresos	áreas de compras		Compras numero	a la base SC	para la recepción		
	los documentos no					hoja de dictos			existan rechazos		de mercancías y	Almacenes	
	estén duplicados y					1 persona					de los productos		
	que su código de										captura		
	barras sea el correcto												
Verificación de	Que el envío solicitado	Media	Diario	Mañana y tarde		1 Copiora	El requerido por las						
Recepción	en facturas sea						áreas de compras						
	el que realmente llegó												
Captura de	Que el artículo en el sis	Alta	Diario	Mañana y tarde		1 Persona 1 Terminal	El requerido por las	Compras	Hojas de pedidos con	Consulta en línea	Almacenes el sistema	Compras Sucursales	
Base de datos	ema de compras						áreas de compras		Compras	a la base SC	Que la información	Cuentas por pagar	
	sea la correcta										para Sucursales y		
											Cuentas por pagar		

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX. SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
Verificación de	Que la información sea	Alta	Diario	Tarde		1 Persona 1 Terminal	1 Día por las	Informática		Procesos de Switch	Emisión de Notas	Formatos preimpresos	
Base de datos	Suficiente para poder					1 Impresora disponible	urgencias			para Facturas	Existencias y Cantidad	Hoja de Catálogo	
	verificar adecuadamente					para la HP 2100					de productos con	Lectores Scanner	
						formatos preimpresos					Usuarios para los que	Cambios de precio	
						para documentos de					y sus condiciones para		
						Facturas - compras							
Entrega de	Se requiere la orden	Alta	Diario	Mañana y tarde		1 Persona	Inmediato	Informática	Ingresar de	Manual	Entregar a compras		
Mercancía	física de la factura y							mercancía	documentos		para que revise y		
	la compras										de ahí		
											pasa a bodega a tomar		
											para que verifiquen		
Control de	Registrar y actualizar	Alta	Diario	Mañana y vespertino		1 Persona					Hojas de Entrada	Sucursales y oficina	
	inventarios al recibir					1 PC					Hojas de Cargo		
	un artículo nuevo					Impresora					Transferencias		
											Cancelados		
Pedidos	Elaborar un pedido	Alta	Diario	Mañana		1 Persona					Formatos de Pedidos	Sucursales altos de	
						1 PC						departamento	
						1 Impresora						Oficinas	
Almacén	Consulta de stocks	Media	Diario	Todo el día		1 WIN 3x45						Sucursales altos de	
	y cantidades de pedido					1 Terminal						departamento	
						1 Impresora							

CENTRO COMERCIAL S.A. DE C.V.

ENCUESTA PARA DEPARTAMENTOS ADMINISTRATIVOS

DEPARTAMENTO: COMPRAS.

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX. SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
[illegible]	[illegible]	Alta	Diario	[illegible]		1 PC conectada a la HP 3000	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	Alta	Diario	[illegible]		1 PC conectada a la HP 3000	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	Alta	Diario	[illegible]		1 PC conectada a la HP 3000 Reportes de captura en sucursales	[illegible]	Sucursales [illegible]	[illegible]		[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	Alta	[illegible]	[illegible]		1 PC conectada a la HP 3000 Reportes de captura en sucursales	[illegible]	Sucursales [illegible]	[illegible]				

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX. SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
[illegible]	[illegible]	Alta	Diario	Horas y días hábiles		[illegible]	Ninguno	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	Alta	Diario	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]
[illegible]	[illegible]		[illegible]	[illegible]		[illegible]	Ninguno	[illegible]	[illegible]		[illegible]	[illegible]	
[illegible]	[illegible]	Alta	[illegible]	Horas y días hábiles		Terminales y [illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]

CENTRO COMERCIAL S.A. DE C.V.

ENCUESTA PARA DEPARTAMENTOS ADMINISTRATIVOS

DEPARTAMENTO: COMPRAS.

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX. SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
[illegible]	[illegible]	Alta [illegible] Media (mercaderias)	Diario	Nocturno		[illegible] HP-3000/902	30 min	[illegible]		Proceso batch	[illegible]	Misma Area	[illegible]
	[illegible]	Alta [illegible] Media (mercaderias)	Diario	Diario (despues de las 17:30 hrs)		1 terminal [illegible] a la HP-3000/910	5 hrs	[illegible]		Proceso batch	[illegible] de datos [illegible] INGRES	[illegible] etc.	[illegible]

DEPARTAMENTO: MERCADERIAS.

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
[illegible]	[illegible]	Alta	Diario	Nocturno	[illegible] y el marzo [illegible] de cada mes		1 Semana	Mercaderias y sucursales	[illegible]	Proceso batch	Actualizacion en base de [illegible] cuentas [illegible]	Contabilidad	
[illegible]	Cheques [illegible]	Alta	Semanal (miercoles)	Nocturno	Todos los meses [illegible] y el marzo [illegible] de cada mes	[illegible]	1 Semana	[illegible]	[illegible]	Proceso batch	Cheques [illegible]	[illegible] general [illegible]	
[illegible]	Cheques [illegible]	Alta	Semanal (miercoles)	Nocturno	Todos los meses son criticos y el marzo [illegible] de cada mes	[illegible]	[illegible]	[illegible]	[illegible]	Proceso batch	Cheques [illegible]	[illegible] general [illegible]	

Nota: Todas las aplicaciones se necesitan : 1 Persona, 1 Terminal , 1 PC conectada a la HP-3000/902

CENTRO COMERCIAL S.A. DE C.V.

ENCUESTA PARA DEPARTAMENTOS ADMINISTRATIVOS

DEPARTAMENTO: RECURSOS HUMANOS.

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
[illegible]	[illegible]	Alta	[illegible]	[illegible]	Dias criticos		48 Hrs	[illegible]	[illegible]	[illegible]	Nomina Calculada	[illegible]	[illegible]
	[illegible]				[illegible] 23 de cada mes				[illegible]	[illegible]		[illegible]	[illegible]
								[illegible]	Fondo de bancos				[illegible]
									[illegible]				[illegible]
[illegible]	[illegible]	Alta	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	IMSS	[illegible]
y SAR	[illegible]				[illegible]				[illegible]	y del SAR	[illegible]		[illegible]
	[illegible]				[illegible]						[illegible]		
	[illegible]	[illegible]	[illegible]	[illegible]	y Diciembre		1 Dia	[illegible]	[illegible]	[illegible]	Consultas	[illegible]	
	[illegible]				Dias criticos			[illegible]	[illegible]				
					[illegible]				[illegible]				

Nota: Se necesitan 2 personas, 2 terminales, lapices y escritorio

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
[illegible]	Representacion		[illegible]			PC (Excel) [illegible]	[illegible]				Reporte		
[illegible]	[illegible]					[illegible]							
[illegible]	[illegible]												
[illegible]	[illegible]												
	[illegible]												
[illegible]	[illegible]		Eventual			[illegible]	1 Mes				[illegible]		
[illegible]	[illegible]					[illegible]					[illegible]		
	[illegible]												
	[illegible]												
	[illegible]												
[illegible]	[illegible]		[illegible]			[illegible]					[illegible]		
[illegible]	[illegible]					[illegible]							
	[illegible]					[illegible]							
[illegible]	[illegible]		Eventual			[illegible]	[illegible]				[illegible]		
[illegible]	[illegible]					[illegible]					[illegible]		
[illegible]	[illegible]												
	[illegible]												

CENTRO COMERCIAL S.A. DE C.V.

ENCUESTA PARA DEPARTAMENTOS ADMINISTRATIVOS

DEPARTAMENTO: RECURSOS HUMANOS.

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX. SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
[illegible]	[illegible]		[illegible]			1 PC[illegible]	2 Meses				Respaldo en disco		
[illegible]	[illegible]		[illegible]			1 PC[illegible]	1 Semestre				Reporte, respaldo en [illegible]		
[illegible]	[illegible]		[illegible]			1 PC[illegible]	10 días				[illegible]		
[illegible]	[illegible]		[illegible]			1 PC[illegible]	[illegible]				Reporte [illegible] en disco		

APLICACION	DESCRIPCION	PRIORIDAD	FRECUENCIA	HORARIO	MESES Y DIAS CRITICOS	NECESIDAD	TIEMPO MAX. SIN OPERAR	AREA DE LA QUE DEPENDE	INFORMACION REQUERIDA	EJECUCION	INFORMACION GENERADA	USUARIOS FINALES	PROCESO OPCIONAL
[illegible]	[illegible]		[illegible]			[illegible]					Reporte [illegible] en disco		
[illegible]	[illegible]					1 PC[illegible]	20 días				Reporte [illegible]		
[illegible]	[illegible]		[illegible]			1 PC[illegible]	20 días				Reporte [illegible]		
[illegible]	[illegible]		[illegible]			1 PC[illegible]	8 días				[illegible]		
[illegible]	[illegible]		[illegible]			1 PC[illegible]	[illegible]				[illegible] en disco		
[illegible]	[illegible]		[illegible]			1 PC[illegible]	8 días				Reporte [illegible] en disco		

CENTRO COMERCIAL S.A. DE C.V.

ENCUESTA PARA INFORMATICA.

SISTEMA: MERCADERIAS

DIRECTORIO DE PROCESOS CRITICOS

NOMBRE	DESCRIPCION	PERIO-DO	PRIORI-DAD	RESPONSA-BLE EJEC.	PROC. PREV.	RE-PROC.
CPJB2246	Respaldo del archivo CBMD0020					
	MERCAD INTERFAS para Reproceso de					
	Cheques y vouchers					
CPJB232A	Reproceso de Letras					
CPJB234A	Respaldo del archivo APMD0501					
	MERCAD INTERFAS para reproceso de L					
ESJB1000	Genera concentrado de Compras			USUARIO		
	Devoluciones y Cambios de Precio					
ESJB2000	Reporte de Proveedores más Importantes			USUARIO		
	por división					
ESJB3110	Depuración anual estadística de artículos					
ESJB3120	Depuracion anual estadística de compras					
ESJB4100	Estadísticas por artículo por división					
ESJB4200	Estadísticas por artículo por familia					
ESJB4300	Estadísticas por artículo por línea					
ESJB4400	Estadísticas por artículo por artículo					
ESJB700	Reporte de Proveedores con IVA					
ESJB8100	Estado de Resultados por Proveedor					
PPJB3000	Actualización de Precios Programados			USUARIO		
PPJB3010	Graba Cambios de Precio de Artículos			USUARIO		
	con Precio Programados					
PPJB4020	Carga Ventas diarias de Precios Progr					
PPJB8010	Reporet Mensual de Ventas con Precios					
	Programados					
PPJB8030	Reporte Mensual de Rotación de					
	Inventarios					
TIJB0010	Emisión de Estadística de Cambios de			USUARIO		
	Precio					
TIJB0020	Emisión de Estadística de Compras y			USUARIO		
	Devoluciones					
TIJB1600	Reporte de Folios Progresivos del módulo			USUARIO		
	de tiendas					

CENTRO COMERCIAL S.A. DE C.V.

ENCUESTA PARA INFORMATICA.

SISTEMA: MERCADERIAS

DIRECTORIO DE PROCESOS CRITICOS

NOMBRE	DESCRIPCION	PERIO-DO	PRIORI-DAD	RESPONSA-BLE EJEC.	PROC. PREV.	RE-PROC.
CPJB2246	Respaldo del archivo CBMD0020					
	MERCAD INTERFAS para Reproceso de					
	Cheques y vouchers					
CPJB232A	Reproceso de Letras					
CPJB234A	Respaldo del archivo APMD0501					
	MERCAD INTERFAS para reproceso de L					
ESJB1000	Genera concentrado de Compras			USUARIO		
	Devoluciones y Cambios de Precio					
ESJB2000	Reporte de Proveedores más importantes			USUARIO		
	por división					
ESJB3110	Depuracion anual estadistica de articulos					
ESJB3120	Depuracion anual estadistica de compras					
ESJB4100	Estadisticas por articulo por división					
ESJB4200	Estadisticas por articulo por familia					
ESJB4300	Estadisticas por articulo por linea					
ESJB4400	Estadisticas por articulo por articulo					
ESJB700	Reporte de Proveedores con IVA					
ESJB8100	Estado de Resultados por Proveedor					
PPJB3000	Actualización de Precios Programados			USUARIO		
PPJB3010	Graba Cambios de Precio de Artículos			USUARIO		
	con Precio Programados					
PPJB4020	Carga Ventas diarias de Precios Progr					
PPJB8010	Reporte Mensual de Ventas con Precios					
	Programados					
PPJB8030	Reporte Mensual de Rotación de					
	Inventarios					
TIJB0010	Emisión de Estadistica de Cambios de			USUARIO		
	Precio					
TIJB0020	Emisión de Estadistica de Compras y			USUARIO		
	Devoluciones					
TIJB1600	Reporte de Folios Progresivos del módulo			USUARIO		
	de tiendas					

CENTRO COMERCIAL S.A. DE C.V.

ENCUESTA PARA INFORMATICA.

SISTEMA: MERCADERIAS

DIRECTORIO DE PROCESOS CRITICOS

NOMBRE	DESCRIPCION	PERIO-DO	PRIORI-DAD	RESPONSA-BLE E/SC.	PROC. PREV.	RE-PROC.
VEJB6300	Facturas de Ventas					
VEJB6400	Notas de Crédito por Devoluciones	E	M	USUARIO	NO	NO
VEJB6500	Notas de Crédito por Bonificación sobre	E	M	USUARIO	SI	NO
	Ventas con Talones de Empleados					
VEJB6600	Notas de Crédito por Bonificación al IVA					
VEJB7300	Reporte Semanal de Ventas Netas	E	M	USUARIO	NO	NO
VEJB8000	Contabilización de Ventas					
VEJB8100	Afectación Contable de Ventas					
VEJB8200	Contabilización de Devoluciones					
VEJB8300	Contabilización de Resumen por Cajera					
VEJB8400	Generación de Póliza contable de					
	Bonificación sobre Ventas					
VEJB8500	Contabilización de Recibo de Ingresos					
VEJB7400	Reporte Semanal para Compradores					
VEJB7501	Informe de Ventas Navideñas					
CPJB2240	Corrida y Emisión de Cheques y Vouchers	D	M	USUARIO	NO	SI
CPJB2320	Corrida y Emisión de Letras de Cambio	S	M	USUARIO	NO	SI
	y Vouchers Interface con Sist. Admvo.					
CPJB2250	Proceso de Letras no Negociables	S	M	USUARIO	NO	NO
	Interface con Apoyo a Proveedores.					
CPJB1530	Impresión de Arqueo de Ctas. por Pagar.					
CPJB1540	Impresion de Arqueo de Ctas. por Depto.					
CPJB1550	Impresión de Arqueo de Ctas. por Pagar					
	con Movimientos Pendientes de Pago.					
CPJB1600	Impresión de Cifras de Control y anticipos					
	otorgados.					
CPJB2220	Modificación Global de Fechas por apertura					
	de Tiendas. Reporte de facturas					
	Procesadas en la apertura.					
CPJB2245	Reproceso de Emisión de Cheques y					
	Vouchers					

CENTRO COMERCIAL S.A. DE C.V.

ENCUESTA PARA INFORMATICA.

SISTEMA: MERCADERIAS

DIRECTORIO DE PROCESOS CRITICOS

NOMBRE	DESCRIPCION	PERIO-DO	PRIORI-DAD	RESPONSA-BLE EJEC.	PROC. PREV.	RE-PROC.
PIJB1000	Cálculo de Documentos	D	M	USUARIO	NO	SI
PIJB3140	Generación de Registros de Archivos de	M	M	USUARIO	NO	SI
	Interface con Conciliaciones	M	M	USUARIO	NO	NO
PIJB3180	Respaida Archivo CMBD0020 para interface	M	M	USUARIO	NO	NO
	con Conciliaciones Bancarias					
PIJB1400	Reportes de Margen Diario	D	B	USUARIO	NO	NO
PIJB1600	Reporte de Cargos,Abonos y deferencias					
	de las Pólizas					
PIJB2200	Impresion de Hojas de Inventario					
PIJB2300	Reporte de Inventario Físico					
PIJB2500	Reporte de Folios Faltantes					
PIJB2600	Contabilización al Corte por Inventario					
PIJB2700	Reporte de Movimientos de existencias					
	por Inventario					
PIJB2800	Reporte de Merma Semestral					
PIJB3010	Cálculo para la Bonificación Especial	A	M	USUARIO	NO	NO
PIJB3050	Contabilización al cierre Mensual					
PIJB3140	Generación de Reistros en archivo de	A	M	USUARIO	NO	SI
	Interface con contabilidad					
PIJB3160	Balanza de Movimientos					
PIJB3180	Respaldo de Archivo CBMD0020 para					
	Interface con Conciliaciones Bancarias					
	en HP-3000/980					
PIJB4010	Reporte de Facturas Duplicadas					
PIJB4020	Rep de Cambios de Precio Duplicados					
PIJB4030	Proc. de Cambio de Precio mal Elaborados					
PIJB4040	Estadistica Mensual de Compras	E	M	USUARIO	NO	NO
	y Devoluciones					
PIJB4050	Reporte de Vencimineto Semanal de	E	M	USUARIO	SI	NO
	Facturas					
PIJB4074	Reporte de Documentos Pagados del Cierre	E	M	USUARIO	NO	NO
	del Mes para Aclaraciones					

CENTRO COMERCIAL S.A. DE C.V.

ENCUESTA PARA INFORMATICA.

SISTEMA : COMPRAS.

DIRECTORIO DE PROCESOS CRITICOS

NOMBRE	DESCRIPCION	PERIO-DO	PRIORI-DAD	RESPONSA-BLE EJEC.	PROC. PREV.	RE-PROC.
SCJB1500	Catalogo Alfanumérico de Proveedores	E	A	USUARIO	NO	SI
SCJB1600	Catálogo Numérico de Proveedores	E	A	USUARIO	NO	SI
SCJB1700	Catálogo Numérico de Proveedores	E	A	USUARIO	NO	SI
	que tengan L en PRO-DOCTO-PAGO					
SCJB1800	Catlg de Proveedores con Bonificación	E	A	USUARIO	NO	SI
SCJB1900	Rep de Proveedores de baja en el mes	E	A	USUARIO	NO	SI
SCJB3410	Impresion Diaria de Cambios de Precio	D	B	USUARIO	SI	SI
SCJB3510	Imp Selectiva de Cambios de Precio	D	A	USUARIO	SI	SI
SCJB4100	Impresion de Hojas de Catálogo y Pedido	D	A	USUARIO	SI	SI
	Normal de Servicios a Compras					
SCJB4160	Impresión Selectiva de Compras	E	A	USUARIO	SI	SI
SCJB4162	Impresión Selectiva de Compras Pedido	E	B	USUARIO	NO	SI
	Normal					
SCJB4190	Impresión Global de Compras	E	M	USUARIO	SI	NO
SCJB4310	Impresión Diaria de Tiendas y generación	D	M	USUARIO	SI	NO
	Automatica de Cambios de Precio					
SCJB4420	Ipresión Selectiva de Tiendas	E	A	USUARIO	SI	SI
SCJB4422	Impresión Selectiva de Tiendas Pedido	E	A	USUARIO	SI	SI
	Normal					
SCJB4460	Impresión Global de tiendas	E	B	USUARIO	SI	SI
SCJB4520	Relación de Documentos Cancelados	D	B	USUARIO	NO	NO
SCJB4600	Emisión de Artículos con Precio Oficial	E	A	USUARIO	SI	SI
	y Vigentes de la hoja de Catálogo y Pedido					
	Especial					
SCJB4640	Relación de Documentos Vigentes	E	A	USUARIO	SI	SI

CENTRO COMERCIAL S.A DE C.V.

ENCUESTA PARA INFORMATICA

SISTEMA: INFORMACION ESTRATEGICA A COMPRAS

DIRECTORIO DE PROCESOS CRITICOS

NOMBRE	DESCRIPCION	PERIO-DO	PRIORI-DAD	RESPONSA-BLE EJEC.	PROC. PREV.	RE-PROC.
PPJB5000	Carga de Ventas por Artic	D	M	USUARIO	SI	NO
ESPF8400	Genera Archivos para la	D	M	USUARIO	SI	SI
	diaria de Ingres					
PPJB5010	Carga de Ventas por Artic	D	M	USUARIO	SI	NO
ACUMDIAO	Acumulación en Ingres pa	D	M	USUARIO	SI	NO
	Tiendas-Articulos (HP3000/960)					

CENTRO COMERCIAL S.A DE C.V.

ENCUESTA PARA INFORMATICA

SISTEMA: RECIBO AUTONOMO Y PEDIDOS

DIRECTORIO DE PROCESOS CRITICOS

NOMBRE	DESCRIPCION	PERIO-DO	PRIORI-DAD	RESPONSA-BLE EJEC.	PROC. PREV.	RE-PROC.
TRJB9100	Integracion de Informacio	D	M	OPERADOR	NO	NO
	Autónomo a TIBD01					
	(Información recibida por linea)					
TRJB9101	Integración de Informacio	D	M	USUARIO	NO	NO
	Autónomo a TIBD01					
	(Informacion recibida por diskette)					
TRJB2000	Generación de Informacio	D	M	USUARIO	SI	NO
	Cambios de Precio ,Transferencias					
TPJB3100	Integración de Informacio	D	M	USUARIO	SI	NO
	a TIBD02					
TPJB2000	Generación de Informacio	D	M	USUARIO	SI	NO
	Catálogos (Prov. Deptos., Doctos)					
TPJB2130	Generación Diaria de Doc	D	M	USAURIO	SI	NO
	Cancelaciones					

CENTRO COMERCIAL S.A DE C.V

ENCUESTA PARA INFORMATICA

SISTEMA:	DOCTOS POR PAGAR Y COBRANZAS

DIRECTORIO DE PROCESOS CRITICOS

NOMBRE	DESCRIPCION	PERIO-DO	PRIORI-DAD	RESPONSA-BLE EJEC.	PROC. PREV.	RE-PROC.
DPJB4000	Integración de Documentos al Sistema	D	M	USUARIO	NO	NO
DPJB5100	Interface con Mercaderías para Doctos	S	M	USUARIO	NO	NO
	no descontados					
DPJB9000	Proceso de Recompra de Documentos	D	M	USUARIO	NO	NO
COJB1320	Documentos Vigentes	M	M	USUARIO	NO	NO
COJB2140	Interface a Contabilidad y conciliaciones	M	M	USUARIO	NO	NO
BAJB1100	Carga de Cheques Diaria al sistema de	D	M	USUARIO	NO	NO
	Bancos					
COKF1100	Mantenimiento Pagarés	D	M	USUARIO	NO	NO
COFK1200	Mantenimiento a cheques	D	M	USUARIO	NO	NO
COJB2100	Poliza Previa	D	M	USUARIO	NO	NO
COJB0900	Catalogo, Pagarés y Finiquitos	D	M	USUARIO	NO	NO
DPKE1000	Actualización de Doctos	S	M	USUARIO	NO	NO
DPJB3310	Arqueo	M	M	USUARIO	NO	NO
DPJB3710	Recompra	M	M	USUARIO	NO	NO
DPJB3700	Vencimiento de Recompra	M	M	USUARIO	NO	NO

CENTRO COMERCIAL S.A DE C.V

ENCUESTA PARA INFORMATICA

SISTEMA: ADMINISTRATIVOS(CONSUMOS INTERNOS)

DIRECTORIO DE PROCESOS CRITICOS

NOMBRE	DESCRIPCION	PERIO-DO	PRIORI-DAD	RESPONSA-BLE EJEC.	PROC. PREV.	RE-PROC.
CIJB1601	Cambio de Iguales por una fecha	M	B	USUARIO	NO	SI
	determinada					
CIJB2420	Previo de Cheques Semanales	S	M	USUARIO	NO	NO
CIJB2421	Previo de Cheques Diarios	D	M	USUARIO	NO	NO
CIJB242A	Previo de Cheques de Finiquitos	D	M	USUARIO	NO	NO
CIJB2430	Corrida de Cheques Semanal	S	M	USUARIO	SI	SI
CIJB2440	Corrida de Cheques Diarios	D	M	USUARIO	SI	SI
CIJB2450	Emisión de Cheques de Finiquitos	S	M	USUARIO	SI	SI
CIJB2491	Obtención de Pólizas no balanceadas	M	B	USUARIO	NO	NO
CIJB2495	Obtención de Pólizas sin cuenta en	M	B	USUARIO	NO	NO
	Contabilidad					
CIJB2500	Transferencia de Poliza Automatica	M	M	USUARIO	NO	SI
CIJB2520	Ajuste de Centavos	M	M	USUARIO	NO	NO
CIJB2020	Obtención de Honorarios para Contabilizar	M	M	USUARIO	SI	SI
CIJB2630	Comprobación de IVA	M	M	USUARIO	NO	NO
CIJB26-0	Comprobación de Honorarios	M	M	USUARIO	NO	NO
CIJB3121	Resumen Estadishco de Compras	M	M	USUARIO	NO	NO
CIJB3122	Declaración Mensual de Honorarios y	M	M	USUARIO	NO	SI
	Ventas					
CIJB3123	Declaración Mensual de IVA	M	M	USUARIO	NO	NO
CIJB3126	Movimientos Capturados por	M	B	USUARIO	NO	NO
	DET X FECHA					
CIJB3129	Estadistico de Compras por Periodo	M	M	USUARIO	NO	NO
CIJB3130	Estadistico de Cargos y Credito	M	M	USUARIO	NO	NO
CIJB3292	Declaración Anual de Honorarios	A	M	USUARIO	NO	NO
CIJB3460	Porrateo de Publicidad	M	M	USUARIO	SI	SI
CIJB3695	Activacion de Cambios de Precio	M	M	USUARIO	NO	SI
CIJB4000	Generacion de Pagos AGUA,TEL,LUZ	S	M	USUARIO	NO	SI
CIJB4900	Obtención de Ventas Netas de Contabilidad	S	M	USUARIO	NO	NO
CIJB5000	Generación de Pagos de Rentas	S	M	USUARIO	NO	NO
CIJB8110	Carga de Informacion de gastos reportados	D	M	USUARIO	NO	NO
	a nivel directivo					

CENTRO COMERCIAL S.A DE C.V

ENCUESTA PARA INFORMATICA

SISTEMA:	CONCILIACIONES BANCARIAS
	BANCOS (PC-FINANZAS).

DIRECTORIO DE PROCESOS CRITICOS

NOMBRE	DESCRIPCION	PERIO-DO	PRIORI-DAD	RESPONSA-BLE EJEC.	PROC. PREV.	RE-PROC.
CBJB2110	Carga de Cheques Diario	D	M	USUARIO	SI	NO
CBJB4100	Conciliacion de Movimientos Diarios	D	M	USUARIO	SI	SI
CBJB4110	Restauración de Información de la	E	M	USUARIO	NO	NO
	Conciliación					
CBJB1500	Transmisión de Estado de Cuenta del	D	M	USUARIO	NO	NO
	Banco (PC)					
CBKF3100	Captura Fichas de Depósito	D	M	USUARIO	NO	NO
CBKF3120	Captura Fichas de Depósito con %	D	M	USUARIO	NO	NO
CBKF6100	Captura de Movtos Control Bancario.	O	M	USUARIO	NO	NO
CBKF6200	Captura de Movtos Control Bancario (Esp)	D	M	USUARIO	NO	NO
PC						
BAJB1100 BAT	Carga de Cheques HP3000 a PC	D	M	USUARIO	NO	NO
BAPF1200 FOX	Carga de Cheques a Bases de Datos	D	M	USUARIO	NO	NO
BAPF1500 FOX	Interface a Movto. diario de Bancos.	D	M	USUARIO	NO	NO
BAJB1300 BAT	Carga de Cheques entregados a PC	D	M	USUARIO	NO	NO
BAPF1400 FOX	Actualización de cheques entregados	D	M	USUARIO	NO	NO
BAKF2100 FOX	Captura de Conceptos (No entregados)	O	M	USUARIO	NO	NO
BAKF2200 FOX	Captura de Conceptos (Entregados)	D	M	USUARIO	NO	NO
BAKF2300 FOX	Captura manual de Cheques Entregados	E	M	USUARIO	NO	NO
BAZF3400 FOX	Importes totales de Cheques Entregados	D	M	USUARIO	NO	NO
BAZF3800 FOX	Existencia de Cheques en Ventanilla	S	M	USUARIO	NO	NO
BAKF4000 FOX	Todo el módulo de cobro de cheques	D	M	USUARIO	NO	NO
BAZF5400 FOX	Estadística por Proveedor	D	M	USUARIO	NO	NO
BAPF6100 FOX	Inicio del siguiente Cierre	D	M	USUARIO	NO	NO

CENTRO COMERCIAL S.A DE C.V

ENCUESTA PARA INFORMATICA

SISTEMA: NOMINA DE POLICIAS

DIRECTORIO DE PROCESOS CRITICOS

NOMBRE	DESCRIPCION	PERIO-DO	PRIORI-DAD	RESPONSA-BLE EJEC.	PROC. PREV.	RE-PROC.
NPJB1800	Finiquitos	D	M	USUARIO	SI	
NPJB2000	Aumentos Generales	D	M	USUARIO	SI	
NPJB2200	Nómina Normal Previa	Q	M	USUARIO	SI	
NPJB2400	Nómina Adicional Previa	Q	M	USUARIO	SI	
NPJB2500	Nómina Normal Definitiva	Q	M	USUARIO	SI	
NPJB2600	Nómina Adicional Definitiva	Q	M	USUARIO	SI	
NPJB3100	Impresión de Altas	Q	M	USUARIO	SI	
NPJB3600	Impresión de Altas	Q	M	USUARIO	SI	
NPJB3800	Saldos de Vacaciones	Q	M	USUARIO	SI	

CENTRO COMERCIAL S.A DE C.V

ENCUESTA PARA INFORMATICA

SISTEMA:	NOMINA

DIRECTORIO DE PROCESOS CRITICOS

NOMBRE	DESCRIPCION	PERIO-DO	PRIORI-DAD	RESPONSA-BLE EJEC.	PROC. PREV.	RE-PROC.
PEJB3200	Cálculo de nómina normal	Q	M	USUARIO	SI	NO
PEJB3300	Cálculo de Nómina Adicional	Q	M	USUARIO	SI	NO
PEJB4100	Contabilización	M	M	USUARIO	NO	NO
PEJB5110	Declaración Bimestral del IMSS	B	B	USUARIO	NO	NO
PEJB5130	Reproceso de Declaración del IMSS	B	B	USUARIO	NO	SI
PEJB2200	Finiquitos	D	M	USUARIO	NO	NO
PEJB5610	Declaración Bimestral S.A.R.	B	B	USUARIO	NO	NO
PEJB5630	Reproceso de Declaración del S.A.R.	B	B	USUARIO	NO	NO
PEJB4700	Capitalización Trimestral Caja de Ahorro.	T	B	USUARIO	NO	NO
PEJB6310	Liquidacion de Caja de Ahorro	A	B	USUARIO	NO	
PEJB4200	Estados de Cuenta Créditos FONACOT	M	B	USUARIO	NO	
PEJB4800	Estados de Cuenta Créditos INFONAVIT	M	B	USUARIO	NO	
PEJB5300	Cálculo de Variabilidad.	B	M	USUARIO	NO	
PEJB5500	Generación de Cintas de Variabilidad	B	M	USUARIO	SI	
PEJB2910	Generación de Cheques	D	M	USUARIO	SI	
PEJB2920	Generación de Ordenes de Pago	D	M	USUARIO	SI	
PEJB2140	Proceso de Modificación de Sueldos	D	B	USUARIO	ND	
PEJB2150	Proceso de Modificación de Sueldos	D	B	USUARIO	SI	
PEJB2160	Proceso de Modificación de Sueldos	D	B	USUARIO	SI	
PEJB7740	Calculo mensual de incentivos	M	M	USUARIO	NO	
PEJB4120	Proceso de Acumulados	M	A	USUARIO	SI	
PEJB4300	Estado de cuenta de Caja de Ahorro	M	B	USUARIO	NO	
	y Prestamos					
PEKF2110	Captura de Altas	D	M	USUARIO	NO	
PEKF2120	Captura de Movimientos Quincenales	D	M	USUARIO	NO	
PEKF2210	Captura de Bajas	D	M	USUARIO	NO	
PEKF2810	Captura de Deudores Diversos	D	A	USUARIO	NO	
PEKF2700	Captura de Percepciones Adicionales	D	M	USUARIO	NO	
PEJB8010	Documentación de Altas	D	M	USUARIO	NO	

CENTRO COMERCIAL S.A DE C.V

ENCUESTA PARA INFORMATICA

SISTEMA:	NOMINA

DIRECTORIO DE PROCESOS CRITICOS

NOMBRE	DESCRIPCION	PERIO-DO	PRIORI-DAD	RESPONSA-BLE EJEC.	PROC. PREV.	RE-PROC.
PEJB3000	Cálculo de nómina normal	Q	M	USUARIO	SI	NO
PEJB3000	Cálculo de Nómina Adicional	Q	M	USUARIO	SI	NO
PEJB4100	Contabilización	M	M	USUARID	NO	NO
PEJB5110	Declaración Bimestral del IMSS	B	B	USUARID	NO	NO
PEJB5130	Reproceso de Declaración del IMSS	B	B	USUARID	NO	SI
PEJB2230	Finiquitos	D	M	USUARIO	NO	ND
PEJB5610	Declaración Bimestral S.A.R.	B	B	USUARIO	ND	NO
PEJB5630	Reproceso de Declaracion del S.A.R.	B	B	USUARIO	NO	NO
PEJB4700	Capitalización Trimestral Caja de Ahorro	T	B	USUARID	ND	NO
PEJB6310	Liquidación de Caja de Ahorro	A	B	USUARIO	ND	
PEJB4200	Estados de Cuenta Créditos FONACOT	M	B	USUARIO	ND	
PEJB4800	Estados de Cuenta Créditos INFONAVIT	M	B	USUARIO	NO	
PEJB5300	Cálculo de Variabilidad	B	M	USUARIO	NO	
PEJB5600	Generación de Cintas de Variabilidad	B	M	USUARID	SI	
PEJB2910	Generación de Cheques	D	M	USUARIO	SI	
PEJB2920	Generación de Ordenes de Pago	D	M	USUARIO	SI	
PEJB2140	Proceso de Modificación de Sueldos	D	B	USUARIO	NO	
PEJB2150	Proceso de Modificación de Sueldos	D	B	USUARIO	SI	
PEJB2160	Proceso de Modificación de Sueldos	D	B	USUARID	SI	
PEJB7740	Cálculo mensual de incentivos	M	M	USUARID	ND	
PEJB4130	Proceso de Acumulados	M	A	USUARID	SI	
PEJB4300	Estado de cuenta de Caja de Ahorro y Préstamos	M	B	USUARIO	NO	
PEKF2110	Captura de Altas	D	M	USUARIO	NO	
PEKF2120	Captura de Movimientos Quincenales	D	M	USUARIO	ND	
PEKF2210	Captura de Bajas	D	M	USUARIO	NO	
PEKF2810	Captura de Deudores Diversos	D	A	USUARIO	NO	
PEKF2700	Captura de Percepciones Adicionales	D	M	USUARIO	NO	
PEJB8010	Documentación de Altas	O	M	USUARID	ND	

Como se mencionó anteriormente, el área Centro de cómputo y Soporte Técnico es de vital importancia para la empresa, por lo que se consideró realizar un análisis profundo de ésta.

Para poder realizar este análisis se consideraron los siguientes procedimientos estratégicos, que permiten saber que tan protegida está la información:

- Condiciones de Seguridad en el Centro de cómputo.
- Seguridad en el acceso a la información.
- Calendarización de Respaldos.

A continuación se explica cada una de ellas:

Condiciones de Seguridad en el Centro de cómputo

La seguridad de la información es el cumplimiento de actividades y mantenimiento de las condiciones en que se maneja la información, garantizando la seguridad, respaldo y confidencialidad de la misma. Las condiciones de seguridad las dividimos en Físicas y Lógicas.

- Condiciones Físicas

El Centro de cómputo cuenta con piso falso, que al ser evaluado se encontró que la resistencia eléctrica transversal del recubrimiento del piso falso estaba dañado y por lo tanto no evitaba las cargas electrostáticas.

Las condiciones para mantener la temperatura no son suficientes para conservar el equipo en un medio apropiado de humedad y temperatura, esto ocasiona fallas en una minicomputadora, generando una interrupción.

Las demás instalaciones de aire acondicionado, instalaciones eléctricas, temperatura ambiental del Centro de cómputo se encuentran en condiciones aceptables.

Con respecto al mantenimiento de los equipos y periféricos, estos se realizan dos veces por año. Por otro lado se lleva un inventario de los mismos, donde se registran la descripción del equipo, número de serie y cantidad.

- Condiciones Lógicas

Para las actualizaciones del Sistema Operativo y agregar nuevas aplicaciones, se tienen bitácoras de las actualizaciones, esto es para llevar un control interno y poder saber con que software se cuenta. En este punto observamos que el responsable para estas actualizaciones no es único, por lo cual puede causar graves problemas, por ejemplo doble instalación de un producto, ocasionando pérdida de tiempo; mala instalación del sistema operativo, para ello es

necesario conocer ciertas configuraciones e información para la instalación o actualización del mismo.

Los programas donde se encuentran la configuración son :

NMMGR

En este programa se encuentra toda la configuración de la minicomputadora HP-3000. Se encuentra configurados todos los periféricos como impresoras, modems, DTC's y otras computadoras .

SYSGEN

En éste se da de alta todos los paths que identifica los discos, periféricos y terminales. Estos dos programas en conjunto, si están bien configurados, permiten que el sistema trabaje correctamente, de lo contrario puede ocasionar serios problemas.

También existen otras utilerías para diagnosticar si el hardware se encuentra en buen estado, éstas solamente son utilizadas por personal de Soporte Externo, es decir, los ingenieros de mantenimiento.

Seguridad en el acceso a la información

Se mencionó que es muy importante este aspecto, ya que puede ocasionar pérdidas de información, por lo qua llevar un control en el acceso a los diferentes sistemas no está por demás.

Para el caso del Centro Comercial, la seguridad que se lleva es la siguiente :

Para accesar alguna cuenta , tanto de producción y/o desarrollo, es necesario que el administrador del Centro de cómputo dé de alta al usuario con una justificación para su acceso. En este momento el usuario se hace responsable del buen o mal uso de la clave de acceso.

Para la calendarización de procesos (jobs), el administrador debe estar enterado de que procesos serán ejecutados manual o automáticamente. Para el caso en que su ejecución sea manual deberán apuntarlos en una hoja de procesos, donde se registra el número que identifica al proceso, nombre , hora de ejecución y quién es el responsable. Para los automáticos sólo será necesario que se registren una sola vez y el administrador da instrucciones al operador para que estos procesos realmente se ejecuten correctamente. Los operadores deben entregar todos los reportes generados por cada proceso, además, deberán entregarlos a la persona que firmó de responsable; en caso de que el proceso termine mal, se deberá avisar al personal asignado en el área de desarrollo y al responsable administrativo, para que encuentren el problema y lo solucionen.

necesario conocer ciertas configuraciones e información para la instalación o actualización del mismo.

Los programas donde se encuentran la configuración son :

NMMGR

En este programa se encuentra toda la configuración de la minicomputadora HP-3000. Se encuentra configurados todos los periféricos como impresoras, modems, DTC's y otras computadoras .

SYSGEN

En éste se da de alta todos los paths que identifica los discos, periféricos y terminales. Estos dos programas en conjunto, si están bien configurados, permiten que el sistema trabaje correctamente, de lo contrario puede ocasionar serios problemas.

También existen otras utilerías para diagnosticar si el hardware se encuentra en buen estado, éstas solamente son utilizadas por personal de Soporte Externo, es decir, los ingenieros de mantenimiento.

Seguridad en el acceso a la información

Se mencionó que es muy importante este aspecto, ya que puede ocasionar pérdidas de información, por lo qua llevar un control en el acceso a los diferentes sistemas no está por demás.

Para el caso del Centro Comercial, la seguridad que se lleva es la siguiente :

Para accesar alguna cuenta , tanto de producción y/o desarrollo, es necesario que el administrador del Centro de cómputo dé de alta al usuario con una justificación para su acceso. En este momento el usuario se hace responsable del buen o mal uso de la clave de acceso.

Para la calendarización de procesos (jobs), el administrador debe estar enterado de que procesos serán ejecutados manual o automáticamente. Para el caso en que su ejecución sea manual deberán apuntarlos en una hoja de procesos, donde se registra el número que identifica al proceso, nombre , hora de ejecución y quién es el responsable. Para los automáticos sólo será necesario que se registren una sola vez y el administrador da instrucciones al operador para que estos procesos realmente se ejecuten correctamente. Los operadores deben entregar todos los reportes generados por cada proceso, además, deberán entregarlos a la persona que firmó de responsable; en caso de que el proceso termine mal, se deberá avisar al personal asignado en el área de desarrollo y al responsable administrativo, para que encuentren el problema y lo solucionen.

Calendarización de Respaldos

La calendarización de respaldos es importante para cualquier tipo de contingencia, ya que ello impide la pérdida de días de trabajo, de lo contrario habrá grandes pérdidas en cuestión de costos.

Los respaldos que se realizan en el Centro Comercial se llevan a cabo de la siguiente manera :

- Se realizan respaldos totales cada mes.
- Respaldos semanales y
- Respaldos parciales (diarios).

Todos los respaldos son internos y no cuentan con respaldos externos.

Realmente, estos son los puntos más importantes dentro de esta área, pero se necesita tener una buena administración y responsabilidad para lograrlo.

Del análisis efectuado nos dimos cuenta de la problemática que existe para el buen mantenimiento del Centro de cómputo, no depende directamente del responsable del área, sino también del apoyo proporcionado por la dirección para realizar cambios y/o nuevas adquisiciones de materiales y equipos, y por ende dar un buen servicio a los usuarios y poder tener una buena posición en el mercado, es decir, si se tiene una buena administración se puede garantizar un gran éxito para la empresa.

5. ELABORACION E IMPLANTANCION DEL PLAN DE SEGURIDAD DE INFORMACION

Debido a que cada día las empresas presentan una mayor dependencia de los equipos de cómputo y de comunicaciones, y al peligro de una interrupción en el procesamiento normal de la información, es importante que las empresas de hoy en día se preparen y planeen los procedimientos a seguir en caso de un desastre, por lo que es recomendable que la propia organización desarrolle un plan de seguridad de información.

Para desarrollar un plan de seguridad e información es necesario que exista un departamento coordinador del mismo. Dicho departamento debe encargarse de la elaboración, la implantación, la evaluación de los resultados y el mantenimiento del plan. Dicho plan deberá ser definido de tal manera para que se adecue a las características de operación de la organización.

El departamento que se encargará de la coordinación del plan será el de informática o alguien de ese departamento, ya que aquí es donde se encuentra el equipo en donde se almacena y procesa la información y por lo tanto toda la continuidad de la operación de los procedimientos van a depender de la disponibilidad del equipo de cómputo que se maneja, y de los respaldos de la información que se tengan. Para ello es importante que se cuente con personal capacitado para coordinar el desarrollo de dicho plan de seguridad.

El desarrollo del plan de seguridad de la información es un compromiso importante que requiere de un tiempo considerable y de los esfuerzos coordinados de varias personas; con la finalidad es la de contar con una guía para la restauración rápida y uniforme de las operaciones de cómputo, después de una interrupción de éstas. El plan de seguridad debe especificar las técnicas, métodos y alcances de las acciones a seguir para restablecer el funcionamiento del Centro Comercial.

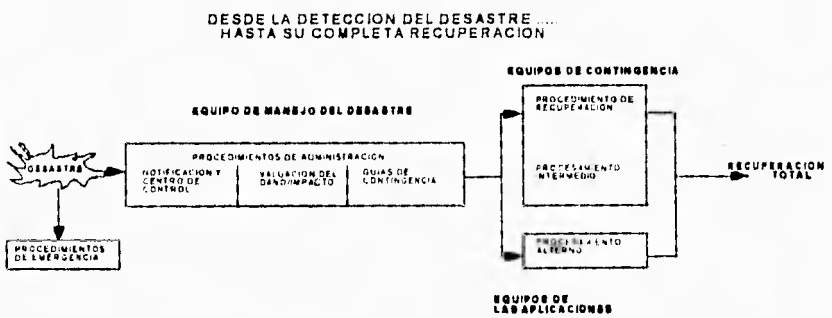


Figura 5.1 Secuencia de eventos que siguen a un Desastre

En la figura 5.1 se presenta la secuencia de eventos que sigue a un desastre, desde la detección del mismo hasta su completa recuperación. La secuencia de las acciones, es la siguiente :

- Ocurre un desastre
- En caso necesario, son invocados de inmediato los procedimientos de emergencia para proteger las vidas y minimizar el daño.
- Al mismo tiempo, se le notifica al equipo de manejo de desastres y se reúne en un local anteriormente especificado.
- El equipo de manejo de desastres valúa el daño y evalúa su impacto. Considera diferentes alternativas de recuperación y emite una directiva.
- Los equipos de recuperación entran en acción para establecer el procesamiento intermedio para aplicaciones críticas, usando instalaciones de respaldo.
- Mientras tanto, los equipos de aplicaciones inician el procesamiento alterno de aplicaciones críticas usando procedimientos manuales, hasta que nuevamente esté disponible el procesamiento de cómputo.
- Tan pronto como se establezca el procesamiento intermedio, los equipos de recuperación tomarán las acciones necesarias para restaurar totalmente las operaciones normales.

Para el desarrollo del plan de seguridad de la información para el Centro Comercial, se evaluaron las metodologías de un plan de seguridad presentadas en el segundo capítulo y los resultados de las encuestas presentadas en el capítulo cuatro. Con base a esta información se determinaron las etapas que se deben tomar en cuenta para la realización de dicho plan:

1. Clasificación de la información
2. Identificación del personal.
3. Seguridad Física
4. Seguridad Lógica
5. Seguridad en Comunicación
6. Evaluación de Riesgos
7. Plan de Contingencias
8. Plan de recuperación

Para la elaboración de la metodología que se llevará a cabo en el Plan de Contingencias y en el Plan de Recuperación, se requiere de las seis primeras etapas. A continuación se definirán cada una de las etapas y las actividades a seguir en cada una de ellas.

5.1. Clasificación de la Información.

La clasificación de la información se llevó a cabo basándonos en los resultados obtenidos en las encuestas aplicadas en el capítulo IV, con la finalidad de identificar los diferentes niveles en las situaciones que presentan los procesos mencionadas a continuación.

A) Situaciones Críticas :

1. Procesar en otro Computador

Si los equipos del Centro de Cómputo llegarán a tener fallas irreversibles, será necesario migrar toda la información a un Centro de Cómputo Alterno, para poder realizar la recuperación de los procesos que son vitales para el Centro Comercial. Dentro de los principales procesos vitales tenemos:

- Cuentas por cobrar
- Cuentas por pagar
- Libro Mayor
- Control de inventarios
- Precios y facturación

2. Suspender el procesamiento de información y utilizar procedimientos alternos, requiriendo una recuperación posterior.

Estos procesos, tales como Nómina, Activos Fijos, Compras e Inventarios, son aquellos cuya recuperación inmediata no es necesaria, ya que se pueden realizar manualmente por el personal, sin tener una gran repercusión en la operación del Centro Comercial, pero una vez terminados estos, se deberá seguir a la recuperación de la información para continuar su procesamiento.

3. Suspender el procesamiento y utilizar procedimientos alternos, sin necesidad de recuperación posterior.

Estos procesos son aquellos cuya recuperación no es necesaria, ya que se podrá procesar en forma manual o ayudándose de procedimientos específicos de cada una de las siguientes áreas :

- Caja general
- Auditoría
- Transferencia de información de tiendas a oficinas generales

B) Situaciones no críticas

1. Suspender procedimiento, con necesidad de recuperación posterior.

Son aquellos procesos cuya recuperación no necesita procedimientos alternos y pueden esperar a que se restablezca una situación normal en el Centro de Cómputo para realizar su recuperación, tal es el caso de:

- Recursos humanos

- Inventarios
- Estadísticas por artículo

2. Suspender el procesamiento, sin necesidad de recuperación posterior.

Son los procesos que pueden no ser recuperados y , por lo tanto, no tienen relevancia dentro de la operación del Centro Comercial, los cuales son:

- Control de calidad
- Administración de impuestos

5.2. Identificación del Personal

Cuando se declara un desastre y durante las subsecuentes operaciones de recuperación, todos los Equipos de Recuperación de Desastre y otro personal del Centro Comercial deberán estar en contacto con el centro de control. En estos casos, las comunicaciones son muy críticas, cuando la primera necesidad es el rescate y el tiempo es esencial.

En esta etapa se debe identificar al coordinador o Comité Coordinador del plan de seguridad, el cual tendrá como función principal coordinar todos los aspectos referentes a su planeación, implementación y mantenimiento, así como también identificar al personal de las diferentes áreas del Centro Comercial que participarán en el plan.

La Dirección General deberá seleccionar al comité coordinador del Plan de Seguridad y para su selección se deberán considerar las siguientes características:

- Estar identificado con los objetivos del Centro Comercial.
- Habilidad para administrar proyectos a gran escala.
- Tener la autoridad para pedir la participación de los diferentes departamentos del Centro Comercial en el desarrollo e implantación del Plan de Seguridad.
- Tener contacto con todas las áreas operativas del Centro Comercial.
- Habilidad para manejar conflictos y tomar decisiones.

Considerando las caracteristicas anteriores se recomienda que el comité coordinador sea del Departamento de Informática, cuyas funciones generales serán:

- Formar equipos de trabajo para la implantación del Plan de Seguridad.
- Mantener la seguridad y la distribución correcta del Plan de Seguridad. Deberá establecer mecanismos de seguridad para mantener la seguridad del Plan y de las copias fotóstaticas que se obtengan del mismo. Así mismo distribuirá las copias necesarias al personal correspondiente del Centro Comercial.
- Contar con un fondo de emergencia en caso de desastre. Deberá definir el monto del fondo, y el lugar donde se va a localizar éste. Asi mismo, establecerá los

mecanismos necesarios para el control de dicho fondo y designará un responsable del mismo.

- Seleccionar el Centro de Soporte Alterno según requerimientos.
- Establecer el Centro de Recepción de documentos y control para el material, documentación y equipo requerido.
- Establecer canales y medios de comunicación interna y externa en caso de desastre. Deberá comunicar a los responsables de cada departamento del Centro Comercial y al personal clave de las misma, los canales y medios de comunicación que se utilizarán para comunicarse e informar sobre el desarrollo del Plan de Seguridad en caso de Desastre.
- Controlar los recursos del plan y su costo.
- Mantener comunicación continua con el personal relacionado con el Plan de Seguridad.

Para la realización de la clasificación de la información y para el desarrollo de las metodologías del plan de contingencias y el plan de recuperación se requiere de la participación del siguiente personal:

a) Alta Dirección del Centro Comercial
b) Personal directivo de cada uno de los departamentos
c) Personal de Informática
  - **Area de Sistemas**
  - **Area de Comunicaciones**
  - **Responsables de las Aplicaciones.**

d) Usuarios del sistema
e) Auditores internos
f) Personal de seguridad / incendios
g) Personal de Legal
h) Compras
i) Seguros
j) Bienes raices
k) Personal de transporte

Con la participación del personal anteriormente mencionado, se garantiza que dicho plan tenga una cobertura amplia en el proceso de recuperación de la operación de todo el Centro Comercial. Para ello, se requiere de la formación de equipos de trabajo, integrados de la siguiente manera:

Coordinador del plan de seguridad

Coordina las actividades de los equipos y asegura el cumplimiento de los horarios. Recibe y reporta el progreso de la recuperación y los problemas, entre otras. Investiga y reporta factores de origen, acciones de emergencia y esfuerzos de recuperación asociados con acontecimientos de desorganización.

Líder del equipo de administración

Contacta a los miembros del equipo de administración y comunica: realiza un reporte breve de la situación, ubicación del centro de control y la notificación de alerta para ayudar a la valuación del daño.

Procedimientos:

1. Recibir la notificación del desastre del Coordinador del Equipo de Recuperación.
2. Desarrollar la lista de Verificación.
3. Ayudar en la notificación de los otros líderes del equipo del plan de seguridad.
4. Ayudar al Coordinador del equipo de recuperación en la evaluación y selección de una alternativa de recuperación.
5. Verificar que las operaciones críticas estén ejecutándose en la instalación de respaldo.
6. Determinar el equipo de restauración.
7. Preparar el reporte de revisión del local.

Equipo de Administración

Este equipo es, generalmente, el proveedor de recursos para los miembros de los demás equipos para el manejo de desastres. Las responsabilidades incluyen transportación, seguridad, pólizas de seguro, dinero disponible para gastos, etc.

Miembros del equipo:
Gerencia de Recursos Humanos
Gerencia de Administración de Riesgos

Funciones del Equipo en caso de desastre:

- Recursos Humanos

a) Coordinar los servicios de mensajería entre el Centro de Cómputo, el local de almacenamiento externo y la instalación de respaldo.
b) Revisar el estado del personal durante el desastre, en caso de emergencia, avisar a familiares.
c) Contratar personal temporal o coordinar la transferencia de empleados de otros departamentos.
d) Establecer las relaciones públicas.
e) Preparación de publicaciones internas y externas en cuanto al desastre.

- Administración de Riesgos

a) Resguardar las áreas vitales con personal de seguridad según se requiera:
   - Centro de Cómputo

- Local de almacenamiento externo
- Instalación de respaldo
- Instalación de respaldo de la captura de datos
- Centro de control

b) Mantener unión con los departamentos de policía y bomberos.
c) Proteger los activos corporativos y los recursos humanos.
d) Contactar a la compañía de seguros que cubren activos fijos y seguros de vida.
e) Notificar a los servicios de mensajería el cambio de dirección.

Líder del equipo de recuperación de comunicaciones de datos

Responsabilidades: establecer comunicación de datos para los diferentes Equipos para la recuperación en caso de desastre; comunicar a los miembros del equipo la situación actual, la ubicación del centro de control y la notificación de alerta para ayudar a la valuación del daño para activar sus procedimientos de equipo.

Procedimientos del líder:

a) Conducir la valuación detallada del daño.
b) Ayudar al coordinador de recuperación en la evaluación y selección de alguna alternativa de restablecimiento.
c) Localizar a los distribuidores de cualquier equipo de cómputo que falle durante el período de recuperación.
d) Contactar al líder de grupo de usuarios para requerimientos de hardware y software.
e) Contactar al líder de recuperación de sistemas para asegurar que los requerimientos de hardware y software y de configuración hayan sido cubiertos.
f) Llamar al equipo de administración para que haga los gastos de reparación y reemplazo.
g) Llamar al equipo de recuperación de instalaciones para cualquier cableado adicional.

Procedimientos del equipo de recuperación de comunicación de datos:

a) Ayudar en la valuación detallada del daño.
b) Determinar la comunicación alterna de datos.
c) Activar los medio alternos de transmisión, interrupción de datos y de unidades de redes.
d) Revisar el estado de disponibilidad de usuarios y sistemas.

Líder de recuperación de instalaciones

Funciones:

a) Vigilar la valuación del daño físico de la planta, minimiza futuras pérdidas y salvar recursos recuperables.

b) Preparar y mantener las instalaciones de respaldo para el Centro de Cómputo.
c) Reparar las instalaciones dañadas y prepararlas para las operaciones de cómputo.
d) Coordinar los movimientos de y desde las instalaciones de respaldo.

Procedimientos para el líder de recuperación de instalaciones:

a) Conducir la valuación inicial del daño.
b) Ayudar en la notificación a otros líderes.
c) Ayudar al coordinar del equipo de recuperación en la evaluación y selección de una alternativa de restablecimiento.
d) Trabajar con el equipo de recuperación de sistemas para proporcionar el soporte físico necesario, para los requerimientos inmediatos de sistemas.

Procedimientos para el equipo de recuperación de instalaciones:

a) Conducir una valuación detallada del daño de instalaciones.
b) Estimar el tiempo de recuperación.
c) Registrar el estado de recuperación.
d) Revisar el estado de los servicios locales.
e) Desarrollar los requerimientos del Centro de Cómputo, en el caso de que éste no se pueda salvar.

Equipo del grupo de usuarios

Responsabilidades del Equipo del Grupo de Usuarios son:

a) Mantener la información actualizada con respecto a los recursos necesarios para las aplicaciones críticas de usuarios.
b) Proporcionar un enlace continuo de comunicaciones entre las ubicaciones de los usuarios y la instalación de respaldo.
c) Asegurar que los requerimientos de procesamiento y las prioridades, sean comunicadas al Equipo de Recuperación de Sistemas y a otros equipos, si se requiere.
d) Negociar las prioridades de procesamientos, tal y como se define en las políticas del Centro Comercial.

Miembros del Equipo:

- Líder del Equipo
- Representantes de Usuarios Locales y Remotos
- Soporte de Sistemas
- Programación de Sistemas
- Hardware del Sistema
- Gerentes de Sistemas

Funciones del Equipo en caso de desastre:

a) Obtener información sobre recuperación de aplicaciones críticas.
b) Localizar los datos disponibles y validar el estado de archivos.
c) Proporcionar, si se requiere, instrucciones en la reconstrucción de datos y archivos de transacción.
d) Reportar el estado de recuperación al representante de usuarios.
e) Evaluar el horario de producción, junto con el representante de usuarios y modificar las prioridades, en caso necesario.

Composición del Equipo del grupo de usuarios:

- Gerencia de mercaderías
- Gerencia de personal y finanzas
- Gerencia de contraloría

Alterno:

- Subgerencias y jefaturas de mercaderías
- Subgerencias y jefaturas de personal y finanzas
- Subgerencias y jefaturas de contraloría

Funciones del líder del equipo del grupo de usuarios:

a) El equipo se congrega en las instalaciones de respaldo.
b) Obtener la información sobre la recuperación de aplicaciones críticas.
c) Localizar los datos disponibles y validar el estado de archivos.
d) Reportar el estado de recuperación al representante de usuarios.
e) Evaluar el horario de producción, junto con el representante de usuarios y modificar las prioridades, en caso necesario.

Lista de Verificación de la notificación del líder del Equipo del grupo de usuarios:

a) Contactar a los miembros del equipo del grupo de usuarios para comunicarles:

- Explicación breve de la situación.
- Ubicación del centro de control.
- Notificación de alerta para ayudar en la valuación del daño y para activar los procedimientos del equipo.

Procedimientos del líder del equipo del grupo de usuarios:

a) Recibir la notificación del desastre, del gerente del equipo de recuperación.

b) Se reporta todas las operaciones al centro de control.
c) Desarrollar la lista de verificación de la notificación del líder del equipo de recuperación.
d) Conducir la valuación inicial del daño.
e) Ayudar en la notificación de los otros líderes del equipo de recuperación.
f) Atender a las juntas de la valuación del daño.
g) Si se activó el equipo, dar instrucciones a los miembros para que ejecuten los procedimientos del equipo de recuperación del grupo de usuarios.
h) Conducir la valuación detallada del daño.
i) Ayudar al coordinador del equipo de recuperación, a evaluar y seleccionar una alternativa de recuperación, basada en la valuación detallada.
j) Manejar la operación de recuperación del equipo.
k) Reportar el estado de recuperación al centro de control para anunciarlo en la tabla de avisos.
l) Remitir al personal del equipo del grupo de usuarios, a las instalaciones de respaldo y de usuario.
m) Mantener contacto con los representantes de los usuarios para mantenerlos informados del estado de recuperación.
n) Negociar la calendarización de procesamiento de prioridades y conflictos, con los ejecutivos del Centro Comercial.

Procedimientos del Equipo del grupo de usuarios:

Las siguientes actividades son las responsabilidades del Equipo del grupo de usuarios:

a) Se reúnen en el local convenido.

- Recibir la notificación del equipo de manejo de desastres.
- Se reporta al centro de control.
- Determinar el nivel del desastre y ayudar en la evaluación del daño, tal como lo soliciten los líderes y el coordinador del equipo de recuperación.
- Remitir al personal al local de respaldo.
- Identificar la magnitud de las necesidades requeridas por el soporte de usuarios.
- Remitir al personal de soporte a las instalaciones específicas de usuarios, locales/remotas.

b) Ayudar en la valuación detallada del daño

- Reportar los daños e impacto a los usuarios.
- Determinar el impacto a aplicaciones críticas.
- Desarrollar junto con los usuarios, el calendario de procesamiento de prioridades, de aplicaciones críticas actuales.
- Negociar, en caso necesario, la determinación de aplicaciones críticas con el comité ejecutivo.
- Transmitir los requerimientos del procesamiento de aplicaciones críticas, al equipo de recuperación de sistemas.

- Proporcionar al equipo de control de entrada/salida la lista del contenido de la caja de seguridad, para que saque lo necesario para el procesamiento de las aplicaciones criticas.

c) Visitar las instalaciones locales y/o remotas

- Aconsejar al gerente del equipo sobre cómo informar a la instalación local/remota de los usuarios.

d) Determinar el estado del procesamiento

- Identificar las actividades que estaban ejecutándose cuando ocurrió el desastre.
- Desarrollar el calendario de procesamiento intermedio.
- Desarrollar el calendario de restauración.
- Iniciar el procesamiento intermedio.
- Comenzar la recuperación de datos.
- Reanudar el calendario normal de producción.

Equipo de Recuperación de sistemas

La función principal del Equipo de Recuperación de Sistemas es la de asegurar la reanudación de los servicios de aplicaciones críticas, procurar los medios y recursos necesarios del local de almacenamiento fuera de la instalación y asegurar que haya suficiente personal disponible para la operación de la instalación de respaldo, después de un desastre en el Centro de Cómputo.

Funciones:

A. Soporte del Software del sistema.

a) Es necesario asegurar que la versión correcta del sistema operativo esté cargada.
   - Versión del sistema operativo.
   - Comunicación de datos.
   - Parches requeridos.

b) Iniciar la estructura aplicable de cuentas y software.
c) Identificar y cargar el software que se requiera ya sea propio o de externos.
d) Asegurar que el software de diagnóstico requerido esté disponible para la instalación del sistema.
e) Poner en marcha los parámetros necesarios de tablas del sistema.
f) Administrar los recursos del sistema.
g) Colas (Queues)
h) Espacio libre en disco.
i) Ajuste.

B. Soporte de Aplicaciones.

- Determinar las necesidades de los recursos del usuario.
- Coordinar los requerimientos de la calendarización de aplicaciones críticas.
- Ayudar en la recuperación de aplicaciones críticas.

C. Soporte del Hardware de sistemas.

- Identificar los requerimientos de hardware del Centro de Cómputo de respaldo.
- Asegurar que el equipo necesario esté disponible en el local externo (si es necesario revisar la lista de verificación de los requerimientos de hardware).
- Ejecutar la configuración del sistema.
- Trabajar junto con el ingeniero de soporte de hardware, para la instalación adecuada del sistema.
- Asegurar que las necesidades del entorno sean las adecuadas.
  - Aire acondicionado.
  - Energía eléctrica.
  - Planos del piso.

- Poner en marcha las terminales y comunicaciones de datos para las operaciones y soporte a usuarios.

D. Soporte de Operaciones.

- Proporcionar el soporte operacional requerido.
  - Restauración de archivos.
  - Verificar UDCs. (Archivos de Comandos).
  - Respaldos.
  - Solicitudes de cintas.
  - Procedimientos.
  - Mantener los parámetros adecuados de operación.

- Controlar los requerimientos de cintas.
  - Disponibilidad de cintas.
  - Sistema de manejo de cintas.
  - Proporcionar las cintas de respaldo.
  - Registro y etiquetación de cintas.

- Desempeñar el control de producción.
  - Secciones de planeación.
  - Programación de actividades.
  - Recuperación de aplicaciones cuando éstas abortan.
  - Documentación.

- Ejecutar las remisiones de sistemas.
  - Prioridades.

B. Soporte de Aplicaciones.

- Determinar las necesidades de los recursos del usuario.
- Coordinar los requerimientos de la calendarización de aplicaciones críticas.
- Ayudar en la recuperación de aplicaciones críticas.

C. Soporte del Hardware de sistemas.

- Identificar los requerimientos de hardware del Centro de Cómputo de respaldo.
- Asegurar que el equipo necesario esté disponible en el local externo (si es necesario revisar la lista de verificación de los requerimientos de hardware).
- Ejecutar la configuración del sistema.
- Trabajar junto con el ingeniero de soporte de hardware, para la instalación adecuada del sistema.
- Asegurar que las necesidades del entorno sean las adecuadas.
  - Aire acondicionado.
  - Energía eléctrica.
  - Planos del piso.

- Poner en marcha las terminales y comunicaciones de datos para las operaciones y soporte a usuarios.

D. Soporte de Operaciones.

- Proporcionar el soporte operacional requerido.
  - Restauración de archivos.
  - Verificar UDCs. (Archivos de Comandos).
  - Respaldos.
  - Solicitudes de cintas.
  - Procedimientos.
  - Mantener los parámetros adecuados de operación.

- Controlar los requerimientos de cintas.
  - Disponibilidad de cintas.
  - Sistema de manejo de cintas.
  - Proporcionar las cintas de respaldo.
  - Registro y etiquetación de cintas.

- Desempeñar el control de producción.
  - Secciones de planeación.
  - Programación de actividades.
  - Recuperación de aplicaciones cuando éstas abortan.
  - Documentación.

- Ejecutar las remisiones de sistemas.
  - Prioridades.

- Salidas.
- Administración del controlador de impresiones (spool).

Procedimientos del líder del equipo de recuperación de sistemas:

a) Recibir notificación del desastre del gerente del equipo de recuperación.
b) Reportar al centro de control.
c) Desarrollar la lista de verificación de la notificación del líder del equipo de recuperación.
d) Conducir la valuación inicial del daño.
e) Ayudar en la notificación de los otro líderes del equipo de recuperación.
f) Atender a las juntas de la valuación del daño.
g) Si se activó este equipo, dar instrucciones a los miembros, para que ejecuten los procedimientos del equipo de recuperación del grupo de usuarios.
h) Conducir la valuación detallada del daño.
i) Evaluar y seleccionar una alternativa de recuperación, basada en la valuación detallada del daño.
j) Manejar la operación de recuperación del equipo.
k) Reportar el estado de recuperación al centro de control, para anunciarlo en la tabla de avisos.
l) Se coordina con la operación para restaurar los respaldos.
m) Coordinar los requerimientos críticos de aplicaciones del grupo de usuarios.
n) Coordinar las necesidades de otros equipos.
   - Obtener los requerimientos de hardware y software del sistema, del equipo del grupo de usuarios.
   - Determinar las necesidades del entorno del sistema operativo.
   - Determinar el software de terceras partes y de utilerías necesarias.
   - Verificar que se tenga los respaldos con operación.
   - Obtener el horario de producción para ejecutar los procesos.
   - Verificar los consumibles y papelería con Centro de Cómputo.

o) Levantar el sistema, de acuerdo a los requerimientos.
   - Programar el arranque del sistema junto con el ingeniero de servicio y en caso necesario que este último le ayude.
   - Crear la estructura de cuentas.
   - Restaurar los niveles de software del sistema.
   - Instalar el software necesario de proveedores externos y utilerias
   - Restaurar los archivos de usuario.
   - Verificar consumibles y papelería con Centro de Cómputo.
   - Definir la seguridad adecuada en el sistema de recuperación.

p) Coordinar y asegurar el procesamiento de producción.
   - Junto con el equipo del grupo de usuarios, evaluar las aplicaciones con alta prioridad y determinar el horario de procesamiento.
   - Verificar el cumplimiento satisfactorio de cada actividad de producción.
   - Remitir las salidas del destino apropiado, vía operación y Centro de Cómputo.
   - Controlar los requerimientos de cintas.
   - Proporcionar asistencia de recuperación para aplicaciones especificas.

5.3. Seguridad Física

En esta etapa se revisan las medidas de seguridad física que contempla el Centro Comercial, con el propósito de identificar los posibles riesgos a los que puede estar expuesto el Centro de Cómputo y el Centro Comercial en general.

Las actividades generales a seguir en esta etapa son las siguientes:

1) Revisión de la seguridad física de la empresa. Se revisará las medidas de seguridad con las que cuenta el Centro Comercial con el propósito de medir la seguridad física del área incluyendo los siguientes aspectos:

- Localización del área y áreas circundantes de riesgo.
- Acceso al área.
- Sistema de control de acceso.
- Resistencia al fuego de las paredes.
- Equipo de detección de agua y fuego.
- Sistema de agua y Gas Halón.
- Resistencia al fuego de áreas circundantes.
- Procedimientos de mantenimiento de prueba.
- Planeación de la seguridad organizacional.

2) Revisión de la seguridad física del Centro de Cómputo. La revisión de la seguridad del Centro de Cómputo debe incluir los siguientes aspectos:

- Localización del área y áreas circundantes de riesgo.
- Controles de acceso.
- Protección contra desastres naturales.
- Exposición a incendios.
- Exposición a daños causados por agua.
- Instalación eléctrica.
- Aire acondicionado.
- Suficiencia y respaldo de la fuente de poder.
- Procedimientos de limpieza del Centro de Cómputo.
- Estado de la documentación de los procedimientos de los respaldos para Registros Vitales y Equipo de Cómputo.
- Cobertura del seguro.

5.4. Seguridad Lógica

La seguridad lógica establece políticas y procedimientos para el control de acceso a la información, por lo que las actividades generales que se realizarán en esta etapa son:

1) Revisión de la seguridad de los datos.

La revisión de la seguridad de los datos debe considerar la implementación de cualquier medida sofisticada de seguridad, así como las políticas de seguridad de la información establecidas por el Centro Comercial, dentro de las cuales tenemos:

a) Asignación y control de passwords.

Para los departamentos Administrativos se asignarán passwords:

- A nivel cuenta a través del sistema operativo
- Personales por un software externo (SECURITY /3000) para conectarse a la minicomputadora HP-3000.
- Individuales para accesar a los sistemas de aplicación a través de menús
- El acceso a las aplicaciones se hará por medio de menús y, por lo tanto, sólo pueden accesar la información que les compete y sin tener acceso al Sistema Operativo

Para el departamento de Informática se asignarán passwords:

- A nivel cuenta e individuales para accesar a las bases de datos, a las aplicaciones en mantenimiento y a todos los sistemas que estén en desarrollo.
- Los passwords serán establecidos en forma confidencial por el Administrador donde éstos serán a nivel sesión, usuario y cuenta.

Para todos los Departamentos el cambio de passwords será cada 30 días.

b) Revisión de las políticas y procedimientos de seguridad.

Las políticas establecidas por el Centro Comercial para la seguridad de información son:

- Se deberán justificar por escrito todas las creaciones de cuentas y sesiones.
- El mantenimiento y depuración de las bases de datos se deberá realizar una vez por mes.
- El mantenimiento a los equipos del Centro de Cómputo se deberán realizar dos veces por año.
- Cualquier cambio que se lleve acabo para las bases de datos se deberá notificar al administrador del Centro de Cómputo por escrito.
- Para cualquier actualización de software y/o sistema operativo, el administrador del Centro de Cómputo deberá notificarlo por escrito a todos los líderes de las diferentes áreas que conforman los departamentos.
- El acceso al Centro de Cómputo estará restringido a través de tarjetas magnéticas para el personal autorizado.
- Los respaldos de información se deberán efectuar diariamente, semanalmente y mensualmente.
- Se deberán realizar respaldos externos semanal y mensualmente.

- Se debe justificar por escrito cualquier actualización de información que realicen los diferentes departamentos al Administrador del Centro de Cómputo.

En esta etapa debe considerarse el desarrollo o la adquisición de un sistema de seguridad que no sólo incluya el acceso a equipos y aplicaciones sólo al personal autorizado, también control de password (longitud, expiración, automática, únicos passwords aleatorios, etc.), seguridad por terminal y/o puertos de acceso, encriptación de archivos, detección de posibles violadores, realización de respaldos diarios, etc. Ser cuidadoso con la creación, modificación y borrado de archivos por parte del usuario final y por el personal de desarrollo. Los aspectos anteriores también aplican para las computadoras personales y redes (LAN'S).

5.5. Seguridad en Comunicaciones

La Seguridad en Comunicaciones se enfoca a proteger la información transmitida a través de redes de comunicación mediante el control de acceso, por lo que debe tomar en cuenta aquellos ataques contra la información, donde estos no dependen de tener acceso físico a los archivos protegidos, es decir tanto voz como datos, así como el medio por el cual se realiza la comunicación: satélite, microondas, radio, líneas públicas y privadas,

Cuando sea detectada una situación de desastre por el Centro de Cómputo, y se identifiquen dañadas las instalaciones de comunicación de datos , el hardware y software se deberán corregir en la instalación local, si es el caso, o en las instalaciones remotas que pudieran comprenderse dentro de los servicios de transmisión que trabajan con operaciones comprendidas en la red LAN. En este caso, se seguirán los siguientes procedimientos de solución de problemas :

- Se notificará del problema al personal de operaciones de redes, el cual está encargado de solventar cualquier problema de un usuario de redes o de otro personal en el Centro de Cómputo.
- El personal de comunicación de datos tratará de identificar la categoría en la que cae el problema y después tomará la(s) acción(es) necesaria(s) ya sea para arreglar el problema o para involucrar al personal o distribuidores de los servicios del contrato.
- Si el problema persiste, se notificará al personal especializado en el hardware o software de comunicación de datos.
- Si se registra una falla en el procesador central , los cuales son mantenidos por el área de comunicaciones, se puede tratar de resolver ya sea usando una refacción por el mismo personal que intentará repararlo, siempre y cuando se prevea un tiempo aproximado de no más de dos horas para la restauración del sistema, y si se supone un periodo más prolongado de interrupción se deberá llamar al personal de servicio autorizado y trabajar en una unidad alterna.
- Si se registra una falla en los convertidores de los protocolos, que pudiera no sobrepasar dos horas de interrupción, se deberá contactar al distribuidor para que la repare, si se anticipa un periodo prolongado será necesario obtener una unidad de reemplazo.

- Si los controladores locales de las terminales, que son atendidos por el personal de comunicaciones, llegarán a descomponerse por más de dos horas, se deberá utilizar una central remota de refacción, que se encuentra contenida dentro de la misma caja del controlador, si se prevé un período prolongado se deberá notificar al distribuidor.
- El personal de comunicaciones será el encargado de trabajar, en conjunto con las instalaciones remotas de la red LAN, para la identificación de posibles componentes que llegarán a fallar en los servicios de transmisión, así como de revisar que el microcódigo para poder establecer comunicación con estas instalaciones esté cargado correctamente, si no es así el personal del Centro de Cómputo enviará una unidad nueva, que deberá tener en el almacén con previa anticipación, la unidad dañada se debe enviar de regreso al Centro de Cómputo para ser reparada.
- En caso de que los problemas de datos se identifiquen en los medios de transmisión, se deberá contar con un almacén con un número adecuado de refacciones de circuitos, modems y multiplexores.
- En caso de que se tenga fallas en el software de la central remota de la red LAN, y en el procesador principal de computadores, se tendrá que volver a cargar el componente que está fallando, haciendo pruebas para solucionar el problema. Se deberá también, de ser necesario, intentar resolverlo cambiando la versión o regenerando una configuración en particular o bien contactarse con el distribuidor.
- Si se tienen problemas con el software de datos desarrollado localmente en cada una de las instalaciones, se deberá consultar al personal de sistemas, el cual determinará las acciones apropiadas a tomar, como por ejemplo, respaldar una versión anterior o esperar una corrección.
- En caso de falla en la operación de transmisión de datos de las terminales remotas de la red LAN, el área de comunicaciones deberá coordinar los servicios para instalar los cables y circuitos necesarios para establecer el acceso remoto de los usuarios con el local de respaldo, de acuerdo con la lista de prioridades.
- Cuando se tengan problemas de acceso al sistema por las terminales, se deberá comunicar a cualquiera de las centrales remotas para verificar el estado de conexión del hardware o software de comunicaciones y ejecutar una prueba de principio a fin y también se deberán verificar las conexiones.
- Se deberá encargar también de corregir problemas que presenten los circuitos, modems y multiplexores que usen equipo de pruebas análogico/digital para las conexiones, emitiéndose al mismo tiempo los comandos de la consola del computador principal, para iniciar y detener el control de software de las líneas, controladores y terminales

5.6. Evaluación de Riesgos

Una de las etapas principales del Plan de Seguridad es la EVALUACIÓN DE RIESGOS en la que se debe cuantificar y detectar a que tipo de riesgos está expuesto el Centro Comercial. Realizar un estudio de costo-beneficio para reducir estos riesgos y cuales son las áreas más vulnerables, sin las cuales la empresa se derrumbaria; qué tan probable es que ocurran inundaciones, terremotos, tornados, huracanes, incendios, bombas, huelgas, sabotajes y descomposturas graves del hardware y software. Los propósitos de la evaluación de riesgos son:

- Identificar los riesgos que requieren atención de la gerencia.
- Ayudar a establecer prioridades para la evaluación, selección, adquisición e implementación de protecciones.
- Proveer información para el análisis costo-beneficio de protecciones.
- Proveer una base de auditorías y revisiones de seguridad.

En esta etapa se debe establecer y aplicar medidas adecuadas para reducir la probabilidad de ocurrencia de un siniestro y, de ocurrir, evitar que las actividades se interrumpan por tiempo indefinido, que los daños sean irreparables y que se repita el mismo siniestro.

Fases de la evaluación de riesgos:

- Identificación de activos.
- Estimar el valor de los activos.
- Identificar amenazas.
- Identificar vulnerabilidades.
- Calcular la pérdida asociada con el riesgo.

Factores a considerar:

1) PLAN.
   - Alcance y grado de detalle.
   - Puntos críticos.
   - Técnicas de administración de proyectos.
   - Metodología de evaluación de riesgos.
   - Recursos requeridos.
   -
2) ORGANIZACION
   - Grupo de trabajo.
   - Estándares a utilizar.
3) DIRECCION
   - Relacionar actividades con fechas.
4) CONTINUIDAD.
   - Monitoreo del progreso.
   - Reuniones de avance.

Para llevar a cabo la evaluación de riesgos es necesario realizar:

- Clasificación general de las instalaciones en términos de riesgo alto, medio y bajo.
- Identificación de las aplicaciones que constituyen riesgos altos.
- Cuantificación del impacto producido por la suspensión prolongada del procesamiento en las aplicaciones de alto riesgo.

- Formulación de las medidas necesarias para lograr un nivel de seguridad adecuado, es decir, en equilibrio con los niveles de riesgo.
- Justificación de las medidas de seguridad en cuanto al costo que representan.

5.7. Plan de Contingencias

Un plan de contingencia es un plan escrito en el que se detallan acciones, procedimientos y recursos que deben usarse durante un desastre que cause destrucción parcial o total de los servicios de cómputo. En este plan se definen qué tareas son críticas quién es el responsable de todos los aspectos del proceso de recuperación, y cómo va a funcionar la organización mientras los sistemas están siendo reparados o transportados a un nuevo local. Un plan de contingencia no duplica un entorno comercial (en forma inmediata), pero sí minimiza la pérdida potencial de activos y mantiene al Centro Comercial operando, al tomar acciones decisivas basadas en la planeación anticipada.

Este plan de contingencia completo mitigará los efectos de desastres desafortunados y permitirá una respuesta rápida, una transferencia del procesamiento crítico a otras instalaciones, y una eventual recuperación, de acuerdo al tiempo que de antemano se haya considerado para ello. El éxito de este plan estará en función del tiempo y del costo necesarios para restablecer la operación normal de los sistemas de cómputo. Incrementar la seguridad significa incrementar las posibilidades de salvaguardar los activos del Centro Comercial, reduciendo el riesgo de pérdida financiera. Estas medidas nunca pueden ser por sí mismas garantía contra daños y accidentes y por lo tanto deben de estar en armonía con todo el perfil y el medio ambiente del Centro Comercial. Aún así, un cierto grado de riesgo tendrá que ser aceptado. En este Plan de Contingencias se debe:

1) Organizar los proyectos y recursos de planeación necesarios para realizar un programa de recuperación de desastres.

La administración gerencial debe comprometerse a desarrollar el plan de contingencia en caso de desastre, de tal manera que los recursos necesarios puedan ser asignados al proyecto. Esto involucra la distribución de fondos y personal, incluyendo personal del procesamiento de datos, de apoyo, de planeación de seguridad, el de operaciones de cómputo, el personal de soporte y usuarios. La administración debe entender lo siguiente para considerar el desarrollo del plan:

- La pérdida del poder de cómputo puede significar una desorganización severa del Centro Comercial.
- Una suspensión prolongada es inaceptable.
- La recuperación no es automática.
- El restablecimiento no es fácil.
- El desarrollo y mantenimiento de un programa de recuperación de desastres es un costo esencial del negocio.
- No existe alternativa.

Los objetivos del plan de contingencias es hacer los siguiente:

- Restablecer el procesamiento de aplicaciones criticas lo más pronto posible.
- Recobrar después el procesamiento total.
- Restablecer la capacidad total de procesamiento.

La administración debe identificar los activos del Centro Comercial que necesiten mayor protección e implantar precauciones y procedimientos para la recuperación de desastres.

2) Resolver qué es más importante de proteger y qué se necesita para hacerlo.

El centro de cómputo puede realizar ciertas operaciones, que el personal y los usuarios consideren importantes; pero durante un desastre, no puede hacerse todo porque los recursos clave no están disponibles. Es por esto que durante un desastre, el Centro Comercial debe concentrarse en el procesamiento de cómputo que sea más importante para la sobrevivencia; sus aplicaciones críticas junto con los recursos necesarios para ejecutarlas. La identificación de éstas, es una decisión comercial que requiere que se involucre la alta gerencia. La cantidad de tiempo y trabajo involucrado depende de factores como el tamaño y complejidad de las operaciones del procesamiento de datos, la experiencia del personal, los procedimientos y documentación.

La prioridad de una aplicación que se basa en tres factores principales:

- Valor Monetario. Cantidad de ingresos producidos por la aplicación, o la cantidad de pérdida en caso de que no se ejecute.
- Prioridades. Son las aplicaciones que pueden ser necesarias para pagos fiscales como regulaciones, contratos entre otros o claves comerciales por ejemplo, servicio a clientes o mantenimiento del flujo de dinero.
- Urgencias de tiempo. La necesidad de ejecutar una aplicación en periodos o frecuencias determinadas.. La urgencia se deriva de los dos factores anteriores.

La siguiente información fue utilizada para el llenado de las encuestas por cada departamento en el capítulo 4:

- Aplicación. Identificar la aplicación por su nombre y dar una descripción breve de su uso.
- Usuarios. Describir al grupo de usuarios para la aplicación. No se deben anotar los nombres de los usuarios. Identificar su ubicación, incluyendo número de edificio y localidad relativa dentro de éste (piso, número de oficina, etc.).
- Distribución. Identificar quién recibe las salidas o reportes y cómo son usados.
- Calendario de procesamiento. Revisar la frecuencia del procesamiento de la aplicación. Establecer cuándo es ejecutada normalmente: diario, dias especificos

durante la semana, mensual, trimestral o anualmente. Agregar, si es apropiado, la hora. Si hay periodos de procesamiento más esenciales que otros, es necesario identificarlos por fecha y hora.

- Modo de procesamiento. Revisar si la aplicación es procesada en linea (interactiva) o en lotes (batch). En caso de que sea en lotes, verificar cómo son sometidos los datos. Identificar el origen (fuente) de los datos.
- Dependencias. Listar cualquier aplicación que suministre datos a esta aplicación o que obtenga información de ésta. Esto es usado para identificar las aplicaciones que deben estar al mismo nivel o mayor en las prioridades de procesamiento para la restauración.
- Procesamiento mínimo. Listar los pasos que puedan eliminarse de la aplicación, en caso absolutamente necesario.
- Ingresos/pérdida potencial. Establecer el ingreso ganado por el Centro Comercial por esta aplicación y de otras que dependan de ésta. Estimar la pérdida en caso de que no se ejecute un dia, una semana y un mes.
- Limitaciones y prioridades. Identificar cualquier ley, regulación, contrato u otra limitación que requiera la ejecución de esta aplicación. De la misma manera, identificar las funciones y objetivos de la prioridad comercial que requiera la aplicación.
- Tiempo máximo tolerable de caída. Estimar el tiempo máximo de caída que pueda ser tolerado, basado en el valor monetario y/o las limitaciones y prioridades.
- Clasificaciones. Asignar clasificaciones en base al valor monetario y a la urgencia de tiempo, usando una escala del 1 (menor) al 5 (mayor).
- Valor monetario. Realizar las clasificaciones en base a la pérdida potencial. Las cantidades utilizadas para definirlas deben ser determinadas por la gerencia del Centro Comercial.
- Urgencia de tiempo. Asignar una clasificación basada en el tiempo máximo tolerable de caída:

    5. 8 horas o menos
    4. De 8 a 24 horas
    3. De 2 a 3 dias
    2. 1 semana
    1. Más de 1 semana

Después de haber analizado cada aplicación para determinar su prioridad, basada en su importancia para la operación y sobrevivencia del Centro Comercial, el siguiente paso es elaborar una lista resumida de las aplicaciones por prioridad en orden de restauración durante la recuperación.

Para elaborar la lista, primero se deben clasificar todas las encuestas por prioridad asignada. Después, es necesario decidir cómo organizar las aplicaciones en la lista, considerando dos posibilidades:

Por área funcional. Agrupar todas las aplicaciones que sirvan a la misma función general comercial, por ejemplo, comunicación y procesamiento de órdenes. La ventaja de este agrupamiento es que los gerentes pueden ver rápidamente qué aplicaciones de su área serán procesadas.

Por tiempo tolerable de caída. Agrupar las aplicaciones por tiempo tolerable de una suspensión. Utilizar categorías, tales como "menos de cuatro horas", "de 4 a 8 horas", etc. La ventaja de este agrupamiento es que lo lleva directamente al plan de restauración.

3) Preparar las instalaciones computacionales de respaldo a ser utilizadas durante un desastre y asegurar que todas las copias de seguridad de software, datos y documentación necesarios sean almacenados en un lugar seguro.

Al momento de definir un plan de contingencias todos los archivos y programas vitales deberán estar duplicados y almacenados fuera del site. Posteriormente se deberá implantar una estrategia de respaldo deberá ser implantada. Las opciones para la estrategia de respaldo del centro de cómputo son:

- Facilidad de Respaldo Propia del Centro Comercial. El sistema total es duplicado en un lugar distante del presente centro de cómputo. Esta opción es de muy bajo riesgo y de muy alto costo.

- "Hot Site". Esta es una facilidad de respaldo ofrecida por los proveedores del equipo de cómputo en base a una cuota de ingreso por parte de los usuarios de una familia particular de computadores. En el evento de un desastre los suscriptores pueden utilizar el Hot Site en un periodo de 24 horas y hasta por 3 meses (promedio). Esta alternativa tiene la gran desventaja consistente en que si el desastre es general, el Hot Site puede no tener la capacidad para proporcionar servicio a todos los suscriptores completamente. La opción es de bajo riesgo si el desastre no es extendido y se ofrece a un costo razonable.

- Acuerdo Recíproco. Esta opción establece un arreglo o contrato realizado entre dos compañías por el servicio de cómputo en el caso de desastre de una de ellas. Esto suena como una opción viable, pero generalmente no funciona por dos razones: primeramente, la mayoría de los sistemas de información no tienen el tiempo suficiente para cubrir sus propias necesidades de proceso, por lo que se descarta el procesamiento de información de otra organización; en segundo término, al final de cuentas los sistemas de cómputo se vuelven parcialmente incompatibles, debido a las modificaciones realizadas en una o en ambas empresas, y uno no puede estar prevenido sobre esta situación hasta que es muy tarde.

- Consorcio. Con esta opción varias compañías se reúnen y construyen su propia facilidad de respaldo. Esta opción contiene características de las tres primeras.

- Agencia Comercial de Servicios. La contratación para el procesamiento de emergencia de una agencia comercial de servicio puede ser una opción favorable

bajo ciertas circunstancias. El sistema deberá ser compatible y estar disponible cuando se le necesite. La mayoría de las agencias de servicio, sin embargo, corren sus sistemas a su máxima capacidad. El riesgo, costo y efectividad son moderados en esta alternativa.

- "Shell". Esta alternativa consiste en un edificio que tiene todas las conexiones y salidas necesarias, pero sin contar con el equipo de cómputo. Existe, sin embargo, la disponibilidad inmediata para aceptar e instalar un equipo. Los cascos pueden ser construidos por la organización para su uso propio o suscribirse a uno comercial. Para esta opción el riesgo es moderadamente alto, los costos son bajos y la efectividad va de baja a moderada.

Para el caso particular del Centro Comercial, la alta gerencia se decidió por la opción de facilidad de respaldo propia de la empresa. De acuerdo a esta decisión se establecen las instalaciones, condiciones y procedimientos complementarios de respaldo.

En estas instalaciones se debe seleccionar un local de almacenamiento externo (caja de seguridad) e identificar una o más localidades externas donde se puedan almacenar seguramente los datos y documentación de respaldo. Para la selección de una ubicación externa de almacenamiento, las dos consideraciones principales son acceso y seguridad. Los datos y documentación guardados en la caja de seguridad deben estar disponibles rápidamente después de la notificación, para ser usados en las operaciones de recuperación. Al mismo tiempo, deben ser fácilmente accesibles, desde la instalación primaria para agilizar la transferencia del material a la caja de seguridad. Es por esto que se debe elegir una ubicación de almacenamiento externo con acceso conveniente desde las instalaciones primarias y de respaldo.

Las posibles instalaciones de localidad externa pueden ser en dos o tres sucursales que estén más alejadas del Centro Comercial y una caja de seguridad de depósito de un banco local, rentado por una cuota mensual. Las instalaciones contratadas para el almacenamiento de datos, pueden estar disponibles también en varias áreas y proporcionar la conveniencia adicional de sacar y rotar regularmente, el material. Se debe considerar cuidadosamente el número de cajas de seguridad externas a ser usadas. Aplicando el principio de diversidad al almacenamiento de datos, se sugiere que se preparen múltiples copias del respaldo de datos y se roten regularmente en distintas localidades. El tener múltiples copias de respaldo reduce la posibilidad de pérdida pero también complica la seguridad y control de los datos. La mayor parte de esta tarea involucra la consolidación de esa información para producir un inventario del contenido de la caja de seguridad. El inventario del material guardado fuera de la instalación debe incluir:

- Software del sistema y documentación.
- Software de la aplicación y documentación.
- Datos de la aplicación e instrucciones de su preparación.
- Manual del plan de contingencia en caso de desastre y copia electrónica.
- Guia de respaldo de la instalación.
- Planos de los pisos del centro de cómputo.

- Inventario del centro de cómputo.
- Formas adaptadas y materiales especiales necesarios para las aplicaciones críticas.

Todas las instalaciones, procedimientos, parámetros y librerías de programas del sistema, deben ser identificados y mantenidos continuamente en una localidad externa. También deben ser respaldados, los sistemas de utilería, incluyendo aquellos necesarios para vaciar y restaurar el sistema operativo y los componentes relacionados.

Dependiendo de la disponibilidad del tiempo de procesamiento, pueden emplearse dos métodos para proporcionar respaldo del software del sistema. Primero, debe ser ejecutado un vaciado total de los paquetes del sistema cada vez que se haga el mantenimiento. Segundo, deben bajarse individualmente, a una cinta, los conjuntos de datos y/o librerías más volátiles.

Debe existir documentación del sistema operativo, mostrando la siguiente información: el sistema operativo que se está utilizando, nivel de emisión, todas las modificaciones internas, todos los paquetes de software. Se deben listar todos los manuales usados en la generación y operación del sistema y guardarse una copia en la caja de seguridad externa. Se debe ser cuidadoso, al incluir las instrucciones de arranque para iniciar los entornos interactivos y en lotes (batch). También debe incluir instrucciones de cualquier utilería para almacenar y restaurar datos.

La responsabilidad del control, uniformidad, mantenimiento y seguridad de la documentación debe asignarse para las instalaciones internas y externas. Es necesario asegurarse de agregar al inventario de la caja de seguridad, los respaldos de cualquier software necesario para mantener o usar la forma electrónica. Se debe considerar el procesador de palabra, bases de datos, hoja de cálculo y programas de utilerías.

Es posible que un desastre destruya completamente el centro de cómputo, en ese caso se tendrá que restaurar. Un plano actualizado del piso, que muestre la configuración, facilitará la planeación.

4) Desarrollar, en caso necesario, procedimientos manuales para manejar aplicaciones críticas, hasta que esté establecido el procesamiento intermedio.

Cada aplicación crítica es evaluada para determinar si son necesarios procedimientos de procesamiento alterno, por el período entre un desastre y la recuperación, ya sea en la instalación de respaldo o en el centro de cómputo.

Los procedimientos alternos son una forma de procesar una aplicación sin las instalaciones normales del centro de cómputo. En algunos casos, éstos serán procedimientos totalmente manuales. Esto es, la información será anotada a mano en formas o libros, las facturas pueden ser escritas a máquina, en lugar de ser generadas en la computadora o se pueden

desarrollar procedimientos alternos basados en PCs. De cualquier modo, si se elige desarrollar procedimientos alternos, es necesario que mantengan la continuidad de los datos. No se debe perder información alguna, como resultado de un procedimiento alterno y debe existir una forma de integrar los datos al sistema usual, cuanto esté restaurado el procesamiento. Para cada aplicación crítica que necesite procedimientos alternos, se debe proporcionar lo siguiente:

- Descripción funcional. Una explicación breve de la aplicación y su uso.
- Usuarios. Identificación de la comunidad de usuarios de la aplicación. No se deben utilizar los nombres específicos de las personas.
- Procedimientos anteriores al desastre. Especificar los procedimientos a seguir para asegurar la disponibilidad de todo lo necesario, para ejecutar el procedimiento alterno, incluyendo datos, reportes, documentación, herramientas, etc. Considerar si las copias de esto se deben guardar en la caja de seguridad externa.
- Restaurando el procesamiento normal. Especificar los pasos a seguir para restaurar el procesamiento normal de cómputo, después de la recuperación, ya sea en la instalación de respaldo o en el centro de cómputo.
- Pruebas. Estipular los procedimientos para probar el método alterno y la restauración de las operaciones de cómputo.

Un procedimiento alterno no debe considerarse completamente desarrollado hasta que los usuarios tengan listas, para ser usadas, todas las instrucciones, formas, libros, hojas de cálculo, bases de datos o cualquier otra herramienta involucrada en el procesamiento.

5) Especificar la manera exacta de responder a emergencias y diferenciar entre un "problema" y un "desastre".

Cuando se presenta el caso de una falla en una computadora, un apagón o falla en el aire acondicionado, pueden pasar varias horas o hasta días, antes de que se restablezca el servicio. Durante estas situaciones, el personal de reparación muchas veces es optimista, diciendo que el problema será resuelto en una o dos horas. Cuando transcurrieron las dos horas y el problema aún no es resuelto esta persona puede volver a decir que sólo es cuestión de una hora más. Esto puede continuar por horas, mientras tanto la instalación de cómputo está suspendida.

Para evitar que transcurra mucho tiempo sin saber realmente el nivel del problema o desastre, se establecieron procedimientos de escalación de problemas, que consisten en varios pasos a seguir para saber el nivel de riesgo de los problemas no resueltos. El propósito de los procedimientos de escalación de sistemas es definir la distribución de los pasos del tiempo que llevan a la declaración de un desastre.

En el Centro Comercial se desarrolló un procedimiento de escalación compuesto de cuatro pasos. Comienza con la detección de un problema, atraviesa por las condiciones de Alerta 1 y 2 y termina con la declaración de un desastre. Como se muestra en la figura 5.2.

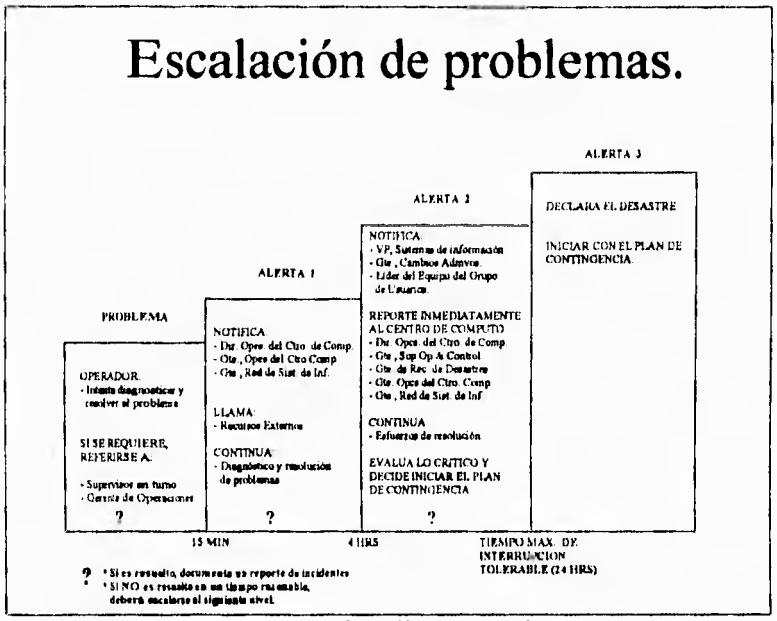


Figura 5.2 Pasos para Escalar Problemas No Resueltos.

El movimiento de un paso a otro es determinado por el tiempo transcurrido en el que el problema permanece sin solución. El tiempo límite de escalación de Alerta 2 a Desastre puede variar, dependiendo de lo crítico de las aplicaciones involucradas, pero como regla general no debe exceder a las 24 horas.

En cada paso el procedimiento especifica lo siguiente:

- A quién hay que notificar
- Quién debe reportarse a la instalación
- Recursos externos que hay que conseguir
- Acciones a tomar

Las diferentes divisiones de los pasos de escalación pueden incluirse en el procedimiento para permitir diferenciaciones, dependiendo si el problema involucra hardware, software, comunicaciones de datos, el entorno o no se ha determinado.

6) Detallar los recursos del procesamiento de datos, de tal forma que el daño pueda ser valuado y los recursos puedan ser reemplazados en caso necesario.

Los procedimientos de administración de desastre dirigen las actividades necesarias para iniciar y llevar a cabo las operaciones de recuperación: notificando a las personas correctas, valuando el daño y su impacto, decidiendo qué hacer, emitiendo una directiva de recuperación y controlando los esfuerzos de restablecimiento. Los procedimientos de administración son efectivos inmediatamente después de un desastre. Su función es alentar decisiones de recuperación con calidad, durante una etapa confusa y llena de tensión. Una vez que la directiva total se ha compuesto, los equipos de recuperación pueden empezar a trabajar estableciendo el procesamiento intermedio y eventualmente restablecer las operaciones normales.

La planeación de procedimientos de administración se enfoca principalmente a identificar a los miembros del Equipo de manejo de desastre, estableciendo la responsabilidad de notificaciones y de decisiones importantes, preparando las listas de verificación necesarias y los procedimientos para guiar las actividades del equipo. Una lista de verificación de los recursos y registros necesarios en el centro de control activado, minimizará el tiempo necesario para hacerlo funcional.

La valuación del daño y del impacto son actividades clave de la administración de desastres, porque proporcionan la información necesaria para la toma de decisiones. A fin de elegir una alternativa de recuperación, la administración debe tener respuestas a dos preguntas básicas.

- ¿Qué ha dañado o perdido? (valuación del daño)
- En qué forma han sido afectadas las aplicaciones críticas por el daño o la pérdida? (valuación del impacto)

Un inventario completo y categorizado puede servir como base para la valuación del daño y del impacto. La valuación del daño puede hacerse primero, revisando rápidamente los elementos de cada categoría de las encuestas y determinando si ha habido o no algún daño dentro de la categoría. Luego, si se ha sufrido algún daño, revisa sistemáticamente las partidas de la categoría para detallar aquellas que han sido dañadas y las que siguen operando.

INVENTARIO

CATEGORIA PARTIDA	*No. NECESARIOS PARA APLICACIONES CRITICAS*	*DAÑO MENOR*	*DAÑO MAYOR*	*TIEMPO DE RECUPERACION*
------	------	------	------	------
------	------	------	------	------

El inventario debe ser dividió en categorías y después subdividido dentro de la categoría, para hacer más fácil la recopilación, la actualización y su uso. Se sugieren las siguientes categorías:

- Hardware
- Software del sistema (incluyendo el de comunicación de datos)
- Software de las aplicaciones
- Datos
- Hardware de comunicaciones de datos
- Documentación
- Materiales y formas
- Personal

La evaluación del impacto va un paso más allá, al examinar el efecto del daño en el procesamiento de aplicaciones críticas. En este se requiere saber si la partida dañada es o no utilizada por las aplicaciones críticas, una estimación del tiempo necesario para la reparación o el reemplazo y el tiempo máximo tolerable de suspensión de las aplicaciones afectadas. La forma que se determinó como más fácil para la recopilación de información fue marcar en el inventario, aquellas partidas usadas por aplicaciones críticas y dejar un espacio para indicar la magnitud del daño y tiempo estimado de reparación.

Una vez ocurrido el desastre (natural o no) y siguiendo la estrategia descrita en el plan de contingencias según el caso, se requiere de un PLAN DE RECUPERACION el cual es un conjunto completo de procesos que describen paso a paso las diferentes acciones y procedimientos que deben considerarse para volver a la normalidad la operatividad de una empresa, una vez corregidos los problemas.

5.8. Plan de Recuperación.

El desarrollo de este Plan de Recuperación tiene como objetivo principal recuperar la operatividad del Centro Comercial en el menor tiempo y costo posible, por medio de la recuperación de la información, y no de la recuperación simple de los datos del Centro de Cómputo. Es decir va a permitir que éste pueda enfrentarse a una situación de Desastre de una manera efectiva, optimizando los procedimientos para la recuperación de los sistemas de información y la operatividad de la misma. Lo que se pretende con este Plan no es evitar un Desastre, sino minimizar los efectos y el impacto de éste.

Como parte de este objetivo, este Plan pretende minimizar lo siguiente:

- El número de decisiones a tomar durante la contingencia.
- La dependencia del Centro Comercial sobre una persona o grupo de personas, en el Proceso de Recuperación.

- La necesidad de desarrollar e implementar nuevos procedimientos durante la Recuperación.
- El impacto negativo de la pérdida de datos, reconociendo que la pérdida de ciertas transacciones es inevitable.

1) Elementos del Plan de Recuperación.

Para que el Centro Comercial se enfrente a una situación de Desastre en forma adecuada, es necesario tener bien definidos cuatro elementos indispensables:

a) Un lugar a donde trasladarse. Se debe contemplar la identificación de un Centro de Soporte Alterno, donde el personal pueda trasladarse por si el acceso al Centro Comercial está parcial o totalmente restringido. Este Centro Alterno pueden ser desde oficinas hasta un lugar con el Equipo necesario para restablecer las operaciones del Centro Comercial. Este Centro Alterno debe contar con el equipo necesario y los requerimientos mínimos de Hardware, Software y espacio para el Personal clave del Centro Comercial, con el propósito de ejecutar los procesos criticos y restablecer lo más pronto posible la operación de éste.

b) Personal que participa en el proceso de recuperación. El Personal Humano es el elemento más importante en el Centro Comercial y el Proceso de Recuperación, ya que si no se cuenta con su participación en forma oportuna y eficaz el Plan no va lograr su óptimo desarrollo. Este personal está integrado en diferentes Comités, los cuales realizarán las actividades definidas en el Plan en forma coordinada. El personal que participa en el Plan de Recuperación es el siguiente: Personal de Alta Dirección, Personal Clave del Centro Comercial, Personal de Sistemas, Usuarios, Personal de Seguridad y también personal externo que esté relacionado con el Centro Comercial, como los proveedores, medios de comunicación, bufete de abogados, etc.

c) Información necesaria para el Proceso de Recuperación. Esta información puede estar contenida en cintas, diskettes, microfilms, microfichas y/o documentos. Es importante que estos medios de almacenamiento sean guardados en un lugar externo al Centro Comercial , con el propósito de que los Comités de Recuperación, tengan un acceso fácil y seguro a ellos y puedan recuperar la operación del Centro Comercial lo más pronto posible. Aunque algunas funciones no se procesen durante las primeras semanas de ocurrido el Desastre, paulatinamente se irán procesando, por lo que se recomienda que esta información esté bien protegida.

d) Un Plan a seguir. En el caso en que el Centro Comercial se enfrente a un Desastre, un Plan estructurado y documentado, va a permitir agilizar los procedimientos a seguir y que el Centro Comercial se recupere en el menor tiempo posible. Es importante contar con la información correcta y actualizada sobre proveedores, clientes, Personal de la Empresa, Comités de Recuperación, es decir todo el personal que participa en el

esfuerzo de Recuperación, así como las funciones de los Comités y la logística de Recuperación a seguir con el propósito de que el Centro Comercial se recupere lo más pronto posible del Desastre. Es muy importante mencionar que, cuanto más clara y accesible se encuentre la información contenida en el Plan, más valiosa se convertirá ésta para el esfuerzo de Recuperación.

2) Establecimiento del alcance y objetivos del Plan de Recuperación.

El alcance del Plan de Recuperación se estableció tomando en cuenta dos características muy importantes:

- Las áreas del Centro Comercial (Divisiones, Departamentos y Sucursales) para las cuales se va a desarrollar el Plan de Recuperación y,
- Las instalaciones del Centro Comercial que se van a contemplar en el Plan de Recuperación.

El alcance del Plan de Recuperación para las diferentes áreas del Centro Comercial se puede referir a toda la organización, o puede estar limitado al departamento de informática. Este Plan de Recuperación será elaborado para todo el Centro Comercial ya que es importante considerar que:

- Los desastres son eventos selectivos y generalmente su impacto no se limita exclusivamente al departamento de Informática.
- El objetivo primario del Plan de Recuperación es recuperar la operatividad del Centro Comercial y no la simple recuperación de los datos.

La planeación del Proceso de Recuperación se iniciará con el Plan de Recuperación para el departamento de Informática (involucrando las áreas de Desarrollo, Producción, Centro de Cómputo y Soporte Técnico), por las siguientes razones:

- Presión (por ejemplo la de los auditores) para desarrollar Planes de Recuperación que se enfoquen inicialmente en el departamento de Informática.
- Informática es vital y central para el Centro Comercial.
- En Informática se centraliza el grueso de la información del Centro Comercial.
- La Planeación del Plan de Recuperación es más fácil ya que se cuentan con más conocimientos y herramientas de planeación.
- Si inicialmente el Plan contempla al departamento de Informática, cuando se desarrolle para todo el Centro Comercial será más sencillo.

3) Proceso de Recuperación para el Departamento de Informática

Este plan va a permitir recuperar lo más pronto posible y al menor costo, la operación de los sistemas de cómputo así como reconstruir las instalaciones dañadas. El Proceso a seguir para la Recuperación del Centro de Cómputo se ilustra en la figura 5.3.

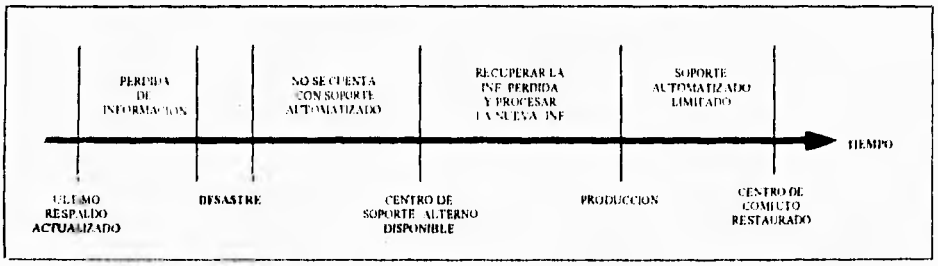


Figura 5.3 Proceso de Recuperación para el departamento de Informática.

En este proceso se está considerando que el personal de sistemas guarda las cintas y discos de respaldos en forma periódica en un lugar externo al Centro Comercial, y que alguna vez a experimentado una situación de Desastre que ha afectado seriamente el Centro de Cómputo. El personal de Informática tiene la función de evaluar el impacto del departamento de Informática ante una situación de desastre, así como la responsabilidad de reconstruirlo o de reemplazarlo. Para esto será necesario mantener contacto directo con proveedores y contratistas durante el Proceso de Recuperación. Por otro lado, antes del Desastre los usuarios de los sistemas han estado trabajando, ingresando información y procesando información en estos. En el momento que el Centro Comercial se enfrenta aun Desastre, la información y las operaciones realizadas entre el último respaldo y el día en que ha ocurrido el desastre se perderán. El personal de Informática deberá contar con procedimientos para reconstruir las operaciones realizadas por los usuarios, será casi imposible recuperar totalmente estas pérdidas de información sin la ayuda de estos.

Se requerirá de cierto periodo de tiempo para que el área de Informática traslade sus operaciones a un Centro de Soporte Alterno. Este periodo de tiempo puede tomar horas, días, o semanas dependiendo del tamaño y capacidad del Equipo Central, de las diferencias en la configuración del Sistema, o de las facilidades que presenta el Centro Alterno en sí. Durante este periodo de tiempo, los usuarios estarán trabajando en forma manual o utilizando otros procedimientos alternos sin los beneficios que brinda el departamento de Informática. Posteriormente, en la mitad de la figura 5.3 se representa el momento en que los usuarios de las aplicaciones podrán ingresar y procesar información en algunas de sus aplicaciones. ya que otras no se van a restablecer en forma inmediata.

Los usuarios de los sistemas van a tener la tarea de ingresar la información perdida y por otro procesar la información acumulada durante el periodo que no se tuvo soporte automatizado. De aquí se puede ver la importancia del por que se realizó con anticipación un estudio sobre las Aplicaciones Criticas del Centro Comercial, para conocer las aplicaciones que se van a recuperar en un primer orden. Así como la importancia de que el usuario haya seleccionado la información y las operaciones criticas a procesar en forma prioritaria. Los usuarios estarán operando y obteniendo soporte del personal de Informática que diferirá significativamente del ambiente al que están acostumbrados.

Este tiempo requiere de un periodo de ajuste en el que el usuario se adapte a la nueva instalación, al nuevo Equipo en el que va a trabajar, y a otro horario diferente al que normalmente opera. Este tiempo del "Soporte Automatizado Limitado" puede tomar meses, hasta que las instalaciones dañadas se reconstruyan o el departamento de Informática sea trasladado a otro lugar. Durante este periodo los usuarios del Centro de Cómputo pueden notar diferencias significativas en los tiempos de respuestas, retardos en los procedimientos y la falta de soporte automatizado de algunas de las áreas menos críticas.

Es importante notar que después de un Desastre, algunos procesos no se restablecerán en forma inmediata, sino que en forma gradual se irán restaurando, para que eventualmente todas las operaciones sean restablecidas. El Proceso de Recuperación termina cuando el Centro de Cómputo queda totalmente restablecido y se notifica el regreso a operaciones normales. Por lo que es importante que esta última fase del Proceso implica un periodo de ajuste, tanto para el personal de sistemas como para los usuarios del Centro de Cómputo y para el personal de las diferentes áreas del Centro Comercial, hasta que cada una de sus áreas tomen su cause normal.

4) Proceso de recuperación para una o más áreas operativas del Centro Comercial

Este plan va a permitir recuperar lo más pronto posible y al menor costo, la operatividad de las áreas automatizadas dañadas del Centro Comercial, tales como Contabilidad y Recursos Humanos. La figura 5.4 muestra el proceso de recuperación.

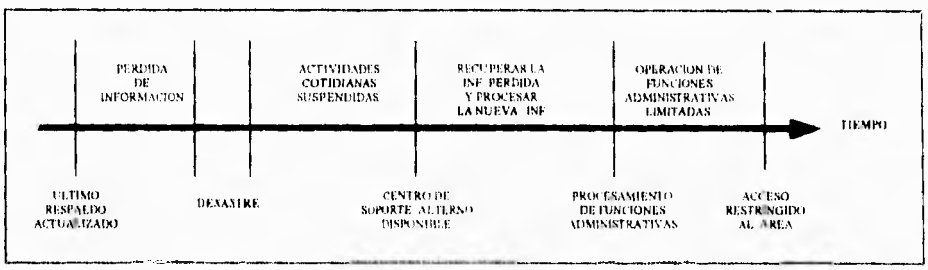


Figura 5.4 Proceso de Recuperación para una o más áreas operativas del Centro Comercial.

Este proceso es similar al que se sigue para la recuperación del departamento de Informática, en el que, el personal de las diferentes áreas operativas del Centro Comercial, realiza respaldos de información periódicamente, las cintas y diskets los almacena en una localidad externa a la empresa. Para diseñar este plan de recuperación se involucraron la gerencia de las áreas operativas del Centro Comercial. Adicionalmente para recuperar la

localidad externa a la empresa. Para diseñar este plan de recuperación se involucraron la gerencia de las áreas operativas del Centro Comercial. Adicionalmente para recuperar la información de las áreas operativas deben contemplar el almacenar su información crítica en una localidad externa, considerando los documentos fuentes, formas , formas preimpresas y reportes, además de las cintas y discos. Si algunas de las áreas operativas de la Empresa o todas han sido afectadas por un Desastre, el personal directivo de estas áreas será el responsable de la Recuperación.

Los usuarios se enfrentarán a la situación de reconstruir y de ingresar la información pérdida en el sistema y de procesar la nueva información acumulada durante el periodo que no se tuvo soporte automatizado, recomendando que cada usuario cuente con un checklist con los requerimientos, mínimos de hardware, software, materiales, documentos y papelería con el propósito de facilitar el Proceso de Recuperación. Así mismo, es importante contar con un Centro de Trabajo Alterno para el personal en caso de que el acceso al Centro Comercial quede restringido. Finalmente, el personal de las áreas operativas, será responsable de trabajar en forma conjunta con el personal de Informática, otros usuarios, personal directivo, así como con el personal externo de la empresa. Este Plan de Recuperación requiere de la participación en forma coordinada del personal que está involucrado en el esfuerzo de recuperación.

5) Proceso de recuperación para todo el Centro Comercial.

Este proceso junto con los anteriores nos permite recuperar la operatividad del departamento de Informática que involucra las áreas de Desarrollo, Producción, Centro de Cómputo y Soporte Técnico y de una o más áreas automatizadas del Centro Comercial afectadas por una situación de Desastre.

El tiempo de Recuperación va a depender del impacto que ha sufrido el Centro Comercial, del Plan de Recuperación con el que cuente en ese momento, del personal y de las áreas operativas afectadas por el desastre.

6) Alcance del Proceso de Planeación.

El Proceso de Planeación abarca lo siguiente:

- Establecimiento de los criterios para determinar un Desastre, basado en el análisis del impacto en el Centro Comercial.
- Definición de las áreas y sistemas críticos del Centro Comercial, y el tiempo necesario para su recuperación.
- Determinación de los recursos necesarios para dar soporte a las áreas críticas del Centro Comercial.
- Identificación de las aplicaciones que son indispensables, para soportar los Procesos críticos del Centro Comercial.

- Establecimiento de los procedimientos a seguir para recuperarse de un Desastre.
- Capacitación del personal involucrado.
- Incluir simulacros y pruebas de los procedimientos establecidos.
- Apoyar el mantenimiento periódico del Plan.

Por lo tanto, la Planeación del Proceso de Recuperación abarca todas las actividades que se tienen que realizar antes de que ocurra un Desastre, con el propósito de que el Proceso de Recuperación se lleve en forma efectiva y oportuna.

7) Determinación del Escenario de Recuperación.

En este parte se define el Escenario de Recuperación, lo cual se refiere a la situación en la que se enfrente el Centro Comercial como consecuencia de un Desastre y determinar el estado en que se encuentre éste. El escenario de Recuperación se definió en función de las siguientes variables:

- Tipo y Grado de Desastre.
- Aplicaciones Críticas.
- Periodos Críticos.

Tipo y grado de desastre.

Nos referimos a tipo de Desastre una vez que se ha identificado las causas que han originado el Desastre, es decir, si es por causas naturales o humanas. En cuanto al grado de Desastre, éste se define en función de las siguientes variables:

- Si el recurso humano crítico está disponible o no.
- Si el Desastre ha afectado al departamento de Informática (particularmente al Centro de Cómputo) en forma parcial o total.
- Si el desastre ha afectado las áreas operativas y/o oficinas de la Empresa en forma parcial o total.
- Si el Desastre ha afectado total o parcialmente al Equipo de Comunicación.

Aplicaciones Críticas.

Uno de los aspecto más importantes a considerar en un Plan de Recuperación es la determinación de las Aplicaciones Criticas dentro del portafolio de Aplicaciones del Centro Comercial. Considerando como Aplicación Critica aquella que es fundamental para la operación del Centro Comercial, ya que al faltar ésta puede ocasionar consecuencias como: no contar con la información oportuna para la toma de decisiones, paralizar algunas operaciones de éste, lo cual a su vez le puede ocasionar un alto impacto económico y en imagen corporativa de la compañia.

Periodos Críticos.

El nivel de operación y el volumen de transacciones que se manejan en forma automática en las Aplicaciones Críticas pueden aumentar en ciertos períodos de la semana, del mes y del año. Es importante identificar estos períodos, ya que dependiendo del momento en que ocurra un Desastre, una Aplicación puede ser afectada en mayor o menor grado y por lo tanto puede variar su prioridad a recuperar.

La identificación de las Aplicaciones Críticas y de los Períodos Críticos para el Centro Comercial se realizó en el capítulo tres. A continuación se proponen tres escenarios de recuperación, en donde se mencionan las características generales de las posibles situaciones a las que se podría enfrentar el Centro Comercial, así como la estrategia y la logística general a seguir.

Escenario 1.

El Centro de Cómputo ha sido afectado en forma total o parcial, pero las áreas operativas del Centro Comercial y sus oficinas siguen operando.

La restauración del área de operaciones del Centro de Cómputo y el restablecimiento de las operaciones pueden tomar 24 horas hasta varios meses, dependiendo del daño sufrido. El Comité de Recuperación asignado evaluará el impacto del Centro de Cómputo. Dependiendo de esta evaluación, se determinará si es necesario trasladarse o no a un Centro de Soporte Alterno.

Estrategia General.

En el caso de que el Centro de Cómputo haya sufrido algún daño menor, se recomienda concentrar todos los recursos necesarios con el propósito de restablecer lo más pronto posible la operación del Centro de Cómputo.

En el caso de que el Centro de Cómputo haya sido dañado en forma total y el traslado a un Centro de Soporte Alterno sea necesario se recomienda realizar los arreglos necesarios para restablecer las operaciones en el Centro de Soporte Alterno, hasta que el Centro de Cómputo se haya reparado o relocalizado. Por otro lado se informará al responsable de cada uno de los departamentos, el espacio asignado, horarios, terminales y medios de transporte disponibles, con el propósito de que el usuario pueda restablecer sus operaciones en el Centro de Soporte Alterno.

Plan Requerido.

El Plan de Recuperación requerido debe incluir actividades generales como:

- Evaluación del impacto del desastre.

Periodos Criticos.

El nivel de operación y el volumen de transacciones que se manejan en forma automática en las Aplicaciones Criticas pueden aumentar en ciertos periodos de la semana, del mes y del año. Es importante identificar estos periodos, ya que dependiendo del momento en que ocurra un Desastre, una Aplicación puede ser afectada en mayor o menor grado y por lo tanto puede variar su prioridad a recuperar.

La identificación de las Aplicaciones Criticas y de los Periodos Criticos para el Centro Comercial se realizó en el capitulo tres. A continuación se proponen tres escenarios de recuperación, en donde se mencionan las caracteristicas generales de las posibles situaciones a las que se podria enfrentar el Centro Comercial, asi como la estrategia y la logistica general a seguir.

Escenario 1.

El Centro de Cómputo ha sido afectado en forma total o parcial, pero las áreas operativas del Centro Comercial y sus oficinas siguen operando.

La restauración del área de operaciones del Centro de Cómputo y el restablecimiento de las operaciones pueden tomar 24 horas hasta varios meses, dependiendo del daño sufrido. El Comité de Recuperación asignado evaluará el impacto del Centro de Cómputo. Dependiendo de esta evaluación, se determinará si es necesario trasladarse o no a un Centro de Soporte Alterno.

Estrategia General.

En el caso de que el Centro de Cómputo haya sufrido algún daño menor, se recomienda concentrar todos los recursos necesarios con el propósito de restablecer lo más pronto posible la operación del Centro de Cómputo.

En el caso de que el Centro de Cómputo haya sido dañado en forma total y el traslado a un Centro de Soporte Alterno sea necesario se recomienda realizar los arreglos necesarios para restablecer las operaciones en el Centro de Soporte Alterno, hasta que el Centro de Cómputo se haya reparado o relocalizado. Por otro lado se informará al responsable de cada uno de los departamentos, el espacio asignado, horarios, terminales y medios de transporte disponibles, con el propósito de que el usuario pueda restablecer sus operaciones en el Centro de Soporte Alterno.

Plan Requerido.

El Plan de Recuperación requerido debe incluir actividades generales como:

- Evaluación del impacto del desastre.

- Declaración del desastre.
- Notificación a los comités de Recuperación.
- Notificación a clientes, a proveedores y personal externo.
- Restablecimiento de todas las operaciones en el Centro de Cómputo.

En el caso de un daño total el Plan debe incluir las actividades generales anteriormente mencionadas así como las siguientes:

- Activación del Plan de Recuperación.
- Confirmación de las funciones de los comités de Recuperación.
- Confirmación de Aplicaciones Críticas.
- Activación del fondo de emergencia.
- Confirmación de canales de Comunicación.
- Evaluación del desarrollo del plan en forma periódica.
- Contactar responsables del Centro Alterno.
- Disposición y coordinación del transporte para el Equipo, Material y Recursos Humanos.
- Preparación del Hardware y Software en el Centro de Soporte Alterno.
- Coordinación de Comités de Recuperación.
- Restablecimiento de operaciones en el Centro de Soporte Alterno.
- Restauración y/o construcción del Centro de Cómputo.
- Evaluación del desarrollo del Plan.

Escenario 2.

El Centro de Cómputo ha sido afectado en forma total o parcial y no se tiene acceso a las áreas operativas, a las oficinas del Centro Comercial.

Estrategia General.

Se recomienda realizar los arreglos necesario para restablecer las operaciones en el Centro de Soporte Alterno, hasta que El Centro de Cómputo esté reparado o relocalizado. Por otro lado, se recomienda contactar al responsable del Centro de Trabajo con el propósito de que el personal que no se traslade al Centro de Soporte tenga espacio de oficina en donde pueda trabajar con el equipo y material necesario.

Plan Requerido.

El Plan de Recuperación Requerido debe de incluir las actividades mencionadas en el Escenario 1, así como las siguientes actividades:

- En caso de huelga comunicación con el Sindicato.
- Contactar responsable del Centro de Trabajo.
- Contactar responsables del Centro de Recepción y Control de Material.

Escenario 3.

El equipo de Comunicación ha sido afectado en forma parcial o total.

Estrategia General.

Concentrar los recursos humanos necesarios para restablecer lo más pronto posible las comunicaciones del Centro Comercial.

Plan Requerido.

El Plan de Recuperación requerido debe incluir las actividades mencionadas en los Escenarios anteriores y contemplar otras actividades como:

- Evaluación del estado del Equipo de Comunicación.
- Instalación de las comunicaciones en el Centro de Soporte.
- Implementación de medidas alternas de Comunicación.
- Información a clientes, proveedores, personal externo y otras instalaciones del Centro Comercial, de las medidas alternas y procedimientos de comunicación establecidos.
- Evaluación de compra o renta de Equipo.
- Restablecimiento de las comunicaciones en el Centro de Cómputo.

Las actividades a realizar en los diferentes Escenarios de Recuperación se han especificado en forma particular en el apartado 5.2 de éste capítulo.

8) Condiciones para activar el Plan de Recuperación.

En el momento que ha sucedido un Desastre, el Comité Coordinador de la Recuperación evaluará el impacto del mismo y determinará el Escenario de Recuperación en el que se encuentra el Centro Comercial. Es muy importante realizar esta evaluación, ya que no siempre es necesario que se active el Plan de Recuperación. Para que el Plan de Recuperación se active, es necesario que se cumplan algunas de las condiciones que se mencionan a continuación:

- El Centro de Cómputo se ha dañado o no se tiene acceso a él.
- Cuando el Desastre haya afectado seriamente el Equipo de Cómputo. Hay que tomar encuentra que no es lo mismo que se haya dañado todo el Equipo de Cómputo, a un periférico en específico.
- Cuando el daño ocasionado afecte directamente la operatividad de las Aplicaciones Criticas y por lo tanto genere un impacto económico o de imagen corporativa negativo.
- Cuando el desastre haya ocurrido en un periodo de tiempo en el cual se vean afectadas varias Aplicaciones Criticas.
- Cuando la corrección del daño ocasionado por el Desastre, tome un periodo de tiempo que el Centro Comercial considere determinante para su operación.

5.9 Almacenamiento y Distribución del Plan de Seguridad.

Resulta necesario establecer criterios de seguridad y acceso a la información en el Plan de Seguridad de la Información. Este Plan debe ser considerado como un documento confidencial, por lo que el acceso a éste deberá ser accesible solamente a cierto personal del Centro Comercial. El responsable del almacenamiento y distribución de las copias del Plan deberá ser el Coordinador del Plan de Seguridad del Centro Comercial. La versión completa del Plan de Seguridad deberá ser accesible únicamente a los integrantes de los Comités de Administración y Coordinación del Plan. Los demás comités tendrán acceso solamente a determinados apartados del Plan. Se deben generar copias de este Plan y algunas de ellas deben ser guardadas en una localidad segura y externa al Centro Comercial. Sin embargo, las copias del Plan deben ser fácilmente accesibles al Personal Clave del Centro Comercial en una situación de desastre. El responsable y el lugar donde se van almacenar las copias del Plan se pueden documentar en el inventario de Suministros Misceláneos. Se deberá tener un control estricto de las copias que se obtengan del Plan y establecer mecanismos de seguridad sobre las mismas. Las copias deberán obtenerse solamente con la previa autorización del Coordinador del Plan.

6. SIMULACRO DE RECUPERACION DE INFORMACION

Algunas Empresas desarrollan su Plan de Seguridad y sin embargo nunca lo prueban. Los simulacros demuestran la efectividad del plan para recuperar la más pronto posible la operatividad de una empresa.

Uno de los objetivos principales para la realización de este simulacro es determinar la efectividad del Plan y verificar la adecuación de los procedimientos utilizados para el proceso de recuperación. Esto es, el realizar el simulacro permitirá demostrar que el plan está documentado de tal manera que permita la adecuada recuperación de las aplicaciones críticas en el caso de un desastre.

El simulacro contempla generalmente la recuperación de algunas aplicaciones críticas y de su ambiente operacional, el cual es llevado acabo con información que ya ha sido procesada en días anteriores con la finalidad de tener un patrón de comparación, para la evaluación de los resultados obtenidos en el simulacro.

Los simulacros deberán de realizarse cada cierto periodo de tiempo, por ejemplo, dos veces por año y no en forma continua, ya que se necesita un periodo de tiempo en el cual se realicen todos los cambios necesarios para ajustar el plan a la situación del Centro Comercial. Así mismo, los simulacros deberán ir avanzando en su complejidad, de ahí la importancia de determinar el alcance de cada uno.

6.1 Actividades para el desarrollo del Simulacro

Las actividades generales a realizar para la planeación para el simulacro son las siguientes:

- Determinación del alcance y objetivos del Simulacro.

Al efectuar el simulacro se pretende corregir deficiencias del plan de seguridad diseñado en el capítulo anterior, ya que no puede conocerse que tan bien funciona el plan de recuperación hasta que éste se prueba, por lo que el plan ya no será solamente un documento teórico si no que se convertirá en un documento dinámico y práctico.

- Desarrollo de una estrategia de prueba

Una vez que se tiene el plan se debe poner en práctica para que la gente además de saber que hacer, realmente lo haga. Con esto se sabrá si el plan funciona o no.

En estas pruebas se debe asegurar de que participe toda la organización, y de que sea lo más real que se pueda de manera que la gente sienta la responsabilidad y el reto de sacar adelante su trabajo y que el plan de seguridad lo conozca tan bien que sólo lo consulte para alguna cuestión rápida.

Después de un análisis detallado se determinó realizar un simulacro significativo en el Centro Comercial en cuestión mediante el establecimiento de un procesamiento en paralelo, operando sobre la base de que ocurriera un desastre.

Este simulacro será de tipo parcial ya que solamente se involucrarán algunas áreas de los diferentes departamentos, tales como : Producción, Desarrollo, Centro de Cómputo y Soporte Técnico, Recursos Humanos y Contabilidad.

- Identificación de los Recursos Humanos, Técnicos y Materiales involucrados en la prueba.

Como se mencionó anteriormente, el líder del Plan de Seguridad es el área de Centro de Cómputo y Soporte Técnico, por lo que con las encuestas realizadas, esta área deberá proveer del equipo de cómputo necesario para poder llevar acabo el simulacro, por lo que se contrato con HEWLETT PACKARD DE MEXICO, S.A DE C.V. el servicio de SITE BACKUP, donde fue solicitado el siguiente equipo:

Hardware:

1 CPU modelo HP-3000/9 (2..9) XL ó Clásica.
1 Unidad de cinta 7980XC, 7980 ó 7978 (1600/6250 BPI) Y DAT (unidad de respaldo).
1 Impresora de 1600, 840, 600 ó 300 LPM.
4 Puertos para la conexión de usuarios.
4 Terminales.
1 PC con 80 Mb en disco y 1.2 en RAM.
1 Sala de Trabajo para 10 personas

Software:

1 Sistema operativo 4.0 MPX/iX.
8.5 GB Espacio en disco.
64 MB Memoria Ram.

Por otro lado, el área de desarrollo en conjunto con el área de Contabilidad y Recursos Humanos informaron al área líder de la información acerca de lo que se requiere para este simulacro.

Contabilidad :

a) Captura de reposición de fondo fijo.
b) Captura de pedidos centralizados.
c) Captura de pedidos descentralizados.
d) Captura de Cheques diarios.

Recursos Humanos:

a) Captura de faltantes de cajeras.
b) Captura de percepciones adicionales.

c) Captura de tarjetas de tiempo.
d) Captura de ingresos y cambios de descuento en caja de ahorro.

Para esto el área de desarrollo informó cuales son los procesos a ejecutar para estas aplicaciones:

a) CIJB3280 Movimientos Contables.
b) CIJB2421 Procesos de previos de cheques diarios para proveedores normales
c) CIJB2420 Proceso de previos de cheques semanales para proveedores normales
d) CIJB2440 Emisión de cheques diarios para proveedores normales.
e) PEJB3400 Reporte de tarjetas faltantes
f) PEJB3200 Cálculo de la Nómina
g) PEJB2910 Emisión de cheques

Con estos datos el área líder decidió que información respaldada será necesaria para poder realizar las aplicaciones anteriores, ya que de esto dependerá la reproducción del ambiente de trabajo adecuado en el SITE BACKUP.

También fue necesario auxiliarse de software extemo:

a) POWER HOUSE (lenguaje de Programación)
b) SUPRTOOL (herramienta para trabajo con bases de datos)
c) MPEX/3000 (extensión del sistema operativo)
d) BULDJOB1 Y BULDJOB2 para la creación de estructuras de las cuentas y archivos de comandos utilizados para dichas aplicaciones.

Definición de las fases a seguir en el simulacro de recuperación.

a) Establecimiento de lugar y fecha de reunión para la realización del simulacro.
b) Creación del ambiente de trabajo bajo la supervisión del área líder
c) Verificación por parte de los usuarios de la información restaurada.
d) Ejecución de los procesos anteriormente citados.
e) Comprobación de los resultados obtenidos.
f) Reporte final.

- Implantación de las fases del simulacro.

1. Lugar y fecha de reunión : 18 de enero de 1995 a las 8:00 hrs., oficinas del Centro Comercial.

2. Salida de las oficinas : 8:45 hrs.

3. Llegada a las instalaciones de Hewlett Packard

Personal autorizado para este simulacro :

Personal del Centro Comercial.

Subdirector de Informática
Subgerente del Centro de Cómputo y Soporte Técnico
Líder de Soporte Técnico
Dos analistas de Soporte Técnico
Dos operadores del área de Producción
Líder de desarrollo de Contabilidad
Líder de desarrollo de Recursos Humanos
Cuatro usuarios de Contabilidad
Tres usuarios de Recursos Humanos
Dos líderes de Auditoría

Personal de Hewlett Packard :

Gerente de Computación Gerencial
Dos ingenieros asignados de cuenta para el Centro Comercial
Ingeniero de hardware asignado a la cuenta
Representantes de Ventas asignado a la cuenta.

4. De 9:30 a 11:20 hrs.

Se creó el ambiente de producción del Centro Comercial en el equipo del site bakup, para ejecutar las aplicaciones de Contabilidad y Recursos Humanos.

1. Creación del grupo Jobs en la cuenta SYS.
2. Restauración de los jobs BULDJOB1 (creación de estructura de cuentas) y BULDJOB2 (catalogación de UDC´s de cuentas, grupos y usuarios).
3. Se ejecuta el job BULDJOB1
4. Restauración de las cuentas de infraestructura de herramientas de software COGNOS (power house) , ROBELLE (Suprtool) y VESOFT (mpex/3000)
5. Restauración de la cuenta de NOMINA. Se tuvieron problemas con la información, por lo que se utilizó 1 hora.
6. Ejecución del job BULDJOB2.

TIEMPO UTILIZADO : 1:50 hrs.

5. De 11:25 a 12:00 hrs.

Verificación, por parte de usuarios e Recursos Humanos, de la información restaurada; así como captura de una muestra de datos del día 9 de enero.

TIEMPO UTILIZADO : 0:35 hrs.

6. De 12:07 a 13:37 hrs

Proceso de ejecución de jobs de Nómina.

TIEMPO UTILIZADO : 1:30 hrs.

7. De 12:02 a 12:46 hrs.

Restauración de las cuenta CINTERNO (contabilidad), al día 11 de enero.

TIEMPO UTILIZADO : 0:44 hrs.

8. De 13:40 a 14:30 hrs.

Revisión de resultados por parte de los usuarios de Recursos Humanos.

TIEMPO UTILIZADO : 0:50 hrs.

9. De 14:30 a 15:10 hrs.

Comida (solamente para los usuarios).

TIEMPO UTILIZADO : 0:40 hrs.

10. De 15:20 a 16:00 hrs.

Verificación de información por parte de los usuarios de Contabilidad, así como captura de una muestra de datos del día 11 de enero.

TIEMPO UTILIZADO : 0:40 hrs.

11. De 15:20 a 17:20 hrs.

Proceso de ejecución de jobs de CINTERNO.

TIEMPO UTILIZADO : 2:00 hrs.

12. De 17:20 a 18:00 hrs.

Revisión y comparación de resultados de usuarios de Contabilidad.

TIEMPO UTILIZADO : 0:40 hrs.

13. De 18:00 a 18:30

Impresión de $STDLIST, descatalogación de UDC's, desinstalación de las aplicaciones de Contabilidad y Recursos Humanos. Comentarios con personal de Hewlett Packard acerca del simulacro.

TIEMPO UTILIZADO : 0:30 hrs.

TIEMPO TOTAL PARA LA REALIZACION DEL SIMULACRO : 9:45 hrs.

Resultados Obtenidos

A) Nivel Lider del Simulacro (Centro de Cómputo y Soporte Técnico).

1. Se minimizó el tiempo de instalación de estructura de cuentas.
2. El tiempo de restauración de la información de las aplicaciones fue bueno.
3. Por error se restauró mal la información de Recursos Humanos (Nómina) por lo que se tuvo que crear de nuevo la estructura de la cuenta y catalogación de UDC´s.
4. Se pudo aprovechar el tiempo, restaurando la segunda aplicación (Contabilidad), aún trabajando usuarios de Recursos Humanos.
5. Se tuvo buena coordinación entre el personal de Soporte Técnico y Operación, con actividades bien definidas.
6. Buena coordinación y comunicación entre usuarios, Soporte Técnico y Operación.
7. Se presentaron problemas como una impresora de otro modelo no conocido por Operación, que en ese momento tuvo que aprender su manejo, lo cual no implicó mucho tiempo.
8. En general, le tomó poco tiempo a Soporte Técnico y Operación tener completo dominio sobre el equipo del site backup.
9. Se imprimieron todos los reportes, tanto los obtenidos en cada área, asi como todos los $STDLIST de los procesos batch que se ejecutaron.

B) Nivel usuarios (Contabilidad y Recursos Humanos).

1. No implicó ningún cambio al usuario, ya que las terminales instaladas en el área del site backup, correspondientes a usuarios, son iguales a las utilizadas en el Centro Comercial.
2. Se probaron las aplicaciones de Nómina y Contabilidad.
3. Hubo suficiente espacio para trabajo de los usuarios.
4. Se trabajó con seriedad.

5. Para las dos áreas, se ejecutó bien sus aplicaciones : pantallas de captura, jobs, procesos tanto en Cobol como en Power House.

C) Nivel Hewlett Packard (Site Backup)

1. Buenas instalaciones, el equipo que se asignó para el simulacro en el site backup fue suficiente, a reserva de mandar a Hewlett Packard una lista de sugerencias para mejorar el servicio.

2. Se contó con el respaldo del área de Ingeniería para cualquier eventualidad como la impresora.

3. Hewlett Packard dio seguimiento al simulacro, para posteriormente dar su opinión y recomendaciones.

4. En todo momento el personal de Hewlett Packard estuvo pendiente de las necesidades del Centro Comercial.

5. Hubo servicio de cafetería todo el tiempo.

6. Se tuvo disponible el comedor para realizar la comida.

7. En general, las condiciones de las instalaciones fueron adecuadas.

PROBLEMATICA ENCONTRADA.

A) Nivel Lider del Simulacro (Centro de Cómputo y Soporte Técnico).

1. Considerar más medios de almacenamiento digital de datos (DDS: Digital Data Storage) y cintas magnéticas scratch para respaldos temporales.

2. Todas las XL's de cada aplicación se encontraban en el grupo PUB de cada cuenta, esto dio lugar para revisar todas las cuentas de producción en todos los equipos, HP3000 del Centro Comercial, esto es para estandarizar y mejorar el manejo de la información.

3. Anotar en el Plan de Contingencias que se debe suprimir el programa SOCE0200.OBJETO.SOPORTEC del job del cálculo de la Nómina (OPJB3200), cuyo propósito es verificar que no existan usuarios conectados a la aplicación cuando se va a ejecutar el job.

4. Anotar en el Plan de Contingencias que se debe omitir de las UDC's que ejecuten QUICK, la referencia XL de STREAMX de Vesoft llamada STREAMX.PUB.VESOFT.

5. A partir del job que crea la estructura de cuentas, hacer otro que borre éstas, y del job que cataloga las UDC's de las estructuras, crear uno que descatalogue.

6. Verificar si algún sistema tiene llamados al intrinseco VECMMND, para realizar pruebas para saber como se comporta SECURITY/3000.

B) Nivel Usuarios (Contabilidad y Recursos Humanos)

1. Por parte de los usuarios de Recursos Humanos, estos capturaron lo que consideraron conveniente para ellos.

2. No hubo ningún problema por parte de los usuarios de Contabilidad.

3. En general, los usuarios trabajaron con seriedad y responsabilidad para este simulacro.

4. Los usuarios de Recursos Humanos y Contabilidad, tuvieron que dedicarle tiempo al personal de Auditoria, para explicarles cómo funcionan sus aplicaciones y de esta manera tratar de auditar las mismas, lo anterior provocó atraso por parte de los usuarios y en un momento dado que se perdiera el objetivo de la visita.

C) Nivel Hewlett Packard (site backup)

1. No se tenía conectada la impresora asignada al equipo de respaldo y además de ser nuevo, por lo que los ingenieros tardaron un poco en configurarla, y al tratar de hacerlo, el equipo falló y se tuvo que restablecer de nuevo.

CONCLUSIONES

Contar con un Plan de Seguridad, implica tomar decisiones significativas antes de cualquier Desastre, contar con lineamientos previamente definidos, que a su vez permitan adecuarse a las circunstancias particulares del momento, y no realizar esta actividad cuando ocurra el Desastre. Cada día son más las Empresas, que reconocen la necesidad de contar con un Plan de Seguridad para casos de Desastre, que no solo abarque el Centro de Cómputo sino todas las áreas operacionales de la Empresa.

Por lo que al desarrollar e implantar este Plan de Seguridad hemos encontrado que toda empresa que cuente con un buen Plan de Seguridad le proporcionará las siguientes ventajas :

- Agilizar los procedimientos del Proceso de Recuperación y por lo tanto resuperar la operatividad de una Empresa en el menor tiempo posible.
- Proporcionar lo más rápido posible, soporte a las áreas críticas de una Empresa.
- Registrar mínimas pérdidas económicas o de información en caso de Desastre.
- Identificar los Procesos y Aplicaciones Críticas dentro del Portafolio de Aplicaciones de la Empresa y sus prioridad a recuperar.
- Tener documentado los Recursos Humanos, técnicos y materiales mínimos requeridos para la operación de los Procesos y Aplicaciones Críticas en una situación de Desastre.
- Establecer medidas altemas de Recuperación en caso de Desastre.
- Contar con personal capacitado para actuar en situación de Desastre.
- Poder realizar simulacros para probar la efectividad del Plan y los procedimientos del Proceso de Seguridad.
- Actualizar en forma periódica la información crítica de la Empresa.
- La seguridad de la información de una Empresa se convierte en una responsabilidad de todos, no solo del área funcional asignada a esta tarea.
- Se concientiza a todas las personas de lo importante que es tener un buen respaldo de toda la información.
- Establecimiento de políticas y procedimientos bien definidos y debidamente actualizados, así como elaboración de manuales con el fin de poder consultarlos y resolver posibles dudas en cualquier momento.

Una parte muy importante del Plan de Seguridad es la realización de Simulacros de Recuperación de Información, que nos permite corregir deficiencias que se llegarán a encontrar en el Plan, ya que no se conoce que tan bien funciona el Plan de Seguridad hasta que se prueba, por lo que el Plan de Seguridad ya no es solamente un documento técnico , si no que se convierte en un documento dinámico y práctico al efectuar el simulacro.

El realizar Simulacros presenta las siguientes ventajas:

- Demuestra que el Plan está documentado de tal manera que permite la adecuada recuperación de las aplicaciones críticas en caso de un Desastre.
- Permite ajustar los planes de Recuperación en respuesta a los problemas y deficiencias encontradas durante la prueba.
- Confirma las espactativas de Alta Dirección en cuanto al soporte del procesamiento de la información durante la Recuperación.

En consecuencia, llegamos a establecer que cualquier empresa que no cuente con un Plan de Seguridad puede enfrentarse a las siguientes situaciones de riesgo:

- Registrar importantes pérdidas económicas y de información.
- No tener identificadas las áreas críticas de la Empresa.
- No procesar las Aplicaciones Críticas de la Empresa durante un periodo de tiempo.
- Tomar decisiones precipitadas y posiblemente incorrectas.
- Actuar sin planeación previa.
- No contar con un Centro de Soporte Alterno.
- No contar con personal capacitado para actuar en situaciones críticas.

A continuación se mencionan otros aspectos que resultan relevantes en la elaboración de un Plan de Seguridad:

- Cada vez que se establezca o se reubique un Centro de Cómputo es necesario definir todos los posibles riesgos a los que se puede enfrentar, por falta de algún tipo de seguridad.

- Hay que tener en consideración que los medios o dispositivos con los que se cuenten para ampliar la seguridad física siempre serán convenientes tenerlos enlazados con elementos de seguridad externa tales como policía, bomberos, etc.

- El área o departamento que se encargue de las contrataciones de todo tipo de individuos, deberá tener bien definidas todas las cláusulas que restrinjan al máximo cualquier intento de violación a dicho contrato en lo referente a la seguridad de software y hardware con el fin de liberar de toda la responsabilidad a la empresa y proceder como lo estipula la ley y sus a autoridades.

- Si se define un buen plan contra contingencias el grado de vulnerabilidad de nuestro equipo e información es menos susceptible de algún daño y si existe algún percance, contar con los medios necesarios de respaldo para echar andar de nuevo esa área y no se vea interrumpido el servicio por un tiempo muy prolongado.

- Es necesario realizar simulacros con el fin de que se puedan prevenir circunstancias impredecibles y con esto poder definir soluciones que quizá en el momento de algún atentado no se tuviera una solución óptima debido a que podría traer fuertes consecuencias la carencia de éstos.

- Los altos mandos de las compañías deberán estar informados de lo importante que este tener definido un buen sistema de seguridad, debido a que la carencia de información acerca de este tema puede ser muy costosa e improductiva.

- La capacitación resulta un factor motivante para el empleado, ya que con esto se le demuestra que se le toma en cuenta y por lo general resulta altamente productivo para ambas partes.

ANEXOS

ANEXO A

PRINCIPALES CARACTERISTICAS DEL PROCESADOR DE PROTOCOLOS TP3/II-3325E

El procesador de protocolos TP3/II'3325E tiene como caracteristicas principales:

- Funciona como un concentrador de líneas y convertidor de protocolos.

- Como concentrador de líneas permite conectar estaciones y reconfigurar el sistema. También se encarga de aislar los nodos problemáticos mediante el punto de concentración.

- Un convertidor de protocolos es aquél que se encarga de efectuar una traducción de un protocolo a otro.

- Es un sistema de tarjetas múltiples basado en el microprocesador Zilog Z-80 con 512 bytes de memoria RAM, y múltiples microprocesadores Zilog Z80-B con 256 Kbytes de memoria cada uno.

- Puede soportar hasta 4 PAD's (packet assembler / disassembler) diferentes.

- Se le puede conectar 48 equipos terminales de datos a una velocidad hasta de 19.2 Kbps mediante 4 LPU's (Line Processor Unit) en donde cada LPU tiene su propio PAD.

- Cada LPU se compone de una APB (Tarjeta Madre) que soporta 4 líneas para DTE's y hasta 2 AEB's (Access Processor Board, tarjeta hija) que también soporta 4 líneas para DTE's cada una.

- Las tarjetas APB (Access Processor Board) y AEB tiene como función principal ensamblar y desensamblar paquetes (PAD) para puertos de baja velocidad con soporte para diversos protocolos.

- Adicionalmente se le puede instalar una sola tarjeta XEB (X.25 Expansión Board) que soporta hasta 4 líneas de usuario e interactuar con las troncales de salida de alta velocidad X.25, así como alojar la memoria principal del TP3325.

- La tarjeta AXPB (Advanced X.25 Processor Board) actúa como administrador y tiene la capacidad de cargar software hacia tarjetas APB y AEB cuando así se requiera. El sistema TP3325 permite efectuar esta carga local de software. Soporta 2 puertos RS232C o 2 puertos V.35 para troncales dúplex hacia la red.

- De acuerdo con el PAD encontrado en un LPU del TP3325, se pueden realizar comunicaciones con los siguientes equipos terminales de datos:

    - Terminal asíncrona (PAD terminal IYI-2)
    - Huésped asíncrono (PAD terminal ITI-2)
    - Terminales 2780/3780 o computadores huésped (PAD X7802)
    - Terminales 3270 en multipunto o unidades de control (PAD terminal BSC 3270 DSPII o SNA3270 DSPII).
    - Huéspedes 3270 (PAD huésped BSC3270DSPII o SNA3270 DSPII)
    - Unidades de control SDLC(HPAD terminal o HPAD/QLLC)
    - Huéspedes SDLC/FEP's (HPAD huésped o HPAD/QLLC)

- EL TP3325 se conecta a la red de conmutación de paquetes mediante uno o dos enlaces X.25 DTE utilizando el protocolo HDLC (High-Level Data Link Control). Cada enlace X.25 puede operar hasta 64 Kbps. Las líneas X.25 pueden soportar las siguientes características de configuración :

    - Transferencia de paquetes ID hacia el TP5 con fines contables.
    - Circuitos Virtuales Conmutados.
    - Cargo revertido.
    - Ventana de tamaño variable de 1 a 7 en cada dirección.
    - Paquete de tamaño variable de 16 a 256 bytes en cada dirección.
    - Facilidades opcionales de X.25
    - Direccionamiento mediante X.121
    - Conmutación local, utilizando la versión adecuada de software.

- La configuración mínima de un TP3325 consiste de una tarjeta AXPB, una tarjeta APB, un chasis con fuente de poder y sistema de enfriamiento.

- Su capacidad en manejo de información alcanza los 120 paquetes por segundo.

ANEXO B

CARACTERISTICAS DEL CONMUTADOR DE PAQUETES TP4/II-4255

El conmutador de paquetes TP4/II-4255 tiene las siguientes características:

- Los conmutadores de paquetes TP4 otorgan los servicios de:
  - Conversión de protocolos,
  - Multiplexaje de datos,
  - Conmutación / enrutamiento de datos,
  - Acceso de terminales y
  - Computadores huésped de la red.

- El conmutador TP4/II-4255 en su versión doble tiene hasta 30 ranuras para instalar LPU's a fin de poder contar un máximo de 224 puertos y manejar hasta 820 paquetes por segundo.

- Manejan líneas hasta una velocidad de 64 Kbps.

- Pueden establecer hasta 32 circuitos virtuales por segundo.

- El TP4255 es un conmutador de distribución utilizado para efectuar conmutación en la red sobre líneas troncales. También puede utilizarse como conmutador final para comunicarse con DTE's X.25, STE's X.75 o líneas X.25.

- EL TP4255 puede ser configurado para comunicarse con dispositivos síncronos y asíncronos que no funcionan en modo paquete mediante el uso de los PAD's adecuados. Además este conmutador puede servir como interfaz para aparatos que funcionan en modo paquete que se conecten en red. Las principales componentes del TP4255 son :

  - Unidad Central de Procesamiento (CPU). Es el responsable de correr el sistema operativo maestro y del proceso del nivel 3 del protocolo X.25 para todos los circuitos virtuales que maneja el conmutador.
  - La Unidad Arbitro-Memoria está compuesta por la tarjeta árbitro y la tarjeta de memoria principal, trabajando como una sola unidad. Las LPU´s y la CPU no pueden accesar la memoria principal si no pasa a través del árbitro.
  - Unidades de Procesamiento en Linea (LPU). Esta tarjeta que maneja 8 líneas de baja velocidad asíncronas (LSLPU), tiene las funciones PAD y X.25 necesarias para manejar los dispositivos que no funcionan en modo paquete. Las LPU de 4 líneas de velocidad media, síncronas por bytes (MSLPU), tienen las funciones PAD y X.25 necesarias para manejar los dispositivos bisíncronos que no funcionan en modo paquete. Las LPU de 8 líneas de alta velocidad, síncronas por bit (HSLPU), tienen la función X.25 necesaria para manejar los dispositivos que funcionan en modo paquete y los paquetes internos de la red.

ANEXO C

CARACTERISTICAS PRINCIPALES DEL CENTRO DE CONTROL DE RED TP5

Las caracteristicas principales del Centro de Control son:

- Cada red dedicada de conmutación de paquetes se monitorea con un centro de control de Red mediante el cual se manejan sus funciones. El sistema de administración de la red (NMS), es un computador de propósito general que tiene un software especialmente diseñado para manejar las tareas administrativas de una red de esta naturaleza.

- El NMS realiza diversas funciones como el cargado remoto del software de red en los nodos al inicializarse o en caso de falla de éstos, recibe datos estadísticos para la evaluación fuera de linea de la red e inicializa los comandos que diagnostican el mal funcionamiento del hardware y/o software y la alteración del estado operacional del equipo.

- Cada TP5 es capaz de comunicarse directamente con su red de conmutación de paquetes, a través de una interfaz de comunicación X.25. Este usa una interfaz X.25 para intercambiar información y comandos con los TP3s y TP4s para conocer su estado.

- Otorga reportes y alarmas de eventos fáciles de comprender por los operadores de la red.

- También contiene el software para el monitor a color de la red que permite visualizar el estado que guardan las componentes de la misma. Su característica de acercamiento facilita al personal del Centro de Control, verificar cualquier área, nodo, tarjeta, puerto o circuito virtual de la red.

- Las tarjetas para conmutación de interfaz conmutan las líneas de una LPU dañada a otra de resplado, además sirve de interfaz entre la LPU las líneas de comunicación.

- Tiene inteligencia para aislar y reemplazar una componente en falla con una unidad de respaldo y diagnosticar la causa de la falla. Esta función se da automática y rápidamente sin intervención de la red.

BIBLIOGRAFIA.

Libros.

Fine, Leonard H.
Seguridad en Centros de Cómputo. (Políticas y procedimientos).
México 1990, Editorial Trillas, 126 Págs.

Echenique, José Antonio.
Auditoria en Informática.
México 1994, Editorial Mc Graw Hill, 158 Págs.

Murdick, Robert G.
Sistemas de Información Administrativa.
México 1988, Editorial Prentice Hall, 716 Págs.

David H. Li.
Auditoria en Centros de Cómputo.
México 1992, Editorial Trillas, 176 Págs.

Uyless Black.
Redes de Computadora (Protocolos, Normas e Interfaces).
México 1991, Editorial Macrobit, 421 Págs.

Tesis.

Zoé Tercero Rodriguez.
Plan de Contingencias en Caso de Desastre para la continuidad del negocio de una organización.
México 1992, Universidad La Salle, 97 Págs

Sandra Jacobo Mina.
Consideraciones para la implantación de un departamento de Sistemas básico, Basado en Minicomputadoras HP-3000.
México 1993, Universidad Lasalle 120 Págs.

Seminario.

Edmon Jones.
Oficce Automation "" Information Security".
ITESM, CAMPUS ESTADO DE MEXICO.

Articulos.

Michel Dobberslein
Computer Decision; Vol. 17.
10 de Septiembre 1985, 102-106 Págs.

Mary Tonne Schaeffer.
Información retrieval & Library.
Automatión; Vol. 21.
Septiembre de 1985, 1-4 Págs.

Stan kolodziej
Mejorando la Seguridad de Redes.
Computer World Focus; Vol. 20.
15 de Enero de 1986, 37-39 Págs.

Gordon Mclachlan
Don't Let Disaster Recovery Plans
Simer on A Back Borner.
Hp Professional ; Vol 5 No.2
Febrero de 1991, 26-32 Págs.

Sandra Jacobo Mina.
Consideraciones para la implantación de un departamento de Sistemas básico, Basado en Minicomputadoras HP-3000.
México 1993, Universidad Lasalle 120 Págs.

Seminario.

Edmon Jones.
Oficce Automation " Informatión Security".
ITESM, CAMPUS ESTADO DE MEXICO.

Articulos.

Michel Dobberslein
Computer Decision; Vol. 17.
10 de Septiembre 1985, 102-106 Págs.

Mary Tonne Schaeffer.
Informatión retrieval & Library.
Automatión; Vol. 21.
Septiembre de 1985, 1-4 Págs.

Stan kolodziej
Mejorando la Seguridad de Redes.
Computer World Focus; Vol. 20.
15 de Enero de 1986, 37-39 Págs.

Gordon Mclachlan
Don't Let Disaster Recovery Plans
Simer on A Back Borner.
Hp Professional ; Vol 5 No.2
Febrero de 1991, 26-32 Págs.