UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

INGENIERIA EN COMPUTACION

VEGA PRADO JOSE ANTONIO

ANALISIS, DISEÑO Y DESARROLLO DE UN PLAN DE RECUPERACION DE DESATRES PARA EMPRESAS CON INFORMACION TECNOLOGICA.

DIRECTOR DE TESIS.- ING. CARLOS SAUCEDO MACIEL

México D.F Septiembre de 2003

TEMARIO

INTRODUCCION

Con el paso del tiempo la Tecnología Informática ha ido ampliando su espectro de operación, hasta convertirse en elemento esencial en cualquier tipo de organización. No sabemos hasta donde llegará la importancia de las computadoras en la sociedad, pero lo que si sabemos es que mientras mas vital sea su función, más importante será el protegerlas de fallas, catástrofes, crímenes, etc. Sin este tipo de tecnologías las empresas y los gobiernos podrían quedar totalmente varados e imposibilitados de realizar sus tareas primordiales de operación.

En la actualidad, la computación se aplica a funciones contables, de manufactura, diseño, publicidad, distribución, etc. en las empresas, esto ha provocado una creciente dependencia hacia esta tecnología. En la medida que esta dependencia se incrementa, también se incrementa el riesgo financiero asociado a una pérdida de la capacidad de procesamiento de datos dentro de una organización, por esta razón los ejecutivos de las empresas deben de prestar especial cuidado con respecto a la seguridad de la información. Este es el propósito de un Plan de Recuperación.

Un Plan de Recuperación tiene como objetivo principal recuperar la operatividad de la empresa en el menor tiempo y costo posible, es decir permite que la empresa pueda enfrentarse a una situación de contingencia de manera efectiva.

En el presente trabajo de investigación se presentan los elementos que constituyen un Plan de Recuperación, así como también se desarrollan cada uno de estos elementos.

En el capítulo uno se menciona la importancia de los sistemas de información en la actualidad y la necesidad de salvaguardar la información mediante medidas de prevención. Se describen los riesgos que afectan la seguridad de las instalaciones físicas de cómputo. Además de mencionar los riesgos que afectan la seguridad de la información en si, a esto se le conoce como seguridad lógica.

En el capítulo dos se presenta el marco conceptual del Plan de Contingencia; en él se incluyen varios conceptos que el diseñador del plan debe conocer antes de comenzar el desarrollo del mismo. Adicionalmente se mencionan las ventajas que representa contar con un Plan de Continencia.

En el capítulo tres se presentan una serie de herramientas enfocadas al desarrollo de este tipo de Planes de Contingencia, así como a la administración de éstos, que se encuentran disponibles en el mercado. Dichas Herramientas se clasifican de acuerdo a sus características: Creación y mantenimiento de Planes Globales de Contingencia, Recuperación de Redes de Computadoras, Estrategias de Respaldo y Almacenamiento de Información.

En el capítulo cuatro Desarrollo de Plan de Recuperación; se mencionan los pasos de la metodología para el desarrollo del Plan de Contingencia que abarca el análisis de impacto al negocio, la determinación de procesos y aplicaciones criticas, el alcance del Plan de Contingencia, la estructuración de Comités de Recuperación, así como la determinación del centro de soporte alterno óptimo para la organización.

En el capítulo cinco se definen los simulacros y la importancia de ejecutarlos para medir de manera objetiva la eficiencia del Plan de Recuperación.

Es muy importante el mantenimiento al plan de recuperación, ya que de esto dependerá el éxito en la restauración de la operatividad de la empresa en cualquier momento que ocurra una contingencia. Lo anterior esta documentado en el capítulo seis llamado Mantenimiento y Actualización.

En el capítulo siete se mencionan las conclusiones de este trabajo de investigación, después de implementar un Plan de Recuperación de Desastres para la empresa Grupo Galaxy Mexicana S.A. de C.V. mencionando lo importante que para esta empresa es contar con un plan de este tipo.

En el apéndice A se describe el caso práctico de la empresa Grupo Galaxy Mexicana S.A. de C.V, desarrollando cada uno de los pasos mencionados en la metodología propuesta mencionada en el capítulo cuatro.

Contar con una herramienta de apoyo al mantenimiento y a la actualización del Plan de Recuperación resulta de gran utilidad ya que optimiza el manejo de la información y agiliza el proceso de documentación. Por esta razón en el Apéndice B se presenta la documentación técnica del Programa SOFDRP, desarrollado para los fines anteriormente mencionados.

Capítulo 1.
Importancia de la Información.

1.1 Grandes avances de la Tecnología en Información.

Las tecnologías de la información, actualmente son elementos fundamentales para la superación y desarrollo de un país. Por eso, los países desarrollados basan su crecimiento en la aplicación y la programación estratégica de las herramientas computacionales y han definido políticas que los inducirán a su permanencia en el dinamismo mundial de los próximos años.

Ante el nuevo entorno económico mundial los países emergentes están obligados a preparar profesionales en áreas de la informática y las telecomunicaciones, capaces de enfrentar los retos que se tienen hoy en día. Asimismo, la presencia de la computación en los sectores productivos es un factor determinante para su funcionamiento.

Por otra parte, la Informática está tan popularizada que es muy difícil que una empresa adquiera una ventaja competitiva por tener computadoras más potentes o una red más extensa. La ventaja competitiva se logra con un uso más eficiente de la tecnología y, por supuesto, optimizando la gestión del negocio y/o empresa.

En esta época de la globalización, la información y la comunicación se han transformado en unas de las más significativas fuentes de riqueza y a la vez en factores de la producción. El mercado de la tecnología de la información se expande y más gente se llega a comunicar rápida e intensivamente. La nueva economía es una revolución tecnológica, económica y de negocios, en donde aquellas compañías que no adopten los nuevos modelos de negocios se quedarán atrás.

En la actualidad los avances tecnológicos son un factor determinante para el logro de las operaciones en un entorno empresarial, las empresas están comprometidas a ofrecer a sus clientes mayor valor de servicio y calidad para lograr esto, realizan grandes inversiones en infraestructura tecnológica e informática.

Cada día más y más funciones vitales para la sociedad están basadas en la tecnología de la información. Mientras más aprovechemos este poderoso recurso e integremos sistemas de cómputo a nuestros procesos operativos y administrativos, más importante se volverá la seguridad de la información. Surgiendo así una necesidad real para incrementar el conocimiento de los temas referentes a seguridad y vulnerabilidad de la información.

La convergencia entre estilos de comunicaciones, históricamente diferenciados, ha sido provocada por la electrónica y la digitalización de los mensajes. Los sonidos y las imágenes pueden ser clasificados y transmitidos como impulsos digitales. Las computadoras pueden manejar estas grandes masas de señales digitales que representan texto, voz o imágenes, con mucha más flexibilidad que en papel.

Estas señales se pueden almacenar en memorias, convertir de formato y transmitir instantáneamente por una red informática.

Por otra parte, según un estudio de la empresa Trends Consulting-IDC Argentina, Estados Unidos y Suecia encabezan la lista de los, informáticamente, mejor preparados entre los países evaluados. Argentina, ubicada dentro del promedio de las naciones evaluadas, es el país de América Latina mejor posicionado para aprovechar las oportunidades de la Revolución de la Información. Asimismo, dentro de los países de la región, el que sigue a la Argentina en su posición es Chile.

En dicho estudio, la citada consultora sostiene que la Revolución de la Información modificará substancialmente la economía del mundo globalizado en los próximos veinte años, exigiendo niveles sin precedentes de compromisos y habilidades. En ese sentido, las inversiones de infraestructura social, de comunicaciones y de computación que cada país haga en la próxima década, determinarán si la nueva era satisface las expectativas, o simplemente marca una nueva división entre países que cuentan y los que no cuentan.

El índice de Imperativos de la Información, señala el referido estudio, se estructura a partir de veinte variables que se sintetizan en un indicador, el progreso de los países hacia una economía adecuada a la nueva ola impulsada por la tecnología informática. Las veinte variables se dividen en tres categorías de infraestructuras críticas (por Ej.: escolaridad, libertad de prensa, derechos civiles), de comunicaciones (líneas telefónicas familiares, fallas en las líneas telefónicas, teléfonos celulares per capita y otros semejantes) y de computación (computadoras instaladas por habitante, porcentajes de computadoras en red, inversiones de hardware/software, cantidad de nodos de Internet, etc.).

En definitiva, la tecnología informática define e impulsa la nueva era, rediseña el marco que se utiliza para describir la realidad. Todos los problemas importantes del hombre se pueden convertir en problemas informáticos. Todo está interconectado, es complejo e interdependiente, la efectividad de los sistemas descansa en la seguridad y protección de la comunicación.

Las computadoras son el epicentro de nuestras vidas. Están en nuestros escritorios, en nuestros bolsillos y aún en los tableros de nuestros autos. Las usamos para trabajar, para jugar, para la educación y para ordenar datos. Y sabemos que las computadoras han calado profundo en la cultura popular.

Pero, ¿Cómo la raza humana a evolucionado a una especie tecnofílica? Las opiniones varían de extremo a extremo. Algunos dicen que fue Apple cuando en 1984 introdujo la Macintosh -- "La computadora para el resto de nosotros" -- Otros dicen que empezó antes, con la primera PC de IBM. Algunos académicos apuntan a 1975 con la aparición de un kit de computadora por Altaír en la portada "Popular Electronics". Este movimiento lanzó una pequeña empresa de programadores llamada Microsoft.

Realmente no es ninguna de estas cosas. Hoy día cuando comemos RAM en el desayuno y nos trasladamos en un conmutador cada mañana, sabemos que la computación empezó mucho antes, alrededor del año 20,000 AC, de hecho. Hemos dependido por muchísimo tiempo de aparatos que hacen cálculos y otros trabajos que nuestro cerebro lo haría con gran esfuerzo.

1.2 Necesidad de salvaguardar la Información.

A partir de la década de 1950, con el surgimiento de la computadora comercial. Las computadoras han tenido cada vez mayor importancia en los procesos administrativos y productivos de las empresas en industrias; es decir, el progreso de la computación ha sido explosivo. Los sistemas de información son ahora componente básico de todos los negocios.

Concepto de Información.

Información es una palabra usada de muchas maneras, pero en relación con el procesamiento electrónico de datos (EDP por sus siglas en ingles), significa “datos recopilados y presentados de modo que contengan un significado” [Daler, T. 1989]

Un sistema efectivo de información basado en EDP que puede producir la información correcta para la persona indicada en el tiempo necesario, apoyando (o habilitando) la toma de decisiones correcta, se ha vuelto uno de los factores competitivos mas importantes en estos días.

Manejo de la Información.

La información y los sistemas de información son muy valiosos. Por lo tanto deberían de ser tratados como un recurso estratégico. Toda la información debe ser protegida para asegurar la credibilidad junto con la calidad y precisión al usuario. El responsable de la seguridad de la información es el “propietario” de la información. [Daler, T. 1989].

Una de las razones por las que la computación ha tenido tan exitosa irrupción en el mundo de los negocios ha sido que resulta de gran utilidad para el manejo de la información, en especial de grandes volúmenes de esta. Y ello cobra más importancia cuanto mayor es el valor de esta información para las empresas.

Un hecho que goza de aceptación generalizada en la actualidad, es que después del personal, la información el recurso más importante para cualquier organización. Por otro lado un objetivo de la administración, es optimizar la utilización de los recursos, para obtener resultados que se reflejen en ventajas competitivas para la organización. Uniendo las dos premisas anteriores, llegamos a la conclusión de que la administración eficiente de la información en una empresa es determinante para el éxito de la misma.

Al hablar de administración de la información estamos incluyendo procesos como la obtención, organización, procesamiento, almacenamiento, y entrega de los resultados en los tiempos y formas requeridos de forma continua. Esto nos lleva irreversiblemente a incluir aspectos relacionados con la seguridad de la información y la necesidad existente de salvaguardarla.

Es de suma importancia que la información esté disponible en cualquier momento; es decir, que exista la información y que existan los medios necesarios para tener acceso a ella. En otras palabras, hay que asegurar el uso de la información.

La computación es una herramienta fundamental para el manejo de información en las empresas de hoy; por lo tanto asegurar la información implica asegurar la disponibilidad en el uso del equipo de cómputo que la maneja, así como los medios que la contienen.

El no contar, por cualquier causa, con el equipo de cómputo, implica no poder utilizar la información, lo que equivale a no tenerla, es evidente que las consecuencias de esto son graves y las estadísticas así lo demuestran.

En promedio una compañía que registra una suspensión del servicio de cómputo que dura más de 10 días nunca se recuperará totalmente. 50 % de ellas estarán fuera del negocio por 5 años.

Las oportunidades de sobrevivir a un desastre que afecte al centro de procesamiento de datos son menos de 7 en 100.

La seguridad de la información tiene como meta proteger los activos o recursos de las organizaciones de pérdida y asegurar la viabilidad de las operaciones de la organización si ésta llegara a ocurrir. William Stallings define seguridad de la información como “el nombre genérico para el conjunto de herramientas diseñadas para proteger los datos”.

Los recursos o activos que deben protegerse de pérdida son la información y el equipo, siendo más importante la primera. Por lo tanto, cuando hablamos de pérdida de estos recursos no estamos refiriendo a daño o divulgación no autorizada de información (intencional o no) y pérdida de medios físicos. Existen también otras causas de “accidentes” informáticos como son: errores del operador, errores o mal funcionamiento de hardware, errores en el software, errores en los datos, daños a las instalaciones, “performance” inadecuado del sistema, etc.

La seguridad de la información también tiene como objetivo combatir lo que se ha dado en llamar “crimen por computadora”. El crimen por computadora puede dirigirse al software, a los datos o al hardware.

Para protegernos de esta vulnerabilidad necesitamos medidas de seguridad, controles administrativos y el especial cuidado de cada uno de nosotros.

Posiblemente existen personas que no creen en lo anterior u otros que creyéndolo no se han percatado de la importancia que tiene. Al leer este capítulo, el lector se dará cuenta de la necesidad de tener seguridad de la información y planes de contingencia, como de la amplitud de estos temas.

1.3 Medidas de Prevención.

El campo de la seguridad presenta nuevos retos a las empresas. Su problemática ha ido ampliándose en los últimos años con los problemas de contaminación en general y de los desastres. La contaminación constituye una seria amenaza no solo a la salud de los pobladores de esta ciudad, sino también a los empresarios, ya que se han convertido en un factor muy importante en la operación de la empresa.

Medidas de Prevención.

A continuación se mencionan algunas de las Responsabilidades Individuales en un Ambiente Corporativo.

- Proteja su terminal cuando no la este usando.- No deje de cerrar la sesión después de completar su trabajo. Si no lo hace es posible que alguien accidental o intencionalmente cause daño o perdida al usar su login.

- Proteja sus equipos.- Mantenga la comida, bebidas y artefactos eléctricos alejados de su computadora y de los medios de almacenamiento.

- Proteja su contraseña (password).- Manténgala en secreto. No la comparta con otros. Nunca escriba su password, ni la coloque cerca de su terminal, ni la guarde en un cajón de su escritorio.

- Proteja sus medios de almacenamiento.- Guarde bajo llave en un gabinete o cajón sus discos flexibles, cintas, casetes e información impresa clasificados como confidenciales o altamente restringidos cuando no se están usando.

- Restrinja el acceso a sus datos según la necesidad de saber.

- Proteja los datos sensibles contenidos en cualquier dispositivo de almacenamiento.

- Ponga etiquetas de clasificación en todos los documentos y medios de almacenamiento.

- Conozca y acate las leyes de propiedad intelectual y las restricciones al uso de licencias. No haga, ni tenga en su posesión duplicados de software de propiedad de la compañía que no sean autorizados o que sean ilegales.

- No hable de información sensible en lugares públicos, tales como ascensores, sanitarios, cafetería o restaurantes.

- Use su tarjeta de identificación y envié las visitas no autorizadas al departamento de seguridad.

1.4 Reducción de los Efectos Negativos.

Pese a todas las medidas de seguridad puede ocurrir un desastre, por tanto es necesario que el un Plan de Recuperación de Desastres, el cual tendrá como objetivo, restaurar el Servicio de Cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles. Solo de esta manera podemos hablar de la reducción de los efectos negativos.

Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo y global posible.

Un Plan de Contingencia de Seguridad Informática consiste en los pasos que se deben seguir luego de un desastre para recuperar, aunque sea en parte, la capacidad funcional del sistema.

Como ya se mencionó, la Seguridad Informática se mantiene gracias a tres pilares básicos: la Seguridad Física, Técnica y Administrativa. El Plan de contingencias será quien sostenga estos tres pilares y la encargada de levantar a cualquiera de ellos que se vea afectado.

El Plan de Contingencia implica un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de cómputo y la información contenida en los diversos medios de almacenamiento.

Análisis de Riesgos.

El análisis de riesgos supone más que el hecho de calcular la posibilidad de que ocurran cosas negativas. Se debe poder obtener una evaluación económica del impacto de estos sucesos. Este valor se podrá utilizar para contrastar el costo de la protección de la información en análisis, versus el costo de volverla a producir (reproducir).

Además se debe tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y cuantificar su potencial desarrollando un plan de acción adecuado.

La evaluación de riesgos y presentación de respuestas debe prepararse de forma personalizada para cada organización.

El análisis de riesgos supone responder a preguntas del tipo:

· ¿Qué puede ir mal?
· ¿Con qué frecuencia puede ocurrir?
· ¿Cuáles serían sus consecuencias?
· ¿Qué fiabilidad tienen las respuestas a las tres primeras preguntas?

Una vez obtenida la lista de cada uno de los riesgos se efectuará un resumen del tipo:

Tipo de Riesgo	Nivel
Robo de hardware	Medio
Vandalismo	Medio
Fallas en los equipos	Medio
Virus Informáticos	Medio
Equivocaciones	Medio
Accesos no autorizados	Medio
Robo de información	Medio
Fraude	Bajo
Fuego	Muy Bajo
Terremotos	Muy Bajo

Según esta tabla habrá que tomar las medidas pertinentes de seguridad para cada caso en particular, cuidando incurrir en los costos necesarios según el factor de riesgo representado.

Niveles de Seguridad.

Un parámetro fundamental en la reducción de efectos negativos que pudieran afectar la operación de una empresa es el poder ubicarla dentro de un estándar o nivel de seguridad, para concientizarnos acerca de la vulnerabilidad de a que estamos expuestos, y sobre todo tomar las medidas necesarias para ir eliminando o reduciendo los efectos no deseados.

El estándar de niveles de seguridad más utilizado internacionalmente es el Orange Book, Desarrollado de acuerdo a las normas de seguridad en computadoras del Departamento de Defensa de los Estados Unidos, en el cual se usan varios niveles de seguridad para proteger el hardware, el software y la información ante un ataque. Los niveles describen diferentes tipos de seguridad física, autentificación y confiabilidad del software y se enumeran desde el mínimo grado de seguridad al máximo. Cabe aclarar que cada nivel requiere todos los niveles definidos anteriormente: así el subnivel B2 abarca los subniveles B1, C2, C1 y el D.

Nivel D

Este nivel contiene sólo una división y está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad. Son sistemas no confiables, no hay protección para el hardware, el sistema operativo es inestable y no hay autentificación con respecto a los usuarios y sus derechos en el acceso a la información. Los sistemas operativos que responden a este nivel son MS-DOS y System 7.0 de Macintosh.

Nivel C1: Protección Discrecional

Se requiere identificación de usuarios permite el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre Usuarios y Administrador del sistema quien tiene control total de acceso.

Muchas de las tareas cotidianas de administración del sistema sólo pueden ser realizadas por este usuario llamado raíz (Root); quien tiene gran responsabilidad en la seguridad del mismo. Con la actual descentralización de los sistemas de cómputo, no es raro que en una organización encontremos dos o tres personas que conocen la contraseña raíz. Esto es un problema, pues no hay forma de distinguir entre los cambios que hizo cada usuario.

A continuación se enumeran los requerimientos mínimos que debe cumplir la clase C1:

Acceso de control discrecional

Distinción entre usuarios y recursos. Se podrán definir grupos de usuarios (con los mismos privilegios) y grupos de objetos (archivos, directorios, disco) sobre los cuales podrán actuar usuarios o grupos de ellos.

Identificación y Autentificación:

Se requiere que un usuario se identifique (mediante passwords) antes de comenzar a ejecutar acciones sobre el sistema. El dato de un usuario no podrá ser accedido por otro usuario sin autorización o identificación.

Nivel C2: Protección de Acceso Controlado

Este subnivel fue diseñado para solucionar las debilidades del C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoria de accesos e intentos fallidos de acceso a objetos. Tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización.

Requiere que se audite el sistema. Esta auditoria es utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios. La auditoria requiere de autenticación adicional para estar seguros de que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos.

Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de la contraseña raíz. Permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.

Nivel B1: Protección Estructurada

Requiere que se etiquete cada objeto de nivel superior por ser padre de un objeto inferior. La Protección Estructurada es el primera que empieza a referirse al problema de un objeto a un nivel mas elevado de seguridad en comunicación con otro objeto a un nivel inferior. Así un disco duro será etiquetado por almacenar archivos que son accedidos por distintos usuarios.

Nivel B2: Dominios de Seguridad

Refuerza a los dominios con la instalación de hardware: por ejemplo el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos diferentes dominios de seguridad. Existe un monitor de referencia que recibe las peticiones de acceso a cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido, todas las estructuras de seguridad deben ser lo suficiente pequeñas como para permitir análisis y pruebas ante posibles violaciones. Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una conexión segura.

Nivel A: Protección Verificada

Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema. Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

1.5 Seguridad de la Información Física y Lógica

Es muy importante ser consciente que por más medidas de seguridad que nuestra empresa tenga implementadas, siempre estará expuesta a riesgos que podrían ser catastróficos para su continuidad, si no se hace un estudio minucioso que pueda disminuir su exposición al riesgo, la seguridad de la misma será nula si no se han previsto puntos como los que se describen a continuación:

1.5.1 Seguridad Física.

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos de seguridad se prevén, otros no, como la detección de un atacante interno a la empresa que intenta a acceder físicamente al site de operaciones.

Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta del site de operaciones, que intentar acceder vía lógica a la misma. Así, la seguridad física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial".

Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo, implementados para proteger el hardware y medios de almacenamiento de datos. No será la primera vez que se mencione en este trabajo, que cada sistema es único y por lo tanto la política de seguridad a implementar no será única. Este concepto vale, también, para el edificio en el que nos encontramos. Es por ello que siempre se recomendarán pautas de aplicación general y no procedimientos específicos.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro de producción y procesamiento de datos.

Las principales amenazas que se prevén en la seguridad física son:

1. Desastres naturales, incendios accidentales tormentas e inundaciones.
2. Amenazas ocasionadas por el hombre.
3. Disturbios, sabotajes internos y externos deliberados.

Ya se trate de actos naturales, errores u omisiones humanas y actos intencionales, cada riesgo debería ser atacado de las siguientes maneras:

1. Minimizando la posibilidad de su ocurrencia.
2. Reduciendo al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.
3. Diseño de métodos para la más rápida recuperación de los daños experimentados.
4. Corrección de las medidas de seguridad en función de la experiencia recogida.

Para ello analizaremos los peligros más importantes que se corren en un centro de procesamiento, con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

No hace falta recurrir a películas de espionaje para sacar ideas de cómo obtener la máxima seguridad en un sistema informático, además de que la solución será extremadamente cara. A veces basta recurrir al sentido común para darse cuenta que cerrar una puerta con llave o cortar la electricidad en ciertas áreas siguen siendo técnicas válidas en cualquier entorno.

Incendios.

Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas. El fuego es una de las principales amenazas contra la seguridad.

El fuego es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas. Desgraciadamente los sistemas antifuego dejan mucho que desear, causando casi igual daño que el propio fuego, sobre todo a los elementos electrónicos. El dióxido de carbono, actual alternativa del agua, resulta peligroso para los propios empleados si quedan atrapados en la sala de cómputo.

Los diversos factores a contemplar para reducir los riesgos de incendio a los que se encuentra sometido un centro de cómputos son:

1. El área en la que se encuentran las computadoras debe estar en un local que no sea combustible o inflamable.
2. El local no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
3. Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.
4. Debe construirse un "piso falso" instalado sobre el piso real, con materiales incombustibles y resistentes al fuego. El espacio entre ambos debe pintarse y mantenerse limpio permanentemente.
5. No debe estar permitido fumar en el área de proceso.
6. Deben emplearse muebles incombustibles, y cestos metálicos para papeles. Deben evitarse los materiales plásticos e inflamables.
7. El piso y el techo en el recinto de ubicación de la computadora y de almacenamiento de los medios magnéticos deben ser impermeables.

Seguridad del Equipamiento.

Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados. Para protegerlos se debe tener en cuenta:

La temperatura no debe sobrepasar los 18º C y el límite de la humedad no debe superar el 65% para evitar el deterioro.

Hay dos tipos de medios de extinción de incendios:

Manuales: En un centro de cómputos deben instalarse suficientes extinguidores portátiles de dióxido de carbono.
Automáticos: También llamados rociadores.

Los centros de cómputos deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.

Condiciones Climatologicas.

Normalmente se reciben por anticipado los avisos de tormentas, tempestades, tifones y catástrofes sísmicas similares. Una vez más las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada. La frecuencia y severidad de su ocurrencia deben ser tomadas en cuenta al decidir la construcción de un edificio.

La comprobación de los informes climatológicos o la existencia de un servicio que notifique la proximidad de una tormenta severa, permite que se tomen precauciones adicionales, tales como la retirada de objetos móviles, la provisión de calor, iluminación o combustible para la emergencia.

Terremotos.

Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas. El problema es que en la actualidad, estos fenómenos están ocurriendo en lugares donde no se los asociaba. Por fortuna los daños en las zonas improbables suelen ser ligeros.

Inundaciones.

Se les define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial.

Esta es una de las causas de mayores desastres en centros de cómputo. Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior.
Para evitar este inconveniente se pueden tomar las siguientes medidas: construir un techo impermeable para evitar el paso de agua desde un nivel superior.

Instalación eléctrica

Trabajar con computadoras implica trabajar con electricidad. Por lo tanto esta una de las principales áreas a considerar en la seguridad física. Además, es una problemática que abarca desde el usuario hogareño hasta la gran empresa.
En la medida que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

Control de Accesos.

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

Utilización de guardias.

a) Control de Personas

El servicio de vigilancia es el encargado del control de acceso de todas las personas a la empresa. Este servicio es el encargado de colocar los guardias en lugares estratégicos para cumplir con sus objetivos y controlar el acceso del personal.

A cualquier personal ajeno a la planta se le solicitará completar un formulario de datos personales, los motivos de la visita, a quien entrevista y hora de ingreso y de egreso. El uso de credenciales de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz del ingreso y egreso del personal a los distintos sectores de la empresa.

b) Protección de Planta.

El servicio de vigilancia verificará que todo el personal de planta utilice la credencial correspondiente.

Las personas también pueden acceder mediante algo que saben (por ejemplo un número de identificación o un password) que se solicitará a su ingreso. Al igual que el caso de las tarjetas de identificación los datos ingresados se contrastarán contra una base donde se almacena los datos de las personas autorizadas.

Utilización de sistemas Biométricos.

Definimos a la Biometría como “la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos”.
La Biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara las características únicas para la identificación de personas. La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos.

Los lectores biométricos identifican a la persona por lo que es (manos, ojos, venas, huellas digitales y voz), a diferencia del PIN o claves de acceso que aceptan a quien la posee.

Los beneficios de una Tecnología Biométrica pueden eliminar la necesidad de poseer una tarjeta para acceder. Aunque las reducciones de precios han disminuido el costo inicial de las tarjetas en los últimos años, el verdadero beneficio de eliminarlas consiste en la reducción del trabajo concerniente a su administración; una tarjeta extraviada debe ser reemplazada o copiada por alguien, hay entonces un costo asociado con el tiempo empleado para completar esa tarea.

Utilizando un dispositivo biométrico los costos de administración son más pequeños, se realiza el mantenimiento del lector, y una persona se encarga de mantener la base de datos actualizada. Sumado a esto, las características biométricas de una persona son intransferibles a otra.

Entre los principales recursos biométricos se encuentran:

Emisión de Calor, huella digital, verificación de Voz, verificación de Patrones Oculares, verificación automática de firmas, etc.

Seguridad con Animales

Sirven para grandes extensiones de terreno, y además tienen órganos sensitivos mucho más sensibles que los de cualquier dispositivo y, generalmente, el costo de cuidado y mantenimiento se disminuyen considerablemente utilizando este tipo de sistema. Así mismo, este sistema posee la desventaja de que los animales pueden ser engañados para lograr el acceso deseado.

Protección Electrónica

Se llama así a la detección de robo, intrusión, asalto e incendios mediante la utilización de sensores conectados a centrales de alarmas. Estas centrales tienen que ser conectadas a los elementos de señalización que son los encargados de hacerles saber al personal de una situación de emergencia. Cuando uno de los elementos sensores detectan una situación de riesgo, éstos transmiten inmediatamente el aviso a la central; ésta procesa la información recibida y ordena en respuesta la emisión de señales sonoras o luminosas alertando de la situación.

Veamos los más conocidos elementos utilizados en sistemas de alarma contra robo-intrusión.

Barreras Infrarrojas y de Micro-Ondas

Estas transmiten y reciben haces de luces infrarrojas y de micro-ondas respectivamente. Se codifican por medio de pulsos con el fin de evadir los intentos de sabotaje. Estas barreras están compuestas por un transmisor y un receptor de igual tamaño y apariencia externa. Cuando el haz de luz es interrumpido, se activa el sistema de alarma, y luego vuelve al estado de alerta. Estas barreras son inmunes a fenómenos aleatorios como calefacción, luz ambiental, vibraciones, movimientos de masas de aire, etc.

Las barreras invisibles fotoeléctricas pueden llegar a cubrir áreas de hasta 150 metros de longitud. Pueden reflejar sus rayos por medio de espejos infrarrojos con el fin de cubrir con una misma barrera diferentes sectores.

Las micro-ondas son ondas de radio de frecuencia muy elevada. Esto permite que el sensor opere con señales de muy bajo nivel sin ser afectado por otras emisiones de radio, ya que están muy alejadas en frecuencia.

Debido a que este detector no utiliza aire como medio de propagación, posee la ventaja de no ser afectado por turbulencias de aire o sonidos muy fuertes, otra ventaja importante es la capacidad de atravesar ciertos materiales como son el vidrio, lana de vidrio, plástico, tabiques de madera, revoques sobre madera, mampostería y hormigón.

Detector Infrarrojo Pasivo

Estos detectores se basan en la detección de fuentes de radiación infrarroja (el cuerpo humano, por ejemplo) en movimiento, generando hasta 24 "paredes invisibles" (zonas de detección). La condición de alarma se produce cuando se atraviesa alguna de las zonas de detección. Estos detectores poseen un filtro de radiaciones indeseables para evitar las falsas alarmas producidas por ejemplo por un rayo de luz, cambios de temperatura o turbulencias de aire.

Detector Ultrasónico

Este equipo utiliza ultrasonidos para crear un campo de ondas. De esta manera, cualquier movimiento que realice un cuerpo dentro del espacio protegido, generará una perturbación en dicho campo que accionará la alarma. Este sistema posee un circuito refinado que elimina las falsas alarmas. Tanto la sensibilidad como el retardo del disparo, pueden ser regulados por medio de un selector interno. Mediante la variación de la sensibilidad, pueden lograrse disparos con movimientos más rápidos o más lentos. La cobertura de este sistema puede llegar a un máximo de 40 metros cuadrados.

Detectores Pasivos sin Alimentación

Estos elementos no requieren alimentación de la línea de batería, sólo van conectados a la central de control de alarmas para mandar la información de control. Los siguientes modelos están incluidos dentro de este tipo de detectores:

1. Detector de aberturas: contactos magnéticos externos.
2. Detector de roturas de vidrios: inmune a falsas alarmas provocadas por sonidos de baja frecuencia; sensibilidad regulable.
3. Detector de vibraciones: detecta golpes o manipulaciones extrañas sobre la superficie controlada.

Sonorización y Dispositivos Luminosos

Dentro de los elementos de sonorización se encuentran las sirenas, campanas, timbres, etc. Algunos dispositivos luminosos son los faros rotativos, las luces intermitentes, etc. Estos deben estar colocados de modo que sean efectivamente oídos o vistos por aquellos a quienes están dirigidos. Los elementos de sonorización deben estar bien identificados para poder determinar rápidamente si el estado de alarma es de robo, intrusión, asalto o aviso de incendio.

Se pueden usar transmisores de radio a corto alcance (VHF) para las instalaciones de alarmas locales. Los sensores se conectan a un transmisor que envía la señal de radio a un receptor conectado a la central de control de alarmas encargada de procesar la información recibida.

Circuitos Cerrados de Televisión

Permiten el control de todo lo que sucede en la planta según lo captado por las cámaras estratégicamente colocadas. Los monitores de estos circuitos deben estar ubicados en un sector de alta seguridad. Las cámaras pueden estar a la vista (para ser utilizada como

medida disuasiva) u ocultas (para evitar que el intruso sepa que está siendo captado por el personal de seguridad).

Todos los elementos anteriormente descriptos poseen un control contra sabotaje, de manera que si en algún momento se corta la alimentación o se produce la rotura de alguno de sus componentes, se enviará una señal a la central de alarma para que ésta accione los elementos de señalización correspondientes.

Edificios Inteligentes

La infraestructura inmobiliaria no podía quedarse rezagada en lo que se refiere a avances tecnológicos. Por lo que lo edificios han cambiado la concepción de sus estructuras para estar en condiciones de albergar la evolución de los tiempos, y estar en posición de satisfacer las necesidades del hombre de hoy.

El Edificio Inteligente (surgido hace unos 10 años) se define como una estructura que facilita a usuarios y administradores, herramientas y servicios integrados a la administración y comunicación.

Este concepto propone la integración de todos los sistemas existentes dentro del edificio, tales como teléfonos, comunicaciones por computadora, seguridad, control de todos los subsistemas del edificio (gas, calefacción, ventilación y aire acondicionado, etc.) y todas las formas de administración de energía.

Acciones Hostiles.

- Robo
  Las computadoras son posesiones valiosas de las empresas y están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero. Es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera, robar tiempo de máquina. La información importante o confidencial puede ser fácilmente copiada

  El software, es una propiedad muy fácilmente sustraíble y las cintas y discos son fácilmente copiados sin dejar ningún rastro

- Fraude
  Cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones, las computadoras han sido utilizados como instrumento para dichos fines. Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imagen, no se da ninguna oportunidad a este tipo de situaciones.

  Estos puntos serán tratados con más profundidad en capítulos posteriores.

- Sabotaje
  El peligro más temido en los centros de procesamiento de datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.

1.5.2 Seguridad Lógica.

Luego de ver como nuestro sistema puede verse afectado por la falta de seguridad física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputos no será sobre los medios físicos sino contra información por él almacenada y/o procesada. Así, la seguridad física, sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena, estas técnicas las brinda la seguridad lógica.

Es decir que la Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo.". Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no esta permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

Los objetivos que se plantean serán:

a) Restringir el acceso a los programas y archivos.
b) Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificarlos programas ni los archivos que no correspondan.
c) Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
d) Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
e) Que la información recibida sea la misma que ha sido transmitida.
f) Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
g) Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Controles de Acceso

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos o en un paquete específico de seguridad. Los controles de acceso constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso. Al respecto, el National Institute for Standars and Technology (NIST) ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema:

Identificación y autentificación

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina Identificación al momento en que el usuario se da a conocer en el sistema; y Autenticación a la verificación que realiza el sistema sobre esta identificación. Al igual que se consideró para la seguridad física, y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

1. Algo que solamente el individuo conoce: por ejemplo una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc.

2. Algo que la persona posee: por ejemplo una tarjeta magnética.

3. Algo que el individuo es y que lo identifica unívocamente: por ejemplo las huellas digitales o la voz.

4. Algo que el individuo es capaz de hacer: por ejemplo los patrones de escritura.

5. Para cada una de estas técnicas vale lo mencionado en el caso de la seguridad física en cuanto a sus ventajas y desventajas. Se destaca que en los dos primeros casos enunciados, es frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan, mientras que por otro lado, los controles de autenticación biométricos serían los más apropiados y fáciles de administrar, resultando ser también, los más costosos por la dificultad de su implementación.

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de allí, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina "single log-in" o sincronización de passwords.

Roles

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

Transacciones

También pueden implementarse controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.

Limitaciones a los Servicios

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

Modalidad de Acceso

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:

- **Lectura**: El usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
- **Escritura**: Este tipo de acceso permite agregar datos, modificar o borrar información.
- **Ejecución**: Este acceso otorga al usuario el privilegio de ejecutar programas.
- **Borrado**: Permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.
- **Todas las anteriores.**

Además existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación:

- **Creación:** permite al usuario crear nuevos archivos, registros o campos.
- **Búsqueda:** permite listar los archivos de un directorio determinado.

Ubicación y Horario

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas. En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana. De esta forma se mantiene un control más restringido de los usuarios y zonas de ingreso. Se debe mencionar que estos dos tipos de controles siempre deben ir acompañados de alguno de los controles anteriormente mencionados.

Control de Acceso Interno

Palabras Claves (Passwords). Generalmente se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones.

Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo. Sin embargo cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas encuentra dificultad para recordarlas y probablemente las escriba o elija palabras fácilmente deducibles, con lo que se ve disminuida la utilidad de esta técnica.

Encriptación. La información encriptada solamente puede ser desencriptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso.

Listas de Control de Accesos. Se refiere a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recurso del sistema, así como la modalidad de acceso permitido.

Límites Sobre la Interfase de Usuario. Estos límites, generalmente, son utilizados en conjunto con las listas de control de accesos y restringen a los usuarios a funciones específicas. Básicamente pueden ser de tres tipos: menús, vistas sobre la base de datos y límites físicos sobre la interfase de usuario (por ejemplo los cajeros automáticos donde el usuario sólo puede ejecutar ciertas funciones presionando teclas específicas).

Control de Acceso Externo

Dispositivos de Control de Puertos. Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem.

Firewalls o Puertas de Seguridad. Permiten bloquear o filtrar el acceso entre dos redes, usualmente una privada y otra externa (por ejemplo Internet).

Acceso de Personal Contratado o Consultores. Debido a que este tipo de personal en general presta servicios temporales, debe ponerse especial consideración en la política y administración de sus perfiles de acceso.

Administración

Una vez establecidos los controles de acceso sobre los sistemas y la aplicación, es necesario realizar una eficiente administración de estas medidas de Seguridad Lógica, lo que involucra la implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas.

La definición de los permisos de acceso requiere determinar cual será el nivel de seguridad necesario sobre los datos, por lo que es imprescindible clasificar la información, determinando el riesgo que produciría una eventual exposición de la misma a usuarios no autorizados.

Sólo cuando los usuarios están capacitados y tienen una conciencia formada respecto de la seguridad pueden asumir su responsabilidad individual. Para esto, el ejemplo de la gerencia constituye la base fundamental para que el entrenamiento sea efectivo: el personal debe sentir que la seguridad es un elemento prioritario dentro de la organización.

Políticas de Seguridad

Se deben crear políticas de seguridad que definan estrategias y criterios generales a adoptar en distintas funciones y actividades.

Capítulo 2.
Introducción al Plan de Contingencia.

2.1 Concepto de Desastre

En la actualidad no es suficiente que la empresa se restrinja a los campos de higiene y seguridad de trabajo o adquiera una póliza de seguros, ahora se tiene que buscar la integral y óptima seguridad, para lograr los siguientes objetivos principales:

- Mejorar la seguridad y salvaguardar la del personal y demás recursos de la empresa.
- Prevenir los desastres, a través de la reducción de los riesgos.
- Asegurar los preparativos para atender las emergencias.

El procesamiento de datos es una función de apoyo al negocio. Por lo tanto, cualquier tipo de amenaza a la seguridad de la empresa, lo es también para la seguridad de las instalaciones de cómputo.

Un desastre es cualquier acontecimiento que desequilibra y puede causar daños a los asentamientos humanos, áreas productivas, etc. Desastre no es tan solo los estados mismos del daño, sino las consecuencias adversas que se caracterizan por alteraciones múltiples del orden normal.

En conclusión un desastre es un evento en el que la sociedad sufre graves daños, de gran magnitud, e incurre en pérdidas. La estructura social y administrativa se desajusta impidiendo la realización de sus actividades esenciales, afectando su funcionamiento y operación normal.

De lo anterior se identifican dos sistemas involucrados en el desastre.

a) El sistema perturbador (SP) que es, el capaz de producir calamidades.
b) El sistema afectable (SA) integrado por el personal, bienes (hardware, software, información, comunicaciones).

Entre los factores externos a la empresa, los desastres representan uno de los riesgos más fuertes. La existencia de este riesgo es una de las razones por las que deben desarrollarse planes de contingencia y aplicarse medidas en pro de la seguridad de la información.

A continuación se presenta la clasificación de calamidades utilizada en las Bases del Sistema Nacional de Protección Civil. Este esquema de clasificación se elaboró con base en algunas características de las calamidades.

El esquema postula cinco tipos de fenómenos:

1. **Geológicos**. Tienen su origen en la actividad de las placas tectónicas y fallas continentales y regionales que cruzan y circundan a la Republica Mexicana.

2. **Hidrometeoros lógicos**. Son de esta clase los fenómenos que derivan de la acción violenta de los agentes atmosféricos, como los huracanes, las inundaciones fluviales y pluviales, etc.

3. **Químicos**. Se encuentran estrechamente ligados a la compleja vida en sociedad, al desarrollo industrial y tecnológico de las actividades humanas, y al uso de diversas formas de energía. Por lo general afectan en mayor medida a las grandes concentraciones humanas e industriales.
4. **Sanitarios**. Se vinculan también estrechamente con el crecimiento de la población y la industria. Sus fuentes se ubican en las grandes concentraciones humanas y vehiculares.

5. **Socio-Organizativos.** Tienen su origen en las actividades de las concentraciones humanas y en el mal funcionamientos de algún sistema de subsistencia que proporciona servicios básicos.

Estas tareas dan origen al establecimiento de una organización que contemple los siguientes puntos:

- Existencia de grupos de trabajo para la recuperación en caso de emergencia.
- Integración y capacitación del personal.
- Elaboración de planes y programas de acción.
- Realización de simulacros.
- Tener en cuenta los planes de protección civil y los planes generales de desastre para la organización.

El rescate o recuperación se compone de once puntos principales:

Alerta: Avisar a los afectados y a los responsables de la atención a emergencias.

Reconocimiento de daños: Estudio y evaluación de daños.

Concentración de auxilio: Coordinar y sincronizar las acciones de los grupos de recuperación.

Seguridad: Orientación a proteger la integridad física.

Rescate: Búsqueda y salvamento de los recursos.

Servicios estratégicos equipamiento y bienes: Restablecimiento de los servicios básicos.

Salud: Atención médica a personal afectado.

Aprovisionamiento: Proveer de los elementos necesarios para realizar las actividades básicas.

Comunicación social de emergencia: Busca lograr la participación de todos y crear una atmósfera de confianza.

Reconstrucción inicial y vuelta a la normalidad: Recupera las condiciones de funcionamiento normal, así como los sistemas afectados. Este último punto es importante ya que el no llevarlo correctamente puede agravar el desastre.

Se puede hablar de tipo de desastre cuando se han identificado las causas que han originado el desastre, es decir es provocado por causas naturales o humanas.

En ambos casos la magnitud de los mismos se determina por el impacto que pueda causar sobre los sistemas.

Los desastres Humanos se caracterizan por tener su origen en actos generados por personas. Ejemplo de estos desastres identificamos los siguientes:

- Sabotaje
- Negligencia.
- Descuidos.
- Mala operación
- Virus.
- Descomposturas originadas por malas instalaciones.

En el ámbito de los desastres naturales encontramos los siguientes:

- Incendio.
- Terremoto.
- Inundación.

El grado de desastre se puede definir en función de las siguientes variables:

- Si el recurso humano crítico está disponible o no.
- Si el desastre ha afectado al centro de cómputo en forma parcial o total.
- Si el desastre ha afectado las áreas operativas y/o las oficinas de la organización en forma parcial o total.
- Si el desastre ha afectado total o parcialmente al equipo de comunicación.

Los daños que pueden causar los desastres en los sistemas de cómputo están en función de la magnitud del desastre y de la vulnerabilidad de los equipos, así un equipo altamente vulnerable y un desastre mayúsculo impactará mayormente al equipo.

Daño = Vulnerabilidad *Magnitud del Desastre

Debe denotarse que la magnitud del desastre se mide por el impacto que este genera sobre los equipos, es decir puede que a un equipo no le afecte en gran medida la interrupción momentánea de sus líneas de comunicación causadas por un terremoto, como le afectaría el que sus discos se dañen por simple desgaste.

En cuanto a la vulnerabilidad del equipo, se refiere a la capacidad que este tiene para operar en condiciones adversas o no previstas como normales.

Al presentarse el desastre se activarán una serie de mecanismos para minimizar el problema en la información y la última medida a la que habrá de recurrirse será al plan de contingencia.

Para hacerle frente a un desastre se toman una serie de medidas clasificadas como: Preventivas, Correctivas, y Activación del Plan de Contingencia.

El **activar el Plan de Contingencia** será la última medida que se tome en caso de que ocurra un desastre. El plan garantiza la recuperación de los sistemas de información fundamentales para la empresa y será decisión de activarse del personal de sistemas en conjunción con la dirección de la empresa.

2.2 Identificación de Riesgos.

Es necesario identificar los factores de riesgo para lograr integridad y seguridad de los datos de peligros potenciales.

En el caso de la integridad de los datos, el peligro es, a menudo, un simple error de cálculo, confusiones o errores cometidos por personas, o fallos de equipos que provocan la pérdida de datos, su corrupción o su incorrecta modificación. En relación con la seguridad, la gente puede tratar de infiltrarse de forma mal intencionada en los sistemas de otras compañías para robar o estropear información.

2.2.1 Integridad de los datos

Se define integridad como un estado inalterado, el estado de estar completo o ser divisible. El objetivo de la integridad de datos es mantener la información de los sistemas en un estado completo e inalterado.

A continuación se examinan algunas de las causas más comunes de pérdida en la integridad de los datos.

2.2.2 Tipos de problemas en la integridad de los datos

Las necesidades de la vida actual obligan a las empresas a dar un mejor servicio, y es por esto que se ven obligadas a utilizar variedades en las marcas de sus equipos, por lo que no existe una estandarización de éstos, ya que algunos equipos utilizan protocolos diferentes, lenguajes de compilación diferentes, etc. Esto origina un caos, es decir, las empresas se ven imposibilitadas de dar un soporte adecuado a los datos.

Las amenazas a la integridad de datos se divide en:

1. Humanos

- Inexperiencia
- Estrés / Pánico
- Falta de comunicación
- Venganza
- Accidentes
- Avaricia

2. Errores en Hardware

- Fallos de discos
- Fallos de los controladores E/S
- Fallos de energía
- Fallos de memoria
- Fallos en medios, dispositivos
- Mal funcionamiento de los chips y de la placa base

3. Errores de Red

- Fallos en los controladores y en las tarjetas de interfaz de red (NIC)
- Problemas en componentes de red
- Problemas de radiación

4. Problemas de tipo lógico

- Errores lógicos
- Corrupción de Archivos
- Errores de intercambio
- Errores de almacenamiento
- Errores del Sistema Operativo
- Requisitos mal determinados

5. Contingencias

- Incendios
- Inundaciones
- Tormentas
- Accidentes Industriales
- Sabotaje / terrorismo

Daremos una descripción breve acerca de cada una de ellos.

1. HUMANOS

Este es el mayor punto débil de los sistemas distribuidos, “La gente que esta a cargo del sistema“. Pero no sólo los usuarios finales cometen errores, también los administradores de la red o del sistema se equivocan. Existen accidentes que no se pueden prever.

A continuación se describen los errores humanos más comunes a continuación:

Accidentes: Este tipo de errores suceden cuando no se escucho bien o porque no se puso atención suficiente a las indicaciones.

Inexperiencia: Este tipo de problema esta dado por la ansiedad en algunos casos de hacer las cosas que les asignan sin tener el debido conocimiento de éstas.

Estrés, pánico: El estrés de ser el administrador del sistema es agobiante y regularmente va de la mano con la inexperiencia.

Falta de comunicación: Uno de los problemas principales es éste, ya que es vital y en muchas empresas. La falta de una buena comunicación con los empleados ya sea por jerarquías mal organizadas que no permiten la comunicación directa con el responsable del área que se encuentra en problemas o por encomendar recados que muchas veces no llegan a tiempo o son distorsionados.

En la actualidad se cuenta con la facilidad del correo electrónico, pero desgraciadamente no siempre son revisados los mensajes a tiempo, o simplemente no son leídos. No debemos dar por hecho que al interesado le llegó el mensaje a tiempo.

Venganza: Esto es muy común, y se da en muchos casos por el enojo y la ira de empleados despedidos “injustamente“, o por algún empleado que aún sigue trabajando en la empresa y simplemente desea vengarse de alguien por este medio.

Avaricia: Es una manera de alterar los datos que generalmente en este caso se refieren a los sueldos.

2. ERRORES EN HARDWARE

Cualquier clase de maquinaria de alto rendimiento sólo puede funcionar durante un cierto tiempo, y se le debe de proveer del mantenimiento necesario para su funcionamiento óptimo.

Resumiremos algunos de las fallas eléctricas y mecánicas más comunes de las computadoras:

Fallos de disco: Uno de los fallos de procesamiento más comunes son los del disco. Un disco duro es una de las piezas más importantes de un equipo de cómputo y se espera que funcione como un reloj.

Sin embargo, no se debe confiar en el tiempo medio entre fallos (MTBF), en cambio, debe acostumbrarse a reemplazar sus dispositivos antes de que sea demasiado tarde. Aparte un disco es relativamente barato, no es así los datos que están almacenados en él. Es por esto que los subsistemas RAID (Serie de Discos Redundantes: Redundante Array of Inexpensive Disks) que tienen mecanismos internos de redundancia para tratar fallos de discos están ganando popularidad.

Fallos de los controladores E/S: Esto ocurre cuando los datos escritos en el disco ya están en mal estado, y no existe ningún proceso que nos permita recuperar los daros originales, verídicos, etc.

Fallos de energía: Existen dos clases de pérdida de energía una es perder la energía de la fuente de alimentación que suministra corriente a la máquina, o bien falla la fuente de alimentación de la misma máquina. En ambos casos la probabilidad de perder datos de forma significativa es muy alta, debido al comportamiento impredecible del sistema cuando le falta la energía.

Es buena idea instalar equipos de alimentación ininterrumpida y sistemas con baterías de reserva en los servidores, que le ayuden a realizar una parada del sistema antes de que se pierda totalmente la energía.

Fallos de memoria: Los circuitos RAM fallan ocasionalmente, si ocurre en error de memoria en un área donde ha sido almacenado un dato, acabará con datos en mal estado y probablemente no se dará cuenta hasta que alguien más note el error en los datos.

Los sistemas servidores que incorporan chequeos de paridad de la memoria podrían ayudarle a combatir este tipo de problemas, identificando los segmentos de código incorrectos en la memoria e impidiendo su ejecución, para que el sistema al tratar de ejecutar el segmento en mal estado no se detenga.

Fallos en medio, dispositivos: Los datos almacenados en medios extraíbles para realizar y recuperar copias de seguridad contienen copias de los datos. Cualquier problema con los dispositivos de almacenamiento o los medio que utilizan podrían tener como consecuencia la pérdida de datos si el servidor también estuviera dañado este tipo de problemas son muy comunes.

Mal funcionamiento de los chips y de la placa base: Los procesadores pueden provocar errores, las placas base pueden fallar, y en general cualquier cosa debido a la manufactura.

3. ERRORES DE RED

En una red de computadoras las líneas que conectan las máquinas están expuestas a una variedad de riesgos incluyendo interferencias y averías físicas. Cualquier anomalía en una red origina la pérdida o la corrupción de datos.

Analizaremos cada problema que se puede presentar en una red:

Fallos en los controladores y en las tarjetas de interfaz de red (NIC): La tarjeta de interfaz de red del dispositivo que la controla son virtualmente inseparables. La mayor parte del tiempo los problemas de las NIC`s y de los dispositivos no dañan los datos; tan solo impiden a los usuarios acceder a ella, y no sabremos con certeza qué archivos abiertos pudieron haber sido corrompidos cuando falla la tarjeta NIC en un servidor.

Problemas en componentes de red: La mayoría de las veces los administradores no prueban la fiabilidad y precisión de los componentes de la red bajo condiciones de carga de trabajo impuestas por los sistemas de almacenamiento y recuperación de copias de seguridad. Cualquier punto débil de estos componentes afectará probablemente al sistema de copias de seguridad.

Problemas de radiación : A partir de que lo que sucede en una computadora se fundamenta en el movimiento de los electrones, y puesto que la radiación tienen la capacidad de mover electrones, se deduce que la radiación y las computadoras pueden combinarse para formar una relación peligrosa, o simplemente datos incorrectos. La mejor estrategia para evitarla es no juntarlos.

4. PROBLEMAS DE TIPO LÓGICO

En las siguientes líneas se muestra una visión general de las formas en las que el software puede contribuir a la pérdida de la integridad de datos:

Errores lógicos: Los errores lógicos abarcan un amplio rango de defectos, relacionados generalmente con la lógica de la aplicación. Es difícil tratar de evitar éstos, ya que ningún fabricante puede probar todas las opciones posibles de utilización.

Corrupción de archivos: Los archivos pueden corromperse debido a problemas físicos o de red; problemas del control del sistema o de la lógica de aplicación. Si el archivo corrompido es utilizado por otros procesos para crear datos, los datos resultantes pueden ser incorrectos, ya que para el usuario final no suele ser evidente saber cuáles son los archivos que intervienen en todo proceso.

Errores de intercambio: El intercambio de archivos entre aplicaciones sucede a menudo, un ejemplo es el de los procesadores de texto que al convertir los datos, ponen en riesgo la integridad de éstos.

Errores de almacenamiento: Este error se da cuando sobrecargamos una máquina, ya que es necesario que el sistema haga toda clase de trabajos extras para acomodarlos y no siempre exista un plan de contingencia y la máquina se pare de manera correcta, probablemente haya archivos que no estén actualizados correctamente.

Errores del sistema operativo: Todos los sistemas operativos tienen su propio conjunto de errores y en algunos casos los datos pueden ser corrompidos. Un ejemplo

de los lugares más frustrantes en los que se encuentran los errores es en el código de las interfaces de programación de aplicaciones (API). Una API es utilizada por software de terceros y desarrolladores de hardware para solicitar o suministrar servicios a los usuarios finales.

Requisitos mal definidos: Si los requisitos del software no describen correctamente el trabajo que el usuario necesita realizar, el sistema podría generar datos incorrectos.

5. CONTINGENCIAS

No existe nada como la destrucción completa de un edificio o del lugar de trabajo para desafiar la integridad de un sistema. A continuación se examina brevemente cada una de las causas posibles de desastre

Incendios: El daño que puede ocasionar el fuego, combinado con el humo, el agua y el resto de los residuos resultantes después de un incendio, pueden hacer irrecuperables los datos.

Inundaciones y Tormentas: Muy comunes pero pueden ser igual de devastadoras que un incendio, ya que la pérdida de los datos es la misma. Una tormenta puede demoler un edificio o al menos destruir los servicios de energía y agua.

Accidentes industriales: Un accidente de esta índole, seguramente la haga imposible acceder a su equipo. Ej. Cables cortados por operadores, escape de gases peligrosos, gente de intendencia irresponsable, etc.

Sabotaje /Terrorismo: Desgraciadamente en esta época existen grupos que se dedican a corromper y estropear los datos por venganza o simplemente por gente que piensa que tiene el derecho a estropear o destruir edificios, datos, etc.

2.2.3 Seguridad de los Datos.

Se define seguridad como la cualidad o el estado de estar libre de daño así como las medidas de protección tomadas contra el espionaje, el sabotaje, el crimen, el ataque o la fuga.

Las amenazas contra la seguridad de los sistemas son desafiantes.

A continuación se examinan algunas de las causas más comunes de amenazas en contra de la seguridad de los datos.

Tipos de problemas de la seguridad de los datos

1. Físicas
   - Robo
   - Dumpster Diving
   - Espionaje
   - ID falsos

2. Basadas en los cables
   - Escuchas
   - Marcación de un número de teléfono
   - Imitación

3. Autentificación
   - ID falsos
   - Suposiciones hechas en algoritmos
   - Edición de contraseñas
   - Captura de contraseñas
   - Averiguación de contraseñas

4. Programación
   - Virus
   - Caballos de Troya
   - Cargas y Actualizaciones
   - Códigos Bomba

5. Puertas de escape del sistema
   - Servicios no seguros
   - Configuración e iniciación
   - Inicialización
   - Piggybacking

A continuación se da una descripción breve de cada uno de ellos.

1. FÍSICAS

La seguridad es un concepto sencillo: no deje conseguir a nadie lo que usted tiene, ni tampoco permita que le espíen.

Robo del equipo: Es muy común ya que es la forma más sencilla de obtener los datos de manera ilícita.

Dumpster Diving: No debemos revolver los disquetes en la basura ni información confidencial y que nos puede ser útil, ya que existen personas que se dedican a hurgar entre la basura para encontrar material costoso.

Espionaje: El espionaje industrial es muy real, Incluso los gobiernos lo hacen de vez en cuando; las organizaciones harán toda clase de acciones inmorales para ahorrar dinero y conocer los secretos de la competencia. El espionaje puede ser tan solo como el que un amigo escriba su password y nosotros lo memorizamos para después entrar y ver que es lo que está almacenando.

ID falsos: Se refiere a la gente que perpetra dichas actividades probablemente sea también bastante seria con su planes y sepan lo que están buscando, por eso plantean una amenaza significativa a sus datos. Ej.: Pasaporte, licencia de conducir, identificación, etc.

2. BASADAS EN LOS CABLES

La utilización de redes de computadoras crea amenazas adicionales de seguridad para sus datos.

Escuchas: La naturaleza del procesamiento distribuido se basa en la comunicación de diversas computadoras a través de un medio. Se deduce que se podría escuchar tráfico de la sesión y recoger información. En una empresa se puede utilizar cifrado para evitar que sus mensajes sean fáciles de descifrar.

Marcación de un número de teléfono: Cualquiera con un módem y un número de teléfono al que llamar puede intentar acceder a una red a través su facilidad de marcación remota.

Imitación: En este caso se les llama a la capacidad de una máquina de parecer otra en una red.

3. AUTENTIFICACION

Es el proceso mediante el cual la máquina determina si alguien está autorizado a solicitar o dar algunos servicios del servidor.

Existen diferentes problemas que se dan con la autentificación:

Captura de contraseñas: Consiste en que alguien escriba y compile un código que tiene el mismo aspecto que su pantalla de presentación al sistema. Este se inserta en la secuencia de introducción al sistema al que se le pide introducirse en él realmente. Todos los usuarios finales ven dos pantallas de presentación, una después de la otra; la primera falla aparentemente de la forma que se solicita al usuario final que se identifique de nuevo, la pantalla no fallo, pero sus datos se escribieron en un archivo que puede ser recuperado posteriormente.

Averiguación de contraseñas: Se trata de adivinar la contraseña de una computadora, y para este tipo de trabajo los profesionales tienen muchas probabilidades de éxito.

Suposiciones hechas en algoritmos: El filtrado de contraseñas funcionan bajo una serie de requisitos que alguien a codificado en alguna parte, y están basados en algún tipo de algoritmo.

Edición de contraseñas: De forma bastante sencilla, alguien dentro de la compañía establece una cuenta ficticia o cambia la contraseña de una cuenta inactiva. De esta forma, la maquina puede ser accedida por cualquiera que conozca el usuario y la contraseña de dicha cuenta.

4. PROGRAMACIÓN

La mayor parte de las violaciones contra la seguridad provienen del código.

Virus: Un virus es un trozo de programa que se produce a sí mismo, accediendo a otros programas en la máquina y transfiriéndose a otras máquinas cuando el programa es transferido a ellas.

Códigos bomba: La mayor parte de los virus destructivos también funcionan como códigos bomba. La idea de los Códigos bomba es que en una determinada hora y fecha, o basados en una secuencia de operaciones de la máquina, éste se disparará realizando su sucio trabajo.

Caballos de Troya: Se le denomina caballo de Troya a un rango de amenazas de códigos malévolos que incluye virus, bombas, gusanos, etc. Este se instala por sí mismo en una máquina y hace el trabajo del programador desconocido.

Actualizaciones y cargas: El instalar una actualización muchas veces resulta peligroso pues no se sabe qué contenga el software y si será del todo compatible con la computadora.

5. PUERTAS DE ESCAPE DEL SISTEMA

Conocida también como puertas traseras, son introducidas en los sistemas operativos para permitir el acceso al sistema en caso de que un cliente pierda toda la información de sus accesos autorizados. Solo la gente que las descubre conoce el proceso de las puertas traseras e incluso ellos no siempre lo saben.

Resumiremos las diversas amenazas contra la seguridad, planteadas por las puertas traseras:

Piggybacking: Significa llevar a cuestas a alguien, en este contexto se hace referencia a una situación en la que un usuario termina la comunicación con otro sistema; pero el puerto permanece activo en el otro sistema; entonces, otro usuario puede empezar la comunicación con este otro sistema en el mismo puerto sin pasar ningún control de seguridad.

Configuración e iniciación: Cuando tenemos que parar a uno de los servidores por cuestiones de mantenimiento, se da el mismo caso que al iniciarlo, ya se han borrado archivos, debido a los mecanismos de seguridad no se iniciaron correctamente, dejando agujeros de seguridad que son utilizados por otros.

2.2.4 Soluciones Generales a las amenazas contra la integridad y la seguridad de los datos.

A continuación se explican algunas de las técnicas que pueden ser utilizadas para mantener la integridad de los datos y la seguridad del sistema.

Herramientas para mejorar la integridad de los datos

La siguiente tabla cataloga las técnicas para recuperar la integridad o la prevención de los datos.

TECNICA	CORRECTIVA /PREVENTIVA
Copias de seguridad	Correctiva
Técnicas de espejo	Preventiva
Archivado	Preventiva
Custodia	Correctiva
Chequeo de paridad	Preventiva
Plan de contingencias	Correctiva
Análisis predictivo de fallos	Preventiva
Alta disponibilidad	Preventiva
Alimentación ininterrumpida	Preventiva
Implementación de técnicas de seguridad	Preventiva

Técnicas de integridad

Cada una de estas técnicas consiste en:

Copias de seguridad: La realización de copias de seguridad es el método más utilizado para restablecer un sistema. Si se pierden los datos, se recupera una copia anterior del sistema a partir de las copias de seguridad.

Técnicas de espejo (Niveles de raid): Son aquellas en las que se copian los datos en un dispositivo o máquina, a otra diferente, según se están escribiendo. Pueden ser realizadas de forma lógica para replicar segmentos del sistema de archivos de una máquina en otra parte de la red. También pueden realizarse estrictamente a un nivel físico mediante dispositivos de disco en espejo, subsistema de E/S y máquinas enteras.

Archivado: Es el proceso de borrado de archivos del sistema de almacenamiento "online" (en línea) en red. Y su copia en elementos de almacenamiento a largo plazo, en cinta o medio ópticos. Se utiliza para aumentar la protección del sistema de archivos borrado datos del sistema de almacenamiento online y colocándolos en armarios dispuestos para ese fin.

Custodia: Nos referimos a la custodia, como el acto de salva guardar las cintas, discos, etc. en los que se realizaron las copias de seguridad.

Chequeo de Paridad: Suministra un mecanismo de guardia que asegura que fallos de memoria inesperado no tengan como resultado el fallo del servidor o pérdida de la integridad de los datos.

Plan de contingencias: Un plan de recuperación de información después de desastres es como una guía para reconstruir su sistema desde cero.

Análisis predictivo de fallos: Es muy difícil darse cuenta de que un dispositivo está fallando, los dispositivos de disco están siendo desarrollados para indicar que están empezando a fallar cuando esto ocurre.

Alimentación ininterrumpida: Se trata de suministrar las baterías de reserva en caso de pérdida de energía, también dan un voltaje consiste y sin fluctuaciones a la máquina, así, como evitar las variaciones de carga.

2.2.5 Herramientas para reducir las amenazas contra la seguridad

La siguiente tabla cataloga las herramientas para conseguir que un sistema tenga un nivel de seguridad adecuado. La tabla explica del lado izquierdo la recomendación y del lado derecho si puede ser implementada por el sistema o si es política personal que debe ser comunicada a los empleados.

RECOMENDACIÓN	SISTEMA / POLITICA
Eliminación de las puertas traseras del sistema	Sistema
Chequeo de virus	Sistema
Seguridad física	Política
Política de máquinas desatendidas	Política
Política de eliminación de basura	Política
Política de contraseñas	Política
Cifrado	Sistema
Obligación de identificación	Sistema, también podrá ser práctica
Cortafuegos para el acceso a Internet	Sistema
Trampas para intrusos	Sistema

A continuación se explica cada una de estas recomendaciones:

Eliminación de las puertas traseras del sistema: Como se explicó anteriormente es mejor cerrar una puerta trasera, a que alguien esté enterado de que existe, y tenga acceso al sistema.

Chequeo de virus: Se puede aplicar una estrategia que incorpore múltiples sistemas de protección y actualización periódicamente contra virus. Es importante poder detectarlos y aún mejor poder prevenirlos.

Seguridad física: Los equipos que se encuentran cerrados con llave en lugares a los que no puede acceder la mayor parte de la gente son más seguros, desde el punto de vista de las amenazas contra la seguridad.

Política de máquinas desatendidas: Se deberán apagar las máquinas en la noche y los fines de semana, así como acostumbrar a los empleados a poner contraseñas en los protectores de pantalla y en los teclados.

Política de eliminación de basura: Se debe triturar la basura en el caso de documentos importantes o confidenciales, en el formato electrónico debemos hacer lo mismo.

Política de contraseñas: Se deben cambiar las contraseñas de forma periódica, no deben ser reutilizadas ni basadas en cosas como apellidos o números de teléfono para evitar que sean descifradas por extraños.

Cifrado: El cifrado revuelve los datos de forma que no pueden ser utilizados, a no ser que sean primero descifrados. El punto débil de todos los esquemas de cifrado es la utilización de algoritmos que pueden ser finalmente decodificados por otra persona.

Obligación de identificación: La identificación que asegura la validez de la persona o el programa en el otro extremo de la sesión es extremadamente importante para muchas organizaciones.

Cortafuegos para el acceso a Internet: Si la empresa da acceso a Internet debe tener instalados cortafuegos, para evitar que los piratas informáticos tengan conocimiento de los detalles de sus sistemas.

Trampas para intrusos: La idea de tener trampas para intrusos es el de saber quien está tratando de entrar al sistema, así como también saber quiénes son, qué productos están utilizando y desde dónde están trabajando.

2.3 ¿Qué es un Plan de Contingencia?

En el mundo de hoy, las organizaciones dependen del procesamiento de datos para el flujo de información esencial. A consecuencia de esto, toda organización es vulnerable en caso de que las operaciones de cómputo no funcionen.

Las amenazas son reales y un desastre puede resultar de diferentes fuentes. Así mismo es importante comprender que un desastre puede ocurrir de la misma forma que producirse. Pero cualquiera que sea la causa, un tiempo prolongado de suspensión del procedimiento de cómputo puede ser devastador, por eso se debe estar preparado.

Un plan de contingencia o plan de recuperación en caso de desastres es una guía para la restauración rápida y organizada de las operaciones de cómputo después de una suspensión. Especifica quién hace qué y cómo. Los objetivos de dicho plan son los de restablecer, lo más pronto posible, el procesamiento de aplicaciones críticas (aquellas necesarias para la recuperación) para posteriormente restaurar totalmente el procesamiento normal de la empresa.

Un plan de contingencia no duplica un entorno comercial normal, pero sí minimiza la pérdida potencial de activos y mantiene a la empresa operando, al tomar acciones decisivas basadas en la planeación anticipada.

Dicho de otra manera, un plan de contingencia es un programa de recuperación de la organización. La base de este plan es una decisión del negocio sobre qué aplicaciones del procesamiento de datos son las más importantes de proteger y recuperar. En otras palabras, el plan de contingencia no es sólo un problema del área de sistemas, sino de todo el negocio.

Algunos autores conciben a un Plan de Contingencia como un plan escrito en el que se detallan las acciones, procedimientos y recursos que debe usarse durante un desastre, el cual cause destrucción parcial o total de los servicios de cómputo. En este plan se definen qué tareas son críticas, quién es el responsable de cada uno de los aspectos del proceso de recuperación, y como va a funcionar la organización mientras los sistemas estén siendo recuperados o transportados a un nuevo lugar.

Los planes de contingencia son semejantes a cualquier otro plan de negocios: deben tener sentido, ser legibles e indicar todos los aspectos de la función en cuestión. El nivel de detalle para el plan de contingencia, para respaldar la información y para los procedimientos de recuperación depende de la importancia de la aplicación y del tipo de información.

Los planes de contingencia han sido desarrollados para los grandes centros de información, así la metodología propuesta en este trabajo de investigación abarca los puntos que son comunes para empresas que cuenten con una infraestructura tecnología mediana, sin embargo el alcance del Plan de Recuperación si deberá ser propio para cada empresa de acuerdo a sus necesidades.

En su concepción, el plan de contingencia es un control netamente preventivo ya que se configura como instrumento que permite prevenir la eventualidad de un desastre, así como mantener el nivel de operación del ambiente informático, tornándose en un control correctivo en la medida en la cual se materializa una contingencia, ya que pretende reducir el impacto de ésta.

2.4 Alcance y objetivos de un Plan de Contingencia

Una de las claves importantes en el desarrollo de un plan de contingencia estriba en la evaluación de posibles riesgos (probabilidad de ocurrencia), que envuelven el ambiente informático. Sin embargo, es imposible prever en un 100% todos y cada uno de los riesgos que acosan la operatividad. Es entonces vital enlistarlos y agruparlos con la finalidad de anticipar la mayor parte de ellos y posteriormente establecer el impacto que pueden causar en caso de su materialización.

Es importante destacar que un plan de contingencia no evita los desastres, sino que provee los medios necesarios para salvaguardar al máximo los recursos del área de procesamiento electrónico de datos y reducir así las posibles pérdidas que resultan de estos desastres.

Un plan de contingencia se genera a partir de un análisis de impacto al negocio, donde se estudian de manera corporativa las aplicaciones económicas, operativas y comerciales que pudiese tener una empresa en caso de privarse de sus servicios de información.

El estudio, denotará cuáles son las áreas del negocio más afectadas por la contingencia destacando las que impactarán mayormente en la operación de la empresa; aunado a esto se cuantificarán las posibles perdidas monetarias y de información en función del tiempo que dure la contingencia.

El análisis anterior permitirá generar los alcances del Plan de contingencia determinando cuál es la prioridad que se dará en la recuperación a cada uno de los servicios de información, que elementos serán necesarios recuperar para que dicha información se genere y cuáles serán los procesos que deben involucrarse en el restablecimiento de los servicios.

Hay que resaltar que el recurso humano es un punto importante dentro del Plan de contingencia. Debe asignarse al personal que trabajará dentro del mismo y formar grupos con objetivos claramente definidos, donde cada miembro debe saber el papel que va a desempeñar, conocer las tareas que asignadas para el cargo de esta actividad y responsabilizar para el éxito del plan de recuperación.

Con los elementos antes mencionados se formará un manual donde se describen las actividades a seguir para la recuperación de los servicios de información. Estas actividades deben estar bien detalladas, puntualizando el personal que participa dentro de ellas, así como el responsable de su cumplimiento.

Dentro de este manual se describen el personal que participa, los servicios de cómputo que deben restablecer, los servicios de cómputo alternativos que serán utilizados, los apoyos materiales, misceláneos, archivos manuales, etc., que se utilizarán y conjuntado todo esto a una serie de procedimientos que indicarán paso a paso como restablecer los servicios de información y las funciones críticas de la empresa.

Una vez conformando el plan deben realizarse pruebas sobre el mismo verificando su correcto funcionamiento. Esto generalmente se realiza con simulacros de desastre donde se presenta el escenario de una contingencia sobre el servicio de información. Después de realizadas las pruebas se realizarán los ajustes correspondientes al plan para tener definitivamente un documento final que será el que proporcione el servicio óptimo para la recuperación.

Al plan de contingencia debe dársele un mantenimiento continuo donde se estén actualizando continuamente sus datos, debido al dinamismo con el que las empresas tienden a cambiar sus esquemas de operación, por lo que el plan debe mantenerse a la par de los movimientos de la compañía.

Por lo tanto, el diseño e implementación de un plan de Recuperación de Desastres de debe contemplar los siguientes objetivos:

- Recuperar la operatividad de las empresas en el menor tiempo y costo posible, permitiendo a las empresas enfrentarse de manera efectiva a situaciones no deseadas.

- Restablecer lo más pronto posible, el procesamiento de aplicaciones críticas (aquellas necesarias para la recuperación) para posteriormente restaurar totalmente el procesamiento normal de la empresa.

- Identificar los riesgos y los porcentajes de factibilidad de éstos a los que está expuesta la organización.

- Asignar las responsabilidades al personal, tanto en las actividades que se realizarán durante la emergencia como en las de preparación y las de recuperación.

- Identificar las aplicaciones (sistemas automatizados) criticas, y de mayor importancia dentro de la producción de datos, para darles la seguridad necesaria.

- Especificar las alternativas de respaldo.

- Definir los procedimientos y políticas a seguir durante el momento de la crisis.

- Definir medidas de eficiencia y de tiempo previsto para la recuperación.

- Integrar las practicas de mantenimiento, entrenamiento en el plan y pruebas del mismo

2.5 Ventajas de contar con un Plan de Recuperación

Un Plan de Recuperación completo mitigará los efectos de los desastres y permitirá una rápida respuesta, una transferencia del procesamiento crítico a otras instalaciones, y una eventual recuperación. La preparación de un plan de contingencia da a los directos de una empresa una excelente oportunidad para aliviar o minimizar problemas potenciales que en un momento dado podrían interrumpir el procesamiento de datos.

Las ventajas de contar con un plan de recuperación son varias, entre las cuales se pueden mencionar las siguientes:

Tener un plan documentado con los procedimientos y acciones específicas a seguir en diferentes escenarios de desastre. Un plan estructurado y documentado va a permitir agilizar los procedimientos que se llevarán a cabo al presentarse una situación de desastre, evitando tomar decisiones equivocadas al improvisar lo que se tiene que hacer al momento de presentarse la contingencia.

Se deben de especificar todas aquellas actividades que deben ser realizadas, especificando si se deben de llevar a cabo en forma paralela a otras acciones o sin la terminación de una actividad es requisito para el inicio de otra. Lo anterior es con el fin de optimizar el tiempo y los recursos a utilizar dentro del plan, evitando así que se presente duplicada en las funciones. Cada actividad puede a su vez dividirse en otras tareas, las cuales deben ser descritas, asignando al personal adecuado para su realización.

Agilizar los procedimientos del proceso de recuperación para restablecer la operatividad de la empresa en le menor tiempo posible. Dependiendo del tipo de empresa, el factor tiempo es primordial para el negocio al presentarse una situación de contingencia, ya que los efectos negativos que se puedan producir aumentarán dramáticamente conforme transcurran los días, semanas o meses. El tiempo de recuperación disminuirá considerablemente al tener los lineamientos adecuados, ya que al tener todo proyectado no se perderá tiempo valioso en toma de decisiones, en compra de equipo, en capacitación del personal, etc.

Proporcionar lo más rápido posible soporte a las áreas críticas de la empresa. Al presentarse una contingencia es muy importante apoyar y brindar la ayuda necesaria a aquellas áreas que son estratégicas para la organización, pues de ello dependerá que la empresa pueda seguir operando y dando servicio a sus clientes.

Registrar mínimas pérdidas económicas o de información en caso de desastre. No cabe duda que el aspecto económico es el que tiene más impacto dentro de una empresa; siempre es más fácil evaluar lo que cuesta prepararse para un desastre que cuantificar lo que se podría perder por no estar preparado.

El plan de recuperación no va impedir que ocurra un desastre; el objeto de éste es reducir al máximo las posibles pérdidas que se puedan presentar, especialmente, las económicas y de información vital.
Siempre es posible reemplazar el equipo, el lugar de trabajo, pero la información no. Para algunas empresas, como bancos, casas de bolsas, aseguradoras, etc., la pérdida de un día de información podría tener graves consecuencias económicas.

Identificar los procesos y aplicaciones críticas dentro del portafolio de aplicaciones de la empresa y su prioridad a recuperar. Una de las actividades principales del plan de recuperación es identificar los procesos y aplicaciones que son fundamentales para la operación de la empresa y que al faltar éstos puede ocasionar serias consecuencias, ya sea en el aspecto económico o de imagen, y a su vez, determinar de antemano la secuencia con la cual se va a recuperar, evitando que al presentarse la contingencia de los procesos crítico desemboca en la recuperación de la empresa.

Tener documentados los recursos humanos, técnicos y materiales requeridos por la operación de los procesos y aplicaciones críticas en una situación de desastre.
Es muy importante tener bien definidos cuales son los requerimientos mínimos de equipo, materiales y de personal que son indispensables para poder llevar a cabo, adecuadamente, cada uno de los procesos críticos, con el fin de tenerlos siempre en existencia y disponibles al momento de presentarse una situación de desastre, evitando así algún retraso o contratiempo dentro del proceso de recuperación.

Contar con un centro de soporte alterno adecuado a las necesidades y requerimientos de la empresa. El plan de recuperación debe contemplar la identificación de n lugar externo donde el personal de la empresa pueda trasladarse si el acceso a las oficinas centrales están parcial o totalmente restringidas a causa de una contingencia. Este lugar alterno debe contar con el equipo necesario y con lo requerimientos mínimos de hardware, software y espacio para que le personal pueda llevar a cabo las actividades más importantes y restablecer lo más pronto posible la operación de la empresa.

Contar con el personal capacitado para actuar en situación de desastre. El elemento más importante del plan de recuperación son las personas que llevarán a cabo el proceso de recuperación, ya que si no se cuenta con su participación en forma oportuna y eficaz el plan no logrará su óptimo desarrollo. Se debe contemplar la participación de personal clave de las diferentes áreas de la empresa los cuales se encargarán de realizar las actividades definidas en forma coordinada.

Una vez seleccionado el personal, es importante capacitarlo con el propósito de que conozca cuales son sus responsabilidades y actividades específicas, así como la interrelación que va a tener con personal de otras áreas.

Poder realizar simulacros para probar la efectividad del plan. Los simulacros demuestran la efectividad del plan para recuperar lo más pronto posible la operatividad de la empresa. El realizar simulacros permite corregir posibles deficiencias del plan, ya que no se conoce que también funciona hasta que se prueba. Se podrá evaluar el funcionamiento del equipo y software de las comunicaciones y del personal que lleva a cabo las actividades principales de la empresa dentro del centro de trabajo alterno.

Actualizar en forma periódica la información crítica de la empresa. Es importante revisar y ajustar periódicamente el contenido del plan en función de posibles cambios de hardware, software y de personal, con el propósito de mantener la información actualizada. Con esto se garantiza que el plan refleje y responda a los cambios ocurridos en la empresa, ya que por más completa que sea la metodología utilizada, si la información contenida en el plan no se actualiza, éste pierde su efectividad.

2.6 Desventajas de no contar con un plan de Recuperación

Toma de decisiones precipitadas y posiblemente incorrectas. Al desconocer las posibles consecuencias que pueden tener una contingencia sobre el negocio, no se podrá determinar con claridad las posibles alternativas para llegar a una solución rápida y efectiva, obligando a tomar, por la premura de tiempo, decisiones sin tener los suficientes elementos y parámetros para tomar la mejor opción.

Actuar sin planeación previa. El desconocimiento de las acciones a seguir, de los recursos involucrados y de los posibles escenarios a los que se pueden enfrentar una empresa en una circunstancia, hace que la situación no se pueda resolver en poco tiempo y que las consecuencias sean imprevisibles.

Registrar importantes pérdidas económicas y de información. Las pérdidas económicas se reflejarán inmediatamente al no poder la organización disponer de forma inmediata de la información vital para seguir operando.

No hay que olvidar que el principal bien de una empresa es su información ya que de ella depende la toma de decisiones y el proporcionar el servicio adecuado e inmediato a los clientes y proveedores. Así mismo, se puede provocar que se haga una mala transacción al tomar decisiones equivocadas que involucren invertir recursos excesivos para recuperar la operatividad de la empresa.

No tener identificadas las áreas críticas de la empresa. Si no se hace un análisis del cual se obtenga el portafolio de actividades que son vitales para la operación de la empresa, no se podrá decidir correctamente que actividades tienen prioridad para recuperar su operatividad, lo que puede ocasionar que se dé mayor preferencia a áreas no tan importantes en el momento de presentarse la contingencia, dejando a un lado las que si son realmente críticas, dando lugar así a un alto impacto en diversos aspectos dentro de la empresa.

No poder procesar las aplicaciones críticas de la empresa durante un período de tiempo. El no poder llevar a cabo los procesos más importantes de la organización por algún tiempo dará como resultado no poder proporcionar el servicio que los clientes esperan de una empresa, no dar la información actualizada al corporativo para la toma oportuna de decisiones y ocasionar así la pérdida de la operatividad. El poder procesar las aplicaciones más importantes dependerá entonces de la rapidez con la que se pueda montar el ambiente en otro lugar o reparar el daño ocasionado por el desastre.

No contar con un centro de soporte alterno. Al no tener contemplado un lugar alterno donde llevar a cabo las actividades imprescindibles de cómputo temporalmente, la empresa no enfrentará al factor tiempo, ya que el restablecimiento del ambiente computacional es una de las actividades más complejas dentro de los procedimientos de recuperación, por lo que mientras es rehabilitado este ambiente, la organización no podrá realizar ninguna de sus actividades automatizadas, generando así pérdidas que aumentaran conforme transcurre el tiempo.

No contar con el personal capacitado para actuar en situaciones críticas. No contar con el personal capacitado para enfrentar una situación de contingencia hace que el proceso de recuperación sea lento y por lo tanto más costoso; al capacitar al personal se le darán las herramientas necesarias para poder realizar acciones inmediatas y llevar a cabo medidas preventivas que minimicen así los efectos negativos que pueda ocasionar una contingencia.

Capítulo 3.

Software en el mercado para apoyar el desarrollo de Planes de Contingencia.

3.1 Introducción

Muchas empresas utilizan productos que ayudan al desarrollo de planes de contingencia con el fin de apoyar el proceso de recuperación. En un principio, cuando la información era menos abundante, los planes de contingencia se "desarrollaban" o escribían en simples procesadores de texto. Sin embargo, desde que un gran volumen de información es manejada dentro de una organización, el procesador de palabras ya no fue suficiente. Por ejemplo, se tiene el caso de la empresa CHI/COR, la cual fue una de las primeras compañías que se dedicó al desarrollo de planes de contingencia.

Esta compañía comenzó usando un procesador de texto y hojas de cálculo como apoyo para el desarrollo de planes de recuperación de acuerdo a las normas acordadas en su momento.

Con el paso del tiempo se observó que las organizaciones no eran consorcios estáticos, y cuando empezaron a aparecer cambios trascendentes dentro de la organización en su estructura humana y en sus recursos tecnológicos, el plan se comenzó a desintegrar, en vista de lo difícil de esta forma de manejar y mantener un plan de recuperación, CHI/COR desarrolló a mediados de los años 80's, una herramienta fundada en una base de datos para apoyar los planes de recuperación.

El determinar cuál software es el más indicado para apoyar a una organización en particular, es una tarea crucial e importante para lograr que el plan sea exitoso. Dependiendo del tipo y tamaño de la empresa, se deberá seleccionar el software de apoyo.

Actualmente se tienen diversos productos disponibles, basados en su mayoría en PC y con diversas herramientas orientadas al desarrollo y administración de planes de recuperación. Abarcando desde simples procesadores de texto, hojas de cálculo hasta sofisticados sistemas expertos, máquinas de inferencias que pueden efectuar un análisis de impacto al negocio, estas herramientas pueden ofrecer interfaces en lenguaje natural, bases de datos relacionales y otros componentes.

A continuación mencionaremos algunos de éstos productos existentes que apoyan los Planes de Recuperación, los cuales agruparemos de acuerdo a sus características:

3.2 Creación y mantenimiento de Planes Globales de Contingencia.

A continuación se enumeran algunas compañías de software, las cuales se dedican a la elaboración de Planes de Contingencia. Así como algunas características más importantes acerca de sus productos.

LDRPS v 9.0
STROHL SYSTEMS GROUP INC.

631 Park Avenue
King of Prussia, PA 19406
Tel.- 800-634-2016; Fax.- 610 768-4120 Soporte Técnico.- Si

Especificaciones:

Los requerimientos mínimos para utilizar esta aplicación son procesador Pentium II a 266 MHz ,64 MB de RAM, espacio en disco duro de 200MB, monitor VGA (800X600). Los sistemas operativos que soporta la aplicación son Windows 95/98/NT/2000/XP, capacidad de hasta 50 usuarios concurrentes. Maneja licencias corporativas y su soporte técnico es de 24 hrs. los 365 días del año.

Resumen:

Provee las herramientas para el desarrollo de un plan de contingencia integral para toda la organización, con mínimas interrupciones en los procesos mientras se realiza el análisis de las funciones del negocio. Identifica y asigna prioridades a las actividades críticas.

Mediante asistentes ayuda a crear planes de contingencia de una manera rápida y fácilmente.

REVOLUTION V 4.0
SUNGARD PLANNING SOLUTIONS

6111 N. River Rd
Rosemont, IL 60018
Tel.- 800-272-9792; FAX.- 708-518-5340

Especificaciones:

Esta aplicación soporta los siguientes sistemas operativos Microsoft Windows 95/98/NT/2000/y XP, cuenta con soporte técnico 24 hrs, los 365 días, los requerimientos mínimos son procesador PII a 166 MHz, con 64 RAM, 250 MB de espacio en disco duro, VGA (800X600).

Resumen:

La instalación se puede realizar en varios lenguajes.

Herramienta basada en Web para el desarrollo de planes de contingencia, dividida en módulos para la administración, la creación y la actualización del plan.

Administración de grupos de usuarios, incluye el protocolo SSL para el manejo de encriptación de datos.

Utiliza como motor de Base de Datos Microsoft SQL Server y su modulo de reporteo esta basado en la herramienta Crystal Reports v 7.0.

COMPAS 5.18
SUNGARD PLANNING SOLUTIONS

6111 N. River Rd
Rosemont, IL 60018
Tel.- 800-272-9792; Fax.- 708-518-5340

Especificaciones:

Esta aplicación soporta los siguientes sistemas operativos Microsoft Windows 95/98/NT/2000/ y XP, cuenta con soporte técnico 24 hrs, los 365 días, los requerimientos mínimos son procesador PII a 166 MHz, con 64 RAM, 250 MB de espacio en disco duro, VGA (800X600). Cuenta con Licencia corporativa.

Resumen:

Esta diseñado para ayudar a los usuarios a documentar los procedimientos necesarios para proteger su negocio en caso de una contingencia.

El software ayuda a los desarrolladores del Plan de Contingencia a crear, probar e implementar el plan. Provee acceso directo a archivos con hasta 150 formatos diferentes. Tiene acceso de seguridad para cada usuario con identificador y clave de acceso. También provee una bitácora de las actividades realizadas por los usuarios.

Cuenta con el manejo de una base de datos personal con el objetivo de prever la disponibilidad de los miembros del Plan así como a los proveedores y contactos importantes. Lleva una bitácora de los cambios realizados al plan y quién realizo dichos cambios. La administración centralizada del plan permite al administrador delegar tareas. Provee capacidades de edición para la documentación.

RecoveryPAC v. 8.0
Computer Security Consultans, Inc (CSCI)

590 Danbury Road, Ridgefield CP 06877
Teléfono: 431-8720; Fax (203) 431-8165; Soporte Técnico: Si

Especificaciones:

RecoveryPac v. 8.0 es soportado por los siguientes sistemas operativos como son: Windows /2000, NT, ME, 98 y 95, para su ejecución se requiere como mínimo procesador Pentium II, con 64 MB en RAM, con 160 MB libres de espacio en disco duro. Licencia corporativa: Si.

Resumen:
Base de datos relacional que proporciona un plan de contingencia a los centro de cómputo o a la organización completa. Permite la administración de proyectos, tiene módulos de prueba. Proporciona una lista de las actividades predefinidas para la recuperación del negocio. Cuenta con dos tipos de licencia Server y por usuario. Cuenta con un modulo de reportes muy completo, integridad de datos automática.

3.3 Herramientas para la Recuperación de Redes de Computadoras.

Aim/LAN 2003: The LAN Recovery Plan

Advanced Information Management
12940 Harbor Dr.
Woodbridge, VA 22192-2921
703-643-1002, FAX: 703-643-2722, Soporte técnico: Si

Especificaciones:

Los requerimientos mínimos para utilizar esta aplicación son procesador Pentium I a 266 MHz ,64 MB de RAM, espacio en disco duro de 100MB, monitor VGA (800X600).

Los sistemas operativos que soporta la aplicación son Windows 95/98/NT/2000/XP, capacidad de hasta 25 usuarios concurrentes. Maneja licencias corporativas y su soporte técnico 15% del costo de la licencia después del primer año.

Resumen:

Aplicación independiente del protocolo, diseñada específicamente para ayudar al usuario a construir un plan de recuperación para redes de computadoras. Permite a los usuarios la recolección de información necesaria, estructurándola para fácil consulta, modela escenarios de recuperación y las acciones a seguir, estructura lógicamente el plan de recuperación.

Developing Network Disaster Recovery Plans

Contingency Strategies Associates, Inc.
111 Simsbury Rd. Avon
800-CSA-5678, FAX: 203-677-5947; Soporte Técnico: Si

Especificaciones:

Los requerimientos mínimos para utilizar esta aplicación son procesador Pentium II a 266 MHz ,64 MB de RAM, espacio en disco duro de 80MB, monitor VGA (800X600). Los sistemas operativos que soporta la aplicación son Windows 95/98/NT/2000/XP. Maneja licencias corporativas y su soporte técnico limitado.

Resumen:

Esta aplicación esta diseñada para la recuperación en caso de desastre de redes de voz y datos. Incluye un generador de base relacional. Crea planes impresos para la recuperación de desastre de redes de comunicación, tutorial del manejo de la aplicación y simulación de impacto al negocio incluidos.

DP/90 PLUS Network (V.5.0.)

SunGrand Planning Solutions. Inc.
(Subsidiary of SunGard Data Systems, Inc.)
1285 Drummers Lane
Wayne, PA 19087
800-341-2688, FAX: 610-687-0108, Soporte técnico: limitado

Especificaciones:

Los requerimientos mínimos para utilizar esta aplicación son procesador Pentium II a 266 MHz, 64 MB de RAM, espacio en disco duro de 100MB, monitor VGA (800X600). Los sistemas operativos que soporta la aplicación son Windows 95/98/NT/2000/XP. Maneja licencias corporativas y su soporte técnico es de manera telefónica.

Resumen:

Programa en PC para ayudar a los diseñadores en telecomunicaciones en el diseño e implementación de planes de recuperación de desastres para redes críticas. Redirecciona todos los elementos recuperables de la red, evalúa la situación del desastre, establece e implanta procedimientos de recuperación.

3.4 Estrategias de Respaldo de Información.

TIVOLI V 5.1.5
IBM Inc.

Madison Avenue NY. 10022
Tel.- 212-745-7252
Soporte Técnico.- Si

Especificaciones:

Soporta las siguientes plataformas: Windows NT/2000/XP, IBM AIX 4.3, HP UX 11, Sun Solaris 2.6, Linux X86, OS 400, Novell Netware 5.1, cuenta con soporta técnico 24 hrs. por 365 días, así como también de Licencia Corporativa.

Resumen:

Herramienta para una completa gestión de almacenamiento, soporta plataformas mixtas, altamente flexibles, Administración central de todos los procesos de gestión de almacenamiento desde cualquier parte de Internet o Intranet.

Optimización del uso de los recursos de almacenamiento (agrupación de discos y agrupación de cintas), manejo de respaldos incrementales, estrategias de respaldo y restauración de información.

ASG-BIP (Business Information Portal)
Allen Systems Group, Inc.

750 11th St. Naples, FL 33940
800-93-ALLEN; 941-263-6700, FAX: 941-263-3692

Especificaciones:

Interfase Web para la administración y gestión de aplicaciones y procesos críticos, cuenta con soporte técnico las 24 hrs, los 365 días del año, además de contar con una administración de Accesos, creación de grupos de usuarios y cuentas de acuerdo a perfiles.

Resumen:

Identifica los archivos vitales para la recuperación en caso de desastres. Este producto permite al personal del centro de cómputo a identificar los respaldos y recuperar archivos vitales en cintas y discos. Proporciona reportes para identificar los archivos críticos y el estatus actual de los respaldos. Periódicamente realiza revisiones para identificar nuevos archivos críticos, verifica la realización de respaldos y sus estatus.

DataStage v 5.0

Ascential Software Corporation
50 Washington Street
Westboro, MA 01581
(800) 966-9875; Soporte Técnico: si

Especificaciones:

DataStage v 5 es soportado por los siguientes sistemas operativos como son: HP-UX, Linux, Windows /2000, NT, ME, 98 y 95, para su ejecución se requiere como mínimo procesador Pentium II, con 64 MB en RAM, con 160 MB libres de espacio en disco duro. Cuenta con licencia corporativa.

Resumen:

Es una herramienta de extracción de registros vitales, soporta la conectividad con aplicaciones empresariales como SAP, SIEBEL, ORACLE, PEOPLESOFT, JDEDWARDS, es una completa herramienta de integración de datos, cuanta con utilidades como ftp, ejecución de aplicaciones Win 32 etc.

Posee una gran variedad de fuentes de datos con las cuales se puede conectar por medio de ODBC y drivers nativos de Microsoft SQL Server, Informix, Oracle y archivos de texto.

Robot/SAVE (V.9.0)
Help/Systems, Inc.

210 Baker Technology Plaza, 6101 Baker Rd.
Minneatonka, MN 55345
800-328-1000; FAX; 612-933-8153, Soporte técnico: Limitado.

Especificaciones:

Es soportado por los siguientes sistemas operativos como son:
HP-UX, Windows /2000, NT, ME, 98 y 95, para su ejecución se requiere como mínimo procesador Pentium II, con 64 MB en RAM, con 130 MB libres de espacio en disco duro, cuenta con Licencia corporativa.

Resumen:

Sistema de protección de desastres y recuperación, mediante la automatización de respaldo del sistema, recuperación y administración de cintas. Guía al usuario a través del proceso de recuperación después de un desastre. Incluye los siguientes módulos, respaldo y recuperación automatizada.

3.5 Herramientas para el Almacenamiento de Información.

CLARIION CX400 SERIES HARDWARE
EMC ²

Hopkington Massachussets
Tel.- 01748-9103

EMC Empresa líder en almacenamiento de información empresarial tiene un producto de tipo Hardware de la series CX400 el cual cuenta con las siguientes características:

Especificaciones:

Dispositivos de tipo Hardware que soportan sistemas operativos Windows NT/2000, Sun Solaris, HP-UX, IBM AIX y Red Hat Linux, Capacidad de almacenamiento de hasta 4.4 TB.

Resumen:

Con las series Clariion CX400, la organización cuenta con disponibilidad de la información al momento, además son totalmente personalizables al tipo de organización dependiendo de la cantidad de información que esta maneje, cuenta con un sistema de balanceo dinámico de almacenamiento, administración dinámica del ancho de banda, acepta redundancia de enlace en caso de falla en el canal principal, cuenta con la capacidad de procesar hasta 680 MB/s, topología punto a punto, compatible con otros sistemas de la empresa EMC.

SNAPVIEW SOFTWARE
EMC ²

Hopkington Massachussets
Tel.- 01748-9103

Especificaciones:

Sistemas Operativos soportados: Windows NT/2000, Sun Solaris, HP-UX, IBM AIX y Red Hat Linux.

Resumen:

Este software de almacenamiento de información es compatible con los equipos de la serie Clariion CX400, CX 600 Y FC4700 de EMC, empresa líder en el almacenamiento de grandes volúmenes de información.

Arreglo de Almacenamiento de información basado en software, crea copias instantáneas de ambientes de producción, alta disponibilidad de la información, cuenta con una interfaz entendible que facilita su administración, acelera los tiempos de desarrollo de aplicaciones ya que al momento de probar las aplicaciones se pueden hacer con los datos mas recientes sin que se vea degradado el rendimiento en el sistema de de producción.

Una característica importante de esta herramienta es que cuenta con un agente que se encarga de comenzar el proceso de almacenamiento diferencial o completo de la información dependiendo de los parámetros de configuración.

SANPOINT CONTROL SOFTWARE
VERITAS Software Corporation

1600 Plymouth St., Mountain View, CA 94043
Tel.- 407-357-7600

Especificaciones:

Sistemas Operativos soportados: Windows NT/2000, Sun Solaris, HP-UX, IBM AIX, Red Hat Linux. y Novell Netware

Resumen:

Con SANPoint Control los administradores del sistema cuentan con una interfaz simple, que reduce las tareas complejas de administrar el almacenamiento de información y concentración de datos, asegurando la disponibilidad y la integridad de la información

Además cuenta con un modulo de seguridad en donde se pueden crear grupos y cuentas en base a roles de usuarios, cuenta con una herramienta grafica para monitorear el proceso de almacenamiento en tiempo real.

Capítulo 4.

Desarrollo del Plan de Recuperación.

4.1 Introducción al Desarrollo del Plan de Contingencia

Un plan de contingencia es una parte fundamental dentro de la seguridad de la información, el cual contempla dos propósitos:

- Asegurar la disponibilidad de los activos o recursos de una organización posteriormente a la ocurrencia de un desastre.

- Reducir el impacto de un evento hasta un nivel aceptable para la dirección de la empresa.

Algunos de los problemas a los que se pueden enfrentar los Directores del departamento de Sistemas para obtener el apoyo de la alta dirección para este tipo de proyectos son los siguientes:

- Justificación de los costos del Plan. Esta crítica puede deberse a que no se justificaron adecuadamente los riesgos de no tener el Plan de Recuperación.
- Si ya se cuenta con seguros ¿Para qué se necesita el Plan? Aún si existe el consenso para desarrollar un plan en papel, es posible que la gerencia se resista a gastar dinero en su implementación.

Una forma de responder a la pregunta anteriormente formulada es entender que los seguros pueden cubrir el costo del daño a la instalación, al hardware y a los medios de almacenamiento de la información, pero el dinero que se pueda reponer no recuperará la información perdida, y el costo que se pagara por la discontinuidad del negocio será considerablemente mayor. Éstos son sólo algunos problemas comunes que pueden tener los Directores de Sistemas para obtener aprobación de la Alta Dirección y presupuesto para el desarrollo e implantación del plan de contingencia.

Desde luego que pueden surgir otros, dependiendo del tipo de empresa, de la personalidad y la cultura de las personas. También se debe explicar a la Dirección que un Plan de Recuperación de Desastres es un proyecto que ahorra dinero.

Es necesario lograr que la Dirección tenga en mente varias aspectos como el costo de oportunidad, competencia e imagen del negocio, así como hay que tomar en cuenta el impacto de la contingencia en aspectos como el económico, operacional, legal, calidad de servicio, pérdida de negocio, etc.

Por lo anterior, el primer paso que se debe realizar es obtener el compromiso de la alta Dirección con el fin de comprometerse a desarrollar el plan de contingencia en caso de desastre, de tal manera que los recursos necesarios puedan ser asignados al proyecto. Esto implica la distribución de fondos y personal, incluyendo personal del procesamiento de datos, de apoyo y usuarios.

Una vez que se obtuvo la aprobación y la participación de la alta Dirección en el Plan de contingencia, es necesario definir cuál será el alcance de éste para la empresa en particular.

La concepción del Plan de recuperación debe tener un alcance tal que permita una completa recuperación de la pérdida eventual, Dependiendo del tiempo que de antemano se haya considerado para ello. Surge entonces la pregunta ¿Qué significa hacer exitoso un Plan de recuperación? Se considera que el éxito del Plan estará en función del tiempo y del costo necesario para establecer la recuperación normal de los sistemas de cómputo.

Una vez que se ha tomado la decisión de llevar a cabo un Plan de Recuperación de Desastres, el Director de Sistemas debe determinar cómo se desarrollará dicho Plan.

Como se mencionó en el capítulo anterior actualmente se pueden encontrar en el mercado varias empresas dedicadas a desarrollar dichos planes y adecuarlos a las necesidades específicas de cada organización. Tales empresas tienen como objetivo el proporcionar la metodología o pasos a seguir al momento en que algún desastre dañe los sistemas de cómputo y/o información para su rápida recuperación, minimizando las pérdidas, tanto económicas como de datos.

Cabe mencionar el significado de los dos conceptos que a partir de este capítulo se mencionan:

Plan de Recuperación de Desastres:

Se trata de un documento que contiene una serie de procedimientos que se desarrollan, se ejecutan y se mantienen al día con el objetivo de que la empresa este preparada ante una situación no deseada.

Plan de Contingencia en Caso de Desastre:

Es una metodología que incluye análisis de impacto al negocio, estrategias de recuperación viables, mantenimiento del Plan, que debe cumplir con los siguientes propósitos:

- Asegurar la disponibilidad de los activos o recursos de una organización posteriormente a la ocurrencia de un desastre.

- Reducir el impacto de un evento hasta un nivel aceptable para la dirección de la empresa.

Cabe mencionar que para algunos expertos en el tema no hacen diferencia entre uno y otro, solo algunos autores son los que marcan diferencias entre un Plan de Contingencia, y un Plan de Recuperación de Desastres.

Para términos prácticos en este trabajo de investigación será indistinto referirse a un Plan de Continencia como a un Plan de Recuperación de Desastres.

4.2 Análisis de las Aplicaciones

Recopilación de Información

Para realizar un análisis de impacto al negocio, es necesario realizar una serie de entrevistas a cierto personal de la empresa, para obtener los datos y la información necesaria para conocer la situación de la organización en forma más detallada. De aquí la importancia de reunirse con el personal de alto nivel para seleccionar al personal que se va a entrevistar. Así mismo, es importante formular un calendario de las actividades a realizar con su duración y ponerlo a la consideración de la Dirección.

El objetivo es aplicar cuestionarios tanto a gerentes de área como a usuarios de sistemas para poder identificar aquellos aspectos más importantes referentes al área es decir:

- Los procesos automatizados que se realizan en cada departamento de la empresa.
- El tiempo que cada uno de ellos necesita para llevarse a cabo.
- Los periodos de más carga de trabajo.
- Determinar las pérdidas que se generarían al posponer alguna función por un determinado tiempo.

En base al análisis de los resultados obtenidos en las entrevistas, se identificarán las aplicaciones críticas de la empresa, la prioridad de cada una de ellas, los elementos materiales y humanos necesarios para su realización, así como los periodos críticos existentes.

Cuestionarios a Gerentes.

Se deben diseñar cuestionarios dirigidos a gerentes para que se obtengan los siguientes datos.

Ejemplo:

CUESTIONARIO PARA GERENTES
PARA DETERMINAR APLICACIONES CRITICAS.

Nombre del entrevistado:

.....

Cargo:

.....

Dirección o Gerencia:

.....

Fecha De Aplicación:

.....

1.- ¿Cuales son sus funciones principales?
.....
.....
.....

2.- ¿Como se interrelaciona esta área con otras áreas de la empresa?
.....
.....
.....

3.- ¿Cuales son las aplicaciones automatizadas que utilizan en su área?
.....
.....
.....

4.- Mencione los responsables por aplicación automatizada.
Especifique.

.....
.....
.....

5.- ¿Cuales son los días pico y los meses o periodos críticos para su área?

Meses del año
Ene, feb, mar, abr, may, jun, jul, ago, sep, oct, nov, dic.

Semanas del mes
1ª.semana, 2da. Semana, 3era. Semana, 4ª semana

Días de la semana
Lunes, Martes, Miércoles, Jueves, Viernes, Sábado

Días del mes
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31

6.- ¿Cual considera usted que es su tiempo de tolerancia?
.....
.....

7.-Explique ¿Cuál sería el impacto sobre la empresa, en el caso en que su aplicación dejara de funcionar en forma automatizada, por un desastre y sin previo aviso durante una semana en un periodo crítico? Enumere cada uno.
.....
.....
.....
.....

8.- En una situación de desastre ¿Que personal requeriría como mínimo para trabajar en un centro de soporte alterno?

.....
.....
.....

9.- ¿Que reportes, documentos y formatos impresos le son indispensables para el manejo y operación de área? Anexar muestras.

.....
.....
.....
.....

10.- ¿Cuales son las empresas que requeriría contactar en caso de desastre (banco, asesores legales, seguros, etc.)?

Empresa: .....
No.cta: .....Tel:.....
Asesor: .....
Dirección:.....
Asunto: .....
Email: .....

Empresa: .....
No.cta: .....Tel:.....
Asesor: .....
Dirección:.....
Asunto: .....
Email: .....

Empresa: .....
No.cta: .....Tel:.....
Asesor: .....
Dirección:.....
Asunto: .....
Email: .....

Empresa: .....
No.cta: .....Tel:.....
Asesor: .....
Dirección:.....
Asunto: .....
Email: .....

11.- Mencione el nombre del Personal que usted considera necesario a entrevistar, para el desarrollo del Plan de Recuperación de Desastres.

.....
.....
.....
.....

Antes de entrevistar a los usuarios de los sistemas, se procede a entrevistar al Gerente del departamento correspondiente, ya que estas personas tienen una visión más completa y global sobre el área, y son los más indicados para seleccionar al personal que se va a entrevistar posteriormente, es decir, los usuarios críticos de cada sistema.

Los puntos que se desean conocer por parte de los gerentes de área son los siguientes:

- Funciones principales del área. El gerente del área es la persona que tiene una visión general acerca del funcionamiento del departamento del cual es responsable; conoce todas las actividades que se llevan a cabo, además de la prioridad de cada una de ellas y las consecuencias que ocasionaría para el área y la empresa el dejar de llevar a cabo alguna de éstas.

- Relación entre las diferentes áreas de la empresa. Al conocer de manera general el funcionamiento del área, el gerente del departamento conoce también la relación que existe con los procesos de las áreas de la empresa, la dependencia entre uno y otro departamento, así de los cuales son los medios o procedimientos para recibir la información de las demás áreas y para así transmitirla a otros procesos.

- Aplicaciones automatizadas e interdependencia entre ellas. El plan de recuperación está enfocado al restablecimiento de la operatividad de las principales aplicaciones, especialmente las automatizadas de la empresa.

  Por lo que el primer paso es conocer por parte del Gerente del departamento todas las aplicaciones existentes en cada área así como su dependencia entre si, y conocer cuál es el grado de automatización de cada uno de ellas. Por otra parte, es necesario que informe cómo los procesos se relacionan entre si, como un proceso depende del funcionamiento de otro u otros, etc.

- Períodos críticos de área. Uno de los aspectos de mayor importancia es el de conocer por parte de los gerentes de área las etapas donde el nivel de operación del área aumenta. El gerente conoce perfectamente cuales son los períodos de más carga de trabajo para cada aplicación a su cargo y cómo influye esto en el desempeño general de su área y en consecuencia, con respecto a las otras áreas de la empresa.

- Tiempo de tolerancia. Se refiere al tiempo que cada aplicación puede dejar de operar normalmente, sin afectar mayormente al área y en consecuencia a la empresa.

  Este es uno de los puntos de mayor relevancia a tratar con los responsables de cada departamento, ya que el conocimiento de esto permitirá evaluar las posibles pérdidas, sobre todo económicas, que puede originar el que uno o varios procesos dejen de llevarse a cabo , y determinar de esta forma cual sería la situación que se presentaría para la empresa, tomando en cuenta que puede afectarse parcial o totalmente a otras áreas estratégicas.

- El Impacto ocasionado por no funcionar alguna de las aplicaciones durante un determinado tiempo. El gerente, al tener relación estrecha con las personas de alta dirección y por las responsabilidades propias de su cargo, tiene un mayor conocimiento de las consecuencias, ya sean económicas, legales, de imagen, etc., que se generarían al dejar de procesar algunas de las aplicaciones por un determinado tiempo.

- Personal responsable por aplicación. El gerente de área puede proporcionar los nombres de las personas responsables de cada proceso, en especial de los usuarios de las aplicaciones automatizadas; el gerente conoce a fondo el desempeño y carácter de cada uno de sus subordinados, lo cual será importante para seleccionar al personal clave que será incluido dentro del Plan de Contingencia.

- Requerimientos mínimos de personal para la recuperación de la operatividad. En cualquier situación importante se debe contar con el personal adecuado para enfrentar cualquier problema que se presente. El gerente del departamento conoce por la relación estrecha y cotidiana que lleva con su equipo de trabajo, el carácter, disposición y capacidad de cada uno de sus subordinados para encarar situaciones difíciles, por lo cual su opinión acerca de las personas que deben integrar el equipo de recuperación es de suma importancia y digno de tomarse en cuenta.

- Documentos y reportes imprescindibles para el funcionamiento del área . El responsable de un departamento o área es la persona que conoce también que información es indispensable para llevar a cabo cada unos de los procesos, manuales o automatizados, y que puede ser en forma de reportes impresos, documentos, disquetes, cintas etc. El tener perfectamente identificados los reportes y la documentación indispensables para la operación del área, así como su localización física, será vital dentro del proyecto de recuperación.

- Información de proveedores y clientes. El contar con la información actualizada referente a los clientes y proveedores de la empresa es fundamental para tener rápida comunicación con ellos al momento de presentarse una contingencia, con el fin de informarles de cuales serán los nuevos procedimientos para realizar los pagos, cobros, adquisiciones, etc., así como para notificarles de la dirección y teléfonos provisionales de la empresa; y son los gerentes de área las personas más indicadas para proporcionar esta valiosa información para el Plan de Recuperación.

- Personal a ser entrevistado. El responsable de área en cuestión puede con toda certeza proporcionar una lista del personal a su cargo que él considere debe ser entrevistado, por la importancia de la información que dichos empleados pueden proporcionar para el desarrollo del plan y por ser los usuarios principales de uno o más procesos de trascendencia para el departamento o para la misma empresa.

  Así mismo, el debe ser quién informe a su personal acerca del Plan de Contingencia, la importancia del éxito de este Plan para la organización y sobre todo, debe concientizarlos acerca de lo importante de su colaboración para el planteamiento, desarrollo y funcionamiento de las estrategias de recuperación de la operatividad del negocio.

Una vez finalizada la conversación con cada director o gerente del área, se le proporciona una guía con los puntos a tratar o el cuestionario a realizar a sus subordinados para su aprobación y sugerencias.

Cuestionarios a Usuarios.

Después de aplicar cuestionarios a los gerentes y con la información que éstos proporcionaron, se debe realizar entrevistas a cada uno de los usuarios de las aplicaciones automatizadas.

En este tipo de entrevista tiene un enfoque más operativo, con la realización de este cuestionario identificamos las áreas de oportunidad para el Plan de Recuperación de Desastres.

Ejemplo:

CUESTIONARIOS PARA USUARIOS

Nombre:

.....

Cargo:

.....

Gerencia:

.....
Fecha De Aplicación:

.....

1.- Funciones Principales, Especifique.
.....
.....
.....

2.- ¿Cuáles son las aplicaciones automatizadas que usted maneja en el área?
.....
.....
.....

3.- ¿Envía datos a otros procesos automatizados?

Si.....
¿Cuáles?.....
.....
.....

¿Para Que?
.....
.....
No.....

4.- ¿Recibe usted datos de otros procesos automatizados?

Si.....
¿Cuáles?.....
.....
¿Para que?
.....
No.....

5.- ¿Cuál es el equipo adicional que utiliza para llevar a cabo sus funciones?

.....
.....
.....

6.- ¿Es necesario software o paquetería adicional para que pueda realizar sus actividades?
.....
.....
.....

7.- ¿Cuál es el tiempo mínimo necesario del equipo central para realizar su aplicación?
.....
.....
.....

8.- ¿Cuánto tiempo puede continuar el departamento y todas sus funciones sin el soporte usual de proceso de datos? Asuma que la perdida del soporte de proceso de datos ocurrió durante su pico mas alto de carga de trabajo, elija solo uno.

a) hasta 1 día
b) hasta 2 días
c) hasta 3 días
d) una semana

9.- Indique, si los hay, los periodos altos de carga de carga de trabajo para sus procesos durante el año, mes y semana.

Meses del año
ene, feb, mar, abr, may, jun, jul, ago, sep, ago, oct, nov, dic.

Semanas del mes
1ª semana, 2da. Semana, 3era. Semana, 4ta. Semana.

Días de la semana
Lunes, martes, miércoles, jueves, viernes.

Días del mes
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31.

10.- ¿Cuántos movimientos son capturados?

Promedio:.....
Días pico: .....
Horas de captura:.....

11.- En una situación de desastre ¿Podría efectuar sus consultas en base a reportes?

Si.....
¿Porque? .....
No.....
¿Porque? .....

12.- ¿Como impactaría a la empresa el hecho de que su aplicación no se pudiera procesar en un lapso mayor de una semana sin previo aviso?

Considere los siguientes parámetros: b = bajo m = medio a = alto

Operacional:
.....
¿Porque?.....
Legal/fiscal:
.....
¿Porque?.....

Perdida del
Negocio:
.....
¿Porque?.....

Imagen
Corporativa:
.....
¿Porque?.....

13.- ¿Que recursos necesitará para operar su aplicación en un centro alterno?

Comunicaciones:
.....
.....
.....

Documentos fuente:
.....
.....
.....

Formas Impresas:
.....
.....
.....

Materiales:
.....
.....
.....

Reportes:
.....
.....

Otros Equipos:
.....
.....

14.- ¿Ha desarrollado o establecido procedimientos alternos, manuales o algún otro que puedan ser utilizados para continuar las operaciones en caso de que su proceso normal no pueda ser llevado a cabo?

Si.....
¿Cuáles?.....
.....

No.....
¿Porque?.....
.....

15.- Especifique cualquier factor que deba ser considerado en la evaluación del impacto de la perdida del proceso.
.....
.....

16.- ¿Cuenta con manuales o procedimientos que explique la operación de la aplicación?

Si..... ¿Cuales? .....
No..... ¿Porque? .....

Las entrevistas con los usuarios de los sistemas se diseñan de tal forma que se pueda obtener los datos siguientes:

- Funciones Principales. Cada usuario debe informar acerca de las diversas actividades que realiza dentro del área, describiéndolas de forma detallada y precisa, especialmente aquellos procesos que se llevan a cabo de forma automatizada, enlistándolos preferentemente por la orden de importancia y/o relevancia para el departamento o la empresa, explicando así mismo cual es la interrelación que existe con respecto a procesos o funciones de la misma área o de otras áreas de la organización.

- Funciones Críticas. Del portafolio de aplicaciones obtenido se determinaron que actividades y funciones son críticas para el área, es decir, se identificaron cuales son fundamentales para la operación del departamento y que de no llevarse a cabo oportunamente pueden ocasionar consecuencias negativas no solo para el área, sino para la empresa en general.

  Esto se define de acuerdo a lo siguiente:

  a) Al número de movimientos realizados tanto en los días normales como en días pico, así como las horas de captura invertidas.

  b) La posibilidad de efectuar algunas de sus operaciones solo en base a reportes; y especialmente.

  c) Al nivel de impacto en la operatividad de la empresa, en cuestiones legales, económicas y de imagen que se ocasionaría a la organización el que cada aplicación no se pudiera llevar a cabo por un lapso de tiempo.

- Funciones que se pueden posponer. Es sumamente importante que cada usuario este consciente de qué aplicaciones y procesos pueden retardarse sin que esto ocasione grandes problemas al departamento, con el fin de poder dar toda la importancia a aquellas funciones que realmente la requieren en situación de contingencia.

  Es muy común que las personas tengan la sensación de que todas las actividades que se desarrollan son igualmente importantes, por lo que se hace necesario que tomen conciencia de la verdadera importancia de cada una de sus tareas y se determinen realmente cuáles no pueden dejar de operar y cuáles pueden posponerse.

- Documentación y Reportes Básicos. Cuando se determina un proceso crítico es necesario tener en cuenta si requiere éste de documentos y reportes impresos para poder llevarse a cabo; esto lo debe de identificar plenamente el usuario de dicho proceso para que sea incluido dentro de los procedimientos de recuperación ante una situación de contingencia.

- Dependencia de algún equipo o software, Los usuarios de aplicaciones automatizadas deben de conocer que equipo están usando para efectuar cada una de sus funciones.

- Períodos críticos y tiempo de tolerancia. Por ser quien conoce perfectamente las cargas de trabajo para cada proceso, el usuario puede informar con certeza que meses, semanas y días de todo el año son los más difíciles y críticos por la gran cantidad de trabajo que se presenta para el departamento . Así mismo, puede advertir el tiempo que puede tolerar el área sin el usual soporte automatizado en el momento de mayor carga de trabajo, sin que se presenten consecuencias negativas.

- Procedimientos alternos. Conocer si el usuario de una aplicación automatizada ha desarrollado métodos alternativos para continuar la operación en caso de no poder llevarse a cabo normalmente es de suma importancia, ya que esto podría ayudar al momento de presentarse una contingencia en donde no se contara con el apoyo computacional para realizar el proceso o cuando el usuario responsable no se encuentre en ese momento.

  Se sugiere que de existir dichos procedimientos se tengan por escrito y se hagan mención de ellos al gerente o responsable del área, y si no se cuenta con ningún método alterno se recomienda establecer uno, probarlo y ponerlo por escrito una vez probada su efectividad.

- Requerimientos mínimos de Recursos Humanos, Técnicos y Materiales. Es muy importante que los usuarios de aplicaciones definan que recursos de comunicaciones (teléfonos, faxes, etc.), papelería y formas impresas, equipos eléctrico o electrónico en particular (calculadoras, lectores ópticos, scanner´s, impresoras, etc.) y otros materiales requieren para poder realizar sus funciones adecuadamente en un centro alterno de trabajo.

  Cabe mencionar que se debe concientizar a cada usuario de que en una circunstancia de contingencia no se podrá contar con todos los elementos que normalmente utiliza para desempeñar su trabajo, y que se laboraría con los elementos mínimos necesarios para efectuar las aplicaciones.

4.3 Determinación de procesos y periodos críticos.

Uno de los aspectos fundamentales que contempla el Plan de Contingencia es la determinación de aplicaciones críticas, se considera aplicación crítica a aquella que es fundamental para la operación de la compañía, ya que al faltar esta puede ocasionar consecuencias, como:

- No contar con la información oportuna para la toma de decisiones.
- Paralizar algunas operaciones de la compañía.
- Problemas legales.

A continuación se mencionan los criterios para determinar las Aplicaciones Críticas en la empresa.

Impacto Operacional.
Grado de afectación en su operación, que sufren los procesos relacionados entre si al fallar alguno de estos.

Impacto legal y fiscal.
Consecuencias legales y/o fiscales que sufriría la empresa al dejar de realizar normalmente procesos que afectan a terceros y a los compromisos contraídos.

Impacto de imagen.
En este punto se contempla la imagen externa y la imagen interna corporativa. Es decir, hacia el exterior, las consecuencias en imagen que ocasionaría el paralizar ciertas aplicaciones con proveedores y clientes de la empresa. Hacia el interior, la imagen que ocasionaría entre el personal, el dejar de procesar la nómina por ejemplo.

Impacto de pérdida del negocio.
Se define como la baja que tendría la empresa de su permanencia en el mercado, al fallar los procesos que le dan presencia en su ámbito de negocio, es decir, al no poder responder oportunamente a las necesidades de los clientes, estos elegirán otra opción que les resuelva sus exigencias.

Impacto económico.
Se refiere a las consecuencias económicas que ocasionaría a la empresa el dejar de procesar ciertas aplicaciones. La gran parte de estas pérdidas no son cubiertas por las compañías de seguros.

En esta metodología se propone una escala de acuerdo al grado de criticidad de procesos y aplicaciones, la cual se muestra a continuación:

Grado de Criticidad de Procesos

3 Crítica. Estas funciones no pueden ser ejecutadas a menos que se consigan recursos son capacidades idénticas a las normales que reemplacen a las afectadas. No pueden ser reemplazadas por procedimientos manuales bajo ninguna circunstancia. La tolerancia a la interrupción en muy baja y el costo de la misma muy alto.

2 Vital. Estas funciones no pueden ser ejecutadas por medios manuales o pueden ser manuales por un periodo muy breve, siempre y cuando las funciones sean restauradas dentro de un cierto límite de tiempo.

1 Sensibles. Estas funciones pueden ser ejecutadas con dificultad pero a un costo tolerable durante periodos más largos de tiempo.

0 No críticas. Estas aplicaciones pueden ser interrumpidas por un lapso grande de tiempo, a un costo muy pequeño o nulo para compañía.

La alta dirección en conjunto con los gerentes de área son los que deben de definir
El factor en porcentaje de los impactos operacional, económico, legal, pérdida del negocio, y de imagen. Dicho factor de porcentaje se obtiene mediante la siguiente formula:

% Factor Valor Total = ∑ Grado de Criticidad (Impacto)/100

Ejemplo:

Factor (%)	20	10	40	10	20	100
Área	Operativo	Imagen	Económico	Legal Fiscal	Pérdida del Negocio	Valor Total
Almacén	2	0	0	0	0	0.4
Comercio Exterior	2	0	2	0	0	1.2
Compras	2	0	0	0	0	0.4
Crédito	1	1	1	0	3	1.3
Cuentas por Pagar	3	1	0	1	0	0.8
Facturación	2	2	1	1	1	1.3
Nómina	3	2	1	3	1	1.7
Ventas	3	3	2	0	3	2.3
Cobranza	1	0	3	0	1	1.6
Contabilidad	1	3	3	1	1	2.0
Costos	2	0	1	0	0	0.8
Estadísticas de Venta	2	1	0	0	0	0.5
Finanzas	0	3	0	0	0	0.3
Seguros	0	0	0	0	0	0
Tesorería	1	1	0	1	0	0.4

De acuerdo con la formula mencionada anteriormente para la obtención del factor
De criticidad para el área de ventas se obtiene de la siguiente manera:

Fórmula:

$$\textbf{Factor de criticidad} = \frac{\sum \textbf{Grado de Criticidad (Factor)}}{\textbf{100}}$$

$$\text{Factor de criticidad De Ventas} = \frac{3(20) + 3(10) + 2(40) + 3(20)}{100} = 2.3$$

En la siguiente tabla se muestran los procesos ordenados de acuerdo al resultado de la evaluación de criticidad.

Criticidad de los procesos.

Área	CALIFICACION
Ventas	2.3
Contabilidad	2.0
Nomina	1.7
Cobranza	1.6
Crédito	1.3
Facturación	1.3
Comercio Exterior	1.2
Cuentas x Pagar	0.8
Costos	0.8
Estadísticas de Ventas	0.5
Almacén	0.4
Compras	0.4
Tesorería	0.4
Finanzas	0.3
Seguros	0

4.3.1 Determinación del objetivo y alcance del Plan de Recuperación de Desastres.

El análisis anterior permitirá generar los alcances del Plan de contingencia determinando cuál es la prioridad que se dará en la recuperación a cada uno de los servicios de información, que elementos serán necesarios recuperar para que dicha información se genere y cuáles serán los procesos que deben involucrarse en el restablecimiento de los servicios.

4. 4 Requerimientos mínimos para procesar Aplicaciones Críticas.

Un centro de cómputo puede realizar cientos de operaciones que el personal y los usuarios consideren importantes, pero en un desastre no puede hacerse todo porque los recursos clave no están disponibles.

Por esto, durante un desastre, una corporación debe concentrarse en el procesamiento de cómputo que sea más importante para sus aplicaciones críticas. Hay que entender que el objetivo de un Plan de Contingencia es minimizar la perdida potencial de los activos y no el de duplicar un entorno normal del negocio.

Una primera opción es cuando se planea una recuperación total, con lo que se puede ahorrar la determinación y clasificación de los sistemas críticos, solo basta con conocer cuáles son los sistemas en producción, esta solución sería posible aunque costosa ya que la infraestructura de recuperación debe ser lo suficientemente robusta para soportar el procesamiento de todos los sistemas en producción.

Como lo anterior pocas veces es factible de realizar, entonces se deben de determinar los requerimientos mínimos de procesamiento de los sistemas críticos, que tiene como objetivo identificar todos los recursos de hardware, software, información, equipo auxiliar, provisiones, etc. que se requieren para procesar los sistemas críticos y vitales de la empresa. Los aspectos que deben identificarse son los siguientes.

a) Usuarios

Determinar el personal clave que llevará a cabo la ejecución de los procesos críticos, así como el espacio físico en el cuál se puedan instalar y trabajar en el centro de soporte alterno.

Es recomendable anexar en esta parte un diagrama de distribución del personal en el centro de soporte alterno.

b) Requerimientos de Ejecución

Se debe tener identificado el tiempo mínimo requerido para procesar aplicaciones críticas, periodos críticos, modelo de CPU, espacio en disco, memoria principal, comunicaciones, redes y diagramas de las configuraciones de redes.

c) Archivos

Archivos de datos, espacio en disco para estos archivos, es necesario identificar los usuarios que trabajen con archivos críticos, para implementar una política de respaldo.

d) Software

Sistema Operativo, Aplicaciones de Proveedores, identificar los programas dependientes, Sistemas críticos de la compañía. También es conveniente identificar el software necesario para la compilación de las aplicaciones, ya que podría ser necesario recompilar antes de instalar en el centro de soporte alterno.

e) Otros

Políticas y manuales de procedimientos (logins, passwords, manuales, documentación de las aplicaciones), impresoras, formas especiales preimpresas etc.

4.5 Comités de Recuperación.

Uno de los elementos más importantes para alcanzar el éxito del Plan de Contingencia es el personal que participará dentro del proceso de recuperación. Así los comités de recuperación están integrados por personal clave de las diferentes áreas de la empresa, esto involucra la participación de alta dirección, sistemas de información, comunicaciones, usuarios de sistemas y personal de seguridad, entre otros.

Si no se cuenta con su participación oportuna y eficaz en el momento de la recuperación, el plan no va a lograr su máxima optimización.

Es recomendable definir los comités de recuperación, dependiendo del giro y dimensiones de la empresa en cuestión. Así mismo, es necesario formalizar las funciones y actividades del personal que integra dichos comités; algunas de estas actividades a considerar son las siguientes:

- Administración del Plan
- Coordinación de la Recuperación
- Comunicación con el Exterior
- Reconfiguracion de Equipos
- Recuperación de Operaciones
- Restauración de Comunicaciones
- Administración de Computadoras Personales
- Apoyo e Interacción con Usuarios

El número de comités de recuperación puede variar, pero hay que considerar que a mayor número de comités, mayor dificultad para la coordinación de los mismos. Para definir el número idóneo se tiene que analizar la estructura de la empresa, el tipo de organización y el personal que la integra.

Estructuración de Comités

Un comité está formado por un grupo de personas, las cuales realizan una serie de actividades interdependientes con el fin de lograr un objetivo común: recuperar la operatividad de la empresa en el menor tiempo posible.

Para lograr el objetivo anteriormente mencionado, es necesario que los integrantes de los Comités hayan sido previamente capacitados, motivados y estén dispuestos a participar en forma activa en el Plan de Recuperación.

A continuación se propone una estructura de comités que resulta fácil implementar ya que intervienen las personas involucradas en el Plan.

Comité Ejecutivo: Integrado por el personal de alta dirección y los gerentes de cada centro de negocios.
Comité Sistemas: Formado por el personal del área de sistemas (responsable del área, personal de desarrollo y soporte técnico)

Comité Operativo: Integrado por usuarios de las principales aplicaciones que se llevan a cabo dentro de la empresa.

Criterios de Selección de Integrantes de Comités

Como se mencionó anteriormente, resulta fundamental el personal que va a integrar los Comités de Recuperación, ya que de la buena selección de éstos, dependerá una oportuna y eficiente participación en el Plan y por lo tanto un mejor resultado la ejecución del Plan de Recuperación de Desastres.

El personal que participe en los Comités del Plan de Recuperación de preferencia deberá cumplir con los siguientes requisitos:

- ✓ Tener un puesto con cierta autoridad y responsabilidad
- ✓ Contar con personal que lo apoye en las funciones correspondientes a su Comité
- ✓ Buena disposición para participar en el Plan

Ya seleccionado el personal, es importante capacitarlo con el propósito de que conozca la dinámica del Plan, su participación dentro de éste, la importancia de la misma, las responsabilidades y actividades especificas a cumplir en caso de desastre y la interrelación que va a tener con los demás Comités.

Cabe mencionar, que esta capacitación se debe realizar con cierta frecuencia, ya que el personal que integra los comités puede cambiar, y por lo tanto se tiene que capacitar al nuevo personal que lo reemplace.

Por otro lado a nadie le gusta pensar en desastres, no es un tema agradable, y la capacitación sirve para concientizar al personal, de la importancia de sus funciones dentro del Plan de Recuperación, así mismo de que un desastre puede ocurrir en cualquier momento, y que es necesario estar lo mejor preparado posible antes de cualquier situación que se presente.

Períodos de Funciones de los Comités

Los Comités tienen funciones específicas asignadas, las cuales se realizan en cuatro diferentes periodos: Preparación, Activación, Desarrollo y Reinstalación.

A continuación se detallan estas funciones:

Preparación; Se refiere a las actividades que se van a realizar antes de presentarse el desastre, como por ejemplo, probar y mantener actualizado el Plan de Recuperación, pruebas periódicas del correcto funcionamiento del equipo alterno, capacitación constante al personal de sus funciones dentro del plan, etc.

Activación y Operación; Se refiere a las actividades que se van a realizar durante el periodo en que ha ocurrido el desastre y la declaración oficial del mismo; a las acciones que se ejecutarán una vez declarado el desastre y activado el Plan de Recuperación.

Así como también a las actividades necesarias para instalar operaciones en un centro de soporte alterno y finalmente, a las tareas que se van a realizar para operar en el mismo, con el propósito de ejecutar los procesos críticos y recuperar en el menor tiempo posible la operatividad de la empresa.

Reinstalación, se refiere a las actividades que se van a realizar para regresar a operaciones normales de la empresa.

Al momento de presentarse una situación de contingencia, los coordinadores de cada comité se reunirán para confirmar sus funciones, disponibilidad del personal y coordinar la logística a seguir, de acuerdo a la situación de desastre en que se encuentra la empresa, después de la contingencia deben de informar el resultado de la activación del Plan de Contingencia.

Determinación de los Niveles de Autoridad

Cada Comité deberá tener cierto nivel de autoridad. Los comités de recuperación deberán contemplar tres niveles de autoridad: máxima, intermedia y limitada.

En el Comité Ejecutivo siempre tendrá la autoridad máxima, ya que es el único que tiene la responsabilidad de aprobar el impacto del desastre declarado y activar el Plan de Contingencia en caso de ser necesario. Su participación dentro del Plan es fundamental ya que este Comité resolverá situaciones críticas que se vayan presentando durante el desastre.

El Comité Sistemas tiene un nivel de autoridad intermedia, ya que tiene la función principal de coordinar las actividades informáticas dentro del Site alterno, así como mantener la operación del equipo de cómputo. Además, mantendrá una comunicación continua con el Comité Ejecutivo para el monitoreo y evaluación del Plan.

El comité Operativo cuenta con un nivel de autoridad limitada, ya que las decisiones que se tomen se tendrán que comunicar tanto al Comité Ejecutivo como al Comité Sistemas para su estudio y aprobación.

Pero aún cuando los diversos comités tienen diferentes funciones y niveles de autoridad los comités deberán trabajar conjunta e interrelacionadamente entre sí, desde el momento que se presenta la contingencia hasta que se restablece la operación en el centro de trabajo original, asumiendo la responsabilidad para realizar la evaluación de los daños y pérdidas originadas por la contingencia, tomar las decisiones pertinentes y seguir una secuencia de actividades previamente definidas, las cuales llevarán a recuperar la operatividad de la organización.

4.6 Determinación de Centros de Soporte Alternos.

En el caso de ocurrir un daño en el Site donde actualmente se encuentran instalados los sistemas de información de la compañía, debe contarse con alternativas para trasladar la operación a otro lugar de trabajo donde se cuente con las instalaciones y el equipo de cómputo adecuado que soporten la reactivación de los sistemas de información prioritarios para la empresa.

En el centro de soporte alterno se buscará en lo posible reducir al mínimo el intervalo de tiempo entre la ocurrencia del desastre y el punto en que se reanude la operación, además de que los usuarios deben poder trabajar normalmente como si se encontraran en las instalaciones originales de la empresa.

Al seleccionar un centro de soporte alterno se deben tomar en cuenta muchos factores, pero indudablemente el más importante es que sea suficiente para soportar los objetivos de recuperación que han sido previamente establecidos.

Características del centro de soporte alterno:

El centro de soporte alterno debe contar con ciertas características necesarias para poder garantizar la continuidad de la operación al momento de ocurrir la contingencia.

Estas características o requisitos están en función de las necesidades de la empresa y sus prioridades van desde la deseable hasta la indispensable. A continuación se mencionan:

- La instalación debe contar con un equipo de cómputo que soporte a los sistemas de información críticos que actualmente operan en la empresa y dar servicio al número de usuarios que se definieron en el Plan de Contingencia.

- El equipo de cómputo del punto anterior, debe tener un site dentro de las instalaciones alternas que cumpla con todos los requerimientos de instalación física que recomienda el fabricante para su operación como lo es: temperatura, piso, techo falso, instalación eléctrica, humedad del ambiente, acceso controlado, etc.

- El centro alterno debe contar con un intervalo de tiempo muy corto para ponerse en operación después de ocurrida la contingencia en el Site primario.

- Cumplir con la compatibilidad del Hardware y Software.

- Contar con la suficiente infraestructura de comunicaciones.

- Suficientes períodos para pruebas.

- Cumplir con relaciones de Costo – Efectividad.

- Las instalaciones del centro deben poder albergar cómodamente a los usuarios que utilicen los servicios de información, proporcionándoles lugares de trabajo adecuados y los servicios de oficina que ocuparán para su labor.

- A los usuarios se les debe poder dar servicio tanto de terminal para acceso a equipo central como a PC´s para trabajos de oficina según sea el caso.

En la ubicación geográfica del centro de soporte alterno debe considerarse lo siguiente:

- No debe encontrarse en un lugar que dificulte el acceso y la transportación para los usuarios que participarán en el Plan de Contingencia.

- Las incidencias de catástrofes en la zona debe ser las mínimas posibles
- (Considerando sismos, inundaciones, actos antisociales, incendios, apagones, etc.)

Si no se puede cubrir en su totalidad el punto anterior por lo menos debe buscarse que un mismo tipo de catástrofe no afecte al mismo tiempo al centro primario y al centro alterno.

- Apoyo del Personal.

- Requisitos contractuales.

Capítulo 5.
Simulacros

5.1 Introducción a los Simulacros del Plan de Recuperación.

Las organizaciones que han desarrollado Planes de Contingencia se pueden dividir en tres categorías:

En la primera categoría se encuentran aquellas que no hacen nada para realizar una medición de su vulnerabilidad o reducir el efecto potencial de un desastre.

El segundo grupo desarrolla un Plan de Recuperación ante un desastre solo para satisfacer a los auditores y directivos, pero nunca enseñan a su personal a usar el plan, jamás prueban sus estrategias y procedimientos.

La tercera clase no solo invierte sus recursos en el desarrollo de un plan, sino que también demuestra la viabilidad de éste a través de un regular régimen de pruebas.

Un plan de recuperación es una actividad que no tiene término, y que requiere de un continuo proceso de revisión que vaya de acuerdo con la dinámica que presente la organización. La preparación ante una contingencia debe ser continua para evitar las posibles deficiencias que se pueden presentar al momento de la ejecución del plan, así como para contabilizar y tener en cuenta los posibles cambios en las aplicaciones, en los respaldos, en el personal y en los recursos contemplados para el Site alterno.

Los simulacros son actividades que se llevan a cabo para demostrar la efectividad de un Plan de Contingencia y con esto cumplir con el objetivo de dicho Plan que es el de recuperar lo mas pronto posible la operatividad de la empresa.

Un simulacro se refiere a probar el Plan de Recuperación simulando que la empresa se encuentra en una situación de desastre. En esta prueba se trata de utilizar todos los recursos necesarios relacionados con el plan para restablecer la operatividad de la organización en el Centro de Soporte Alterno seleccionado.

Se considera que un simulacro tiene éxito cuando la operación de los procesos y aplicaciones críticas se han recuperado en forma satisfactoria y en un periodo de tiempo razonable. El realizar simulacros también es sano por los cambios que se presentan en la organización con respecto a los sistemas y redes, de tal forma que se asegure que el plan esté al día.

Aunque los cambios en el plan deberían ser manejados por eventos mas que por un período programado, los planes deben ser también probados y regulados frecuentemente, algunos afirman que cada seis meses. Esto es porque los empleados son constantemente removidos de sus puestos, cambian sus números telefónicos o intercambian responsabilidades. Los usuarios entonces deberán practicar el poder conseguir realizar su trabajo sin causar impacto a los clientes en el evento de un desastre. Con este hecho se demostrará la crítica relación que existe entre el equipo de soporte a sistemas y el equipo de producción.

El realizar simulacros es un camino para reafirmar la adaptación de las estrategias de recuperación que adoptó la empresa para encontrar pequeños imprevistos; se puede verificar que los requerimientos establecidos son los suficientes para la recuperación y permite identificar nuevos requerimientos. También es una oportunidad para evaluar nuevas tecnologías para una posible contribución en el proceso de recuperación.

Además, el hecho de probar el Plan de Recuperación permite a los participantes de este conocer sus papeles al momento de presentarse una contingencia, un estricto simulacro demuestra que el plan trabaja efectivamente y ayuda a asegurar que se mantendrá así. También se recomienda que las compañías comiencen la prueba de sus estrategias de recuperación al menos tres veces en el primer año.

A causa del gasto involucrado, algunas compañías frecuentemente no invierten el suficiente tiempo en probar el Plan de Recuperación en el Site designado o usualmente solo invierten lo suficiente para identificar nuevos problemas. El realizar simulacros es caro y difícil de justificar, y muchas organizaciones no están en la posibilidad de realizar esta continua inversión.

Algunas empresas desarrollan su plan de contingencia y sin embargo nunca lo prueban. Los simulacros demuestran la efectividad del plan recuperar lo más pronto posible la operatividad de la empresa.

El realizar simulacros permite corregir posibles deficiencias del plan, ya que no se conoce que tan bien funciona el Plan de Recuperación hasta que se prueba. Por lo que después de realizar un simulacro, el plan ya no es solamente un documento teórico, sino que se convierte en un documento dinámico y práctico, al probar su efectividad.

5.2 Objetivos del Simulacro.

Uno de los objetivos principales de los simulacros es determinar la efectividad del plan y verificar la adecuación de los procedimientos utilizados para el proceso de recuperación, es decir, va a permitir demostrar que el plan está documentado de tal manera que permite la adecuada recuperación de las aplicaciones críticas en caso de un desastre.

El propósito inmediato de llevar a cabos simulacros es descubrir defectos en los procedimientos o errores en los planes existentes. A largo plazo, el objetivo es enseñar a los participantes como reaccionar de forma racional ante la irracionalidad de un desastre. Mientras los planes de contingencia no pueden predecir todos los efectos de un desastre, los simulacros prueban como enfrentar a lo inesperado de forma metódica y efectiva. Los miembros de equipo de recuperación pueden comenzar a usar los procedimientos de rutina como punto de inicio en la recuperación en el caso de una actual emergencia.

Con la realización de simulacros se busca asegurarse que cada una de las acciones definidas en cada una de las fases del proceso de recuperación cumple con el cometido para el cuál fue desarrollada (recuperar las funciones principales de la organización), y en caso contrario, determinar cuales fueron las circunstancias y problemas que impidieron que se alcanzaran los objetivos. Las conclusiones que se obtenga de esto serán retroalimentadas al plan para realizar las modificaciones necesarias

Durante los simulacros se prueba la coordinación de los comités de recuperación, todos los procedimientos en detalle, los registros que se almacenan en la localidad externa, la compatibilidad del Centro de soporte alterno con las necesidades de la empresa, la respuesta de todo el personal externo involucrado en el plan, la logística de recuperación y los tiempos que se han estimado para cada actividad entre otros aspectos.

Así mismo, las pruebas del plan sirven como entrenamiento para los integrantes de los equipos de recuperación porque dan una oportunidad a los equipos para familiarizarse un poco más con sus papeles en la recuperación de desastres.

Los simulacros constituyen también un medio valioso para determinar si el personal involucrado dentro del proceso de recuperación ha sido entrenado y orientado adecuadamente, si los procedimientos propios de cada usuario funcionan apropiadamente en la nueva configuración del Site alterno, y si la comunicación entre cada uno de los comités es la correcta.

Cabe aclarar que no se trata de evaluar la capacidad del personal, solo se trata de conocer los problemas a los que se puede enfrentar el personal, con el fin de buscar soluciones óptimas y documentar éstas en el plan de acción.

El simulacro contempla generalmente, la recuperación de algunas aplicaciones críticas y de su ambiente operacional, así como los procedimientos de evacuación del personal y la notificación a los principales clientes, proveedores y al corporativo.

Los simulacros deben realizarse cada cierto periodo de tiempo y no en forma continua, ya que se necesita un periodo en el cuál se realicen todos los cambios necesarios para ajustar el plan. Así mismo, los simulacros pueden ir avanzando en su complejidad, de ahí la importancia de determinar el alcance de cada simulacro.

5.3 Definición de Escenarios de Recuperación y Actividades a Realizar.

Con el fin de mantener un programa permanente de simulacros y lograr que éstos comprendan todos los aspectos que deben probarse en forma individual o combinada, se debe diseñar un programa general de pruebas donde se señalen tiempos y características generales, así como los alcances de dichas pruebas.

La frecuencia de las pruebas debe basarse en la frecuencia de los cambios en el entorno de cómputo, los cuales a su vez, obedecen a los cambios que se suscitan en el negocio. De cualquier forma, debe establecerse una cantidad mínima de pruebas al año.

Es importante recalcar que las pruebas deben realizarse sin causar perturbaciones al procesamiento de cómputo, al menos sin causar inconvenientes a los usuarios de los sistemas ya que no tendría caso crearle problemas artificiales a la empresa.

Definición del escenario de recuperación.

Como se mencionó anteriormente, se define como escenario de recuperación a la situación que enfrenta la empresa como consecuencia de un desastre, Así, el comité Directivo, en conjunto con el área de sistemas, debe determinar que situación crítica se desearía que la organización enfrentara al ocurrir una contingencia y las consecuencias que ésta originaría, todo con el objeto de probar la logística de recuperación planteada y medir el desempeño de cada uno de los comités involucrados.

Es importante señalar que el planteamiento del simulacro debe estar de acuerdo a los riesgos reales a los que se encuentra expuesta la empresa para así poder hacer una prueba que se acerque a su posible realidad. Este paso es muy importante, ya que las actividades que se lleven a cabo antes, durante y después del simulacro van a depender del escenario de contingencia que la empresa haya decidido emular.

El planteamiento del simulacro elegido por el comité ejecutivo debe contemplar lo siguiente:

- Se debe plantear el tipo de desastre que dio origen a la contingencia.
- Las consecuencias originadas, es decir que áreas fueron afectadas y en que forma.
- El o los equipos dañados.
- El día en que se realizará la prueba (recomendándose que se lleve a cabo en un día no laborable).
- La hora de inicio del simulacro.
- Los períodos críticos que se están suponiendo como afectados.
- Las aplicaciones críticas involucradas.
- El personal que participará en el simulacro.
- Los respaldos involucrados así como el o los procesos de restauración de dichos respaldos.
- Los registros vitales.
- Las formas preimpresas necesarias.

Todo lo anterior debe estar basado en el manual de recuperación diseñado anteriormente.

Actividades a realizar:

a) Identificación de las áreas involucradas y aplicaciones críticas.

De acuerdo al escenario de recuperación que se haya definido y la fecha que se haya propuesto que ocurriera la contingencia, el comité ejecutivo se reunirá y determinará, basándose en la tabla de periodos críticos integrada en el manual de recuperación aquellas aplicaciones que se verán implicadas o afectados directamente en su operación normal. Dicho manual ayudará a la definición de cuales serán las áreas involucradas y el personal que será requerido para efectuar el simulacro.

b) Identificar los recursos humanos, técnicos y materiales involucrados en el simulacro.

Una vez definido el punto anterior, se localizará en la carpeta del plan al personal por aplicación que se encargará de procesar aquellas aplicaciones que van a recuperarse. Paralelamente, se determinará el equipo de cómputo, comunicaciones, líneas telefónicas, papelería, formas preimpresas y respaldos que serán requeridos para llevar a cabo el simulacro, todo esto dependiendo del alcance de la prueba planteado inicialmente por los comités ejecutivos y de sistemas.

c) Desarrollo de la prueba del plan.
Se lleva a cabo el simulacro de acuerdo a la logística del plan que se encuentra dentro del manual de recuperación. Se indica a las personas involucradas el objetivo de la prueba, cual es su lugar dentro del site, cual será el horario de trabajo y las nuevas condiciones para llevar a cabo las actividades, la forma de transportación al site secundario. Cada uno de los coordinadores de los comités involucrados deberán estar pendientes del desarrollo del la prueba para poder presentar ayuda a los usuarios que así lo requieran y por si es necesario tomar una decisión importante que se deba resolver en el momento.

d) Conducción de la prueba

El comité ejecutivo, en conjunto con el operativo, nombrará a la persona que supervisará y anotará en una bitácora todos aquellos hechos acontecidos durante el progreso de la prueba. Se debe llevar un registro durante el desarrollo del simulacro donde se anoten todos los problemas encontrados, las causas que las originaron y las soluciones tomadas en ese momento, el desempeño del personal dentro del site, y todo lo relevante que se haya observado, con el propósito de llevar una bitácora de todo lo ocurrido durante el simulacro. Este punto es de suma trascendencia, ya que toda esta información será fundamental para la evaluación de los resultados de la prueba.

e) Evaluación de los resultados.

Se debe comparar el objetivo del simulacro con los resultados obtenidos al finalizar la prueba, todo esto con el fin de identificar los problemas que se presentaron y sus causas, así como los aciertos y las soluciones encontradas durante la prueba, con el propósito de evitar dichos problemas en el futuro y documentar las nuevas soluciones dentro del manual del Plan de Recuperación.

Se evalúa también el desempeño del personal involucrado, su respuesta ante lo limitado de los recursos y su comprensión y adecuado seguimiento de la logística establecida en el manual.

f) Retroalimentación y ajuste del Plan.

En base a los resultados de la evaluación de la prueba, se deberán realizar las modificaciones y los ajustes necesarios al plan para que éste corresponda a la realidad de la empresa y sea lo más eficaz y confiable posible.

g) Repetición de las pruebas necesarias hasta que se cumplan los objetivos deseados en forma satisfactoria.

Es necesario que si alguna de las pruebas no resulto como se esperaba o si se realizaron cambios importantes dentro del Plan de Recuperación , se lleven a cabo nuevos simulacros para ajustar o verificar que los cambios efectuados cumplen con los objetivos trazados en un principio, asegurándose que ningún detalle se haya pasado por alto.

En resumen es importante realizar simulacros con el fin de probar la efectividad del plan y evaluar sus capacidades, así como también es conveniente considerar el alcance del simulacro, ya que dependiendo de esto, el costo de inversión para llevar a cabo las pruebas variará, lo cual es otro aspecto que la empresa deberá tomar en cuenta y que puede ser limitante para poder efectuar las pruebas necesarias.

Capítulo 6.
Mantenimiento y Actualización.

6.1 Introducción al Mantenimiento y Actualización

Cuando una organización adquiere por primera vez una computadora, gran parte de las labores de programación tienen como fin el desarrollo de aplicaciones nuevas. Pero conforme crece el número de programas implantados en la organización, no es raro ver que se dedique más tiempo a la actividad de programación que al mantenimiento.

Durante el ciclo de vida de una aplicación ordinaria, los costos de mantenimiento y mejoras pueden ser de dos a cuatro veces mayores que los costos del desarrollo inicial.

El mantenimiento de los sistemas existentes dentro de una organización puede tomar igual o mayor importancia que el desarrollo de nuevos sistemas. Los cambios en las condiciones externas o internas dentro de una empresa, la obligan a modificar y actualizar constantemente los sistemas desarrollados. Dentro de las modificaciones más frecuentes que se pueden enumerar están las condiciones de operación de un área o de toda la organización; en la aparición de nuevas necesidades para los usuarios; Los cambios en las reglas de negocio, en la modificación de las leyes actuales, etc.

Lo anterior hace necesario el modificar continuamente los programas y sistemas existentes. Esto es posible que abarque desde el análisis del problema hasta el diseño y preparación del sistema. No obstante los gerentes que prefieren la creación de nuevos programas, frecuentemente hacen caso omiso de la necesidad de mantener los ya presentes.

El mantenimiento resulta fundamental en un plan de contingencia pues se trata de un plan dinámico, sujeto a los cambios que se presenten dentro y fuera de la organización, por lo cuál debe estar igualmente subordinado a una revisión constante y minuciosa, logrando con esto que la información contenida dentro del plan corresponda a la realidad de la empresa, manteniendo así su efectividad en una situación de desastre.

6.2 Actualización de la Información.

El mantenimiento del Plan de Recuperación se refiere a renovar periódicamente la información contenida dentro del mismo, con el propósito de contar en todo momento con los datos reales que reflejan la situación actual de la organización. Es decir, es importante revisar y ajustar periódicamente el contenido del plan en función de los posibles cambios en el hardware, software y personal.

El mantenimiento resulta fundamental en un Plan de Recuperación, y debe realizarse en periodos semestrales, o antes si ocurren cambios que así lo ameriten, ya que por completa que sea la metodología empleada, si la información contenida en el plan no se actualiza, éste pierde su efectividad.

A continuación se mencionan algunas preguntas que ayudaran a mantener actualizado el Plan de Recuperación.

1. ¿Estamos actuando rápida y eficazmente ante un evento de desastre, conforme lo indica el plan?
2. ¿Es adecuado el plan, para los casos de desastre presentados hasta ahora?
3. ¿Soporta el plan, cambios a futuro de crecimiento y desarrollo?
4. ¿Han surgido nuevas vulnerabilidades o amenazas no contempladas hasta ahora en el plan?
5. ¿Se están repitiendo con frecuencia eventos similares de desastre?
6. ¿Se detectaron fallas o “huecos” en el plan durante los ensayos?
7. ¿Es clara la información escrita en el plan?
8. ¿Se están cumpliendo los objetivos originales del plan?
9. ¿Se están respaldando y recuperando adecuadamente los registros vitales?
10. ¿Se están recuperando los datos almacenados dentro del tiempo estimado?
11. ¿Es correcta la secuencia de tareas, propuesta por el plan para la recuperación de desastres?
12. ¿Están todas las aplicaciones críticas incluidas en el plan?
13. ¿Esta actualizada la lista de datos de todos los equipos del DRP?
14. ¿Se están administrando correctamente los datos almacenados fuera de sitio?
15. ¿Se han cambiado los contratos con los proveedores, para ajustarse al plan?
16. ¿Se ha cambiado el software o hardware, para cumplir las demandas del plan?

Así, el proporcionar un mantenimiento adecuado y oportuno al plan, conlleva las siguientes ventajas:

- El Plan se mantiene actualizado.
- Se garantiza que el plan refleje y responda a los cambios ocurridos dentro de la organización.
- Mantiene a los directivos de la empresa familiarizados con el Plan.
- Los simulacros son más fáciles de llevar a cabo.

Como toda organización cambia, el plan constantemente debe someterse a una revisión y adecuación constante, que lo mantenga vigente para todos los cambios de tecnología y de estructura organizacional.

Se sugiere que el responsable de llevar el mantenimiento del Plan de Recuperación dentro de una empresa sea el coordinador del plan.
El mantenimiento de la información del Plan de Contingencia involucra varias funciones:

a) Determinar los métodos para efectuar las revisiones del contenido del plan.

Se deben desarrollar procedimientos para realizar los cambios, así como el calendario en que se efectuarán éstas, de manera regular y sistemática. Esto es de gran utilidad para los centros que generan y proporcionan los datos, ya que es una forma de auto-auditarse en la forma como se lleva a cabo el control y el manejo de la información.

b) Recepción y captura de información actualizada.

Recibir la información que cada área generó y su captura dentro del software de apoyo. Para esto, el responsable del mantenimiento deberá mandar un recordatorio a cada gerente de departamento con una semana de anticipación, con el fin de que éstos entreguen su reporte en el día acordado. Una vez que se haya obtenido la información, se captura dentro de la aplicación de apoyo al Plan de Recuperación.

Se necesita contar con los elementos necesarios para preguntarse de que manera debe cambiar el plan para que se refleje los cambios ocurridos en la empresa. Para cada nuevo sistema que se desarrolle o se instale, se debe preguntar si es crítica o no. Si la respuesta es afirmativa es necesario especificar los elementos que son necesarios para su recuperación y los cambios que se tengan que realizar al plan.

Esta es una etapa de suma importancia, ya que es aquí donde el responsable del mantenimiento al plan puede advertir que se presentaron cambios importantes, ya sea dentro del personal crítico de la empresa o en las aplicaciones críticas en sí, como por ejemplo cambio de prioridad en alguna aplicación, equipo donde reside dicha aplicación, periodos críticos o cambios en el personal involucrado en el desarrollo del Plan de Recuperación.

Si esto ocurre el responsable del mantenimiento al plan, deberá de notificarlo al comité ejecutivo con el fin de hacerle de su conocimiento estas modificaciones.

Los responsables de los comités ejecutivos, de sistemas y operativo deberán entonces reunirse para analizar los cambios que se hayan presentado, y en base a este análisis, se deberán realizar los ajustes necesarios en el orden de recuperación, se establecerán los nuevos procedimientos de rehabilitación ante una contingencia, se capacitará al nuevo personal crítico y se deberá realizar un simulacro para probar que los cambios hechos fueron los correctos.

c) Distribución del Plan de Recuperación actualizado.

El correcto funcionamiento del DRP, requiere de la oportuna participación de todas sus partes. El “equipo DRP”, líderes y miembros, junto con otros participantes, deben conocer bien su papel y responsabilidad en el plan. Su tarea deberá ser ejecutada con ejemplar dominio y exactitud, para garantizar el éxito del plan.

El procedimiento para la distribución del plan debe informar de dicho plan a los equipos participantes y al resto de la organización. En la lista de contactos se podrá encontrar los nombres de todas las personas a las que se debe distribuir el documento del Plan de Recuperación de Desastres.

La adecuada distribución y promoción del plan determinarán finalmente su buen éxito. Es por ello indispensable, que el líder de cada uno de los equipos debe asegurarse de

que todo su equipo, esté perfectamente enterado de la visión global del plan, de su papel y de la responsabilidad que se le esta encomendando.

El líder puede tomar ventaja de toda la diversidad de medios informativos disponibles a su alcance para distribuir el plan a su equipo, pero los medios usados deben alcanzar a todo el universo posible de participantes.

Una vez hechos los ajustes necesarios, el encargado del mantenimiento al plan deberá registrar los cambios en la aplicación de apoyo con el objetivo de mantenerlo actualizado, imprimirá todo el manual del plan, y proporcionará a cada uno de los comités una copia para su distribución. El responsable de cada comité es responsable de que el documento no llegue a manos no autorizadas.

Es necesario que el encargado del mantenimiento al Plan, entregue al responsable del site alterno copias actualizadas del Plan en donde se especifique el número de versión del manual, para evitar confusiones y además retirar la versión anterior del Plan de Recuperación.

Este punto merece cierta consideración y cuidado en su ejecución, debido a que el manual del plan de recuperación contiene mucha información confidencial de la empresa, por ejemplo, contiene la lista de sus principales proveedores y clientes, los datos generales de los empleados y directivos, aplicaciones críticas, políticas de respaldo, localización de los registros vitales, inventario de equipo, etc.
Además, es necesario guardar una copia del plan en un lugar externo. Se recomienda que éste sea guardado en el domicilio particular del director de la empresa.

El responsable del mantenimiento tendrá que actualizar la información en el software del plan durante los primeros tres días después de haber recibido los cambios, y en un periodo de tiempo razonable deberá entregar las copias del plan actualizado a los diferentes responsable de los comités antes de realizarse el simulacro, una vez que todos los comités cuenten con el manual actualizado se llevará a cabo una sesión donde se expongan los cambios que se presentaron, se muestren las nuevas estrategias de recuperación y/o se recuerden las ya definidas inicialmente.

d) Mantener el historial de las revisiones al Plan de Recuperación.

El responsable del mantenimiento deberá llevar un registro de cada fecha en que se realizó la actualización del plan y el número de versión correspondiente. De la misma forma, deberá guardar un respaldo de cada una de las versiones del manual de apoyo al plan para cualquier aclaración.

e) Adecuar el período de revisión del Plan

Es necesario que el responsable del mantenimiento adecue el periodo de revisión del plan con los calendarios de entrenamiento y simulacros, para que al realizarse éstos, se cuente con la información real y representativa de la organización en ese momento.

Pruebas al Plan de Recuperación de Desastres.

Las pruebas al Plan de Recuperación en caso de desastre es la única manera confiable de asegurar que el plan funciona y es efectivo en el caso de un desastre real. Mientras más real una prueba simule los efectos de un desastre sobre los recursos de

IT, más útil y concluyente será esta. Las pruebas deberán validar por lo menos una vez al mes que los registros vitales se encuentran disponibles y que estos pueden ser recuperados y utilizados.

Las pruebas de Recuperación en caso de desastre es una responsabilidad compartida entre el equipo DRP y los usuarios finales, y ambas partes deben estar de acuerdo con los objetivos de las pruebas. El equipo DRP normalmente se encargará de la simulación de la recuperación mientras que el usuario deberá validar junto con el equipo DRP, los resultados de las pruebas. El usuario final será el encargado de dar la aprobación final de los resultados de las pruebas. Debe tomarse el debido cuidado al asegurarse de que la totalidad del plan es probado.

El plan debe considerar las amenazas y vulnerabilidades a que se expone o expondrá las funciones críticas del negocio soportadas por IBS, con el fin de cubrir todos los eventos posibles de contingencia.

Cuando se analizan los posibles eventos que pueden crear situaciones de contingencia, lo que se está haciendo en realidad es simular eventos que generen desastres, para proceder a prevenirlos o en su caso corregirlos oportunamente cuando se presenten.

Frecuencia de Pruebas:

Para ser útil, un Plan de Recuperación en caso de desastre de mantenerse actualizado. Cambios en la tecnología, requerimientos del negocio, y cambios en las regulaciones de gobierno pueden causar un continuo cambio en el ambiente de sistemas (IT). Cuando estos cambios tienen lugar, La Evaluación del Riesgo, Los Requerimientos para la Planeación de Recuperación en caso de desastre y Los Planes de Recuperación en caso de desastre necesitan ser revisados para determinar si se requiere hacer cambios a estos.

Durante las pruebas de Recuperación en caso de desastre es frecuente que los equipos identifiquen errores en los diferentes supuestos, o procesos que necesitaran ser corregidos o cambiados en la Planeación de Requerimientos de Recuperación en caso de desastre y/o en el Plan de Recuperación en caso de desastre. Estas correcciones o cambios deben realizarse antes de la preparación del reporte final de la prueba.

6.3 Mantenimiento al Software de Apoyo al Plan.

Debido a que las empresas continuamente están en situaciones cambiantes dado el deseo de responder mejor a las necesidades de sus clientes, sus métodos y procedimientos se deben de actualizar y reestructurar.

Con el objetivo de tener al día la información del Plan de Recuperación y de que esta siempre responda a las necesidades de la empresa, es una buena práctica contar con una herramienta de apoyo al Plan de Recuperación, con la cual se obtendrán las siguientes ventajas:

- Obtener una guía para el desarrollo del Plan de Contingencia.
- Agilizar el proceso de documentación.
- Optimizar el manejo de información.
- Facilitar el mantenimiento y actualización.
- Brindar seguridad a la información.

El correcto mantenimiento consistente en la actualización de la información contenida en el Software, será fundamental para el buen desempeño del Plan de Recuperación de Desastres, se sugiere que sea el equipo de Administración del Plan el que se encargue de realizar esta tarea y además de distribuir las modificaciones realizadas al software.

Objetivos Del Mantenimiento.

La Aplicación de apoyo al Plan debe ser una herramienta de automatización de procesos, y que debe cambiar en la medida que el proceso se modifique, siempre buscando satisfacer los objetivos del Plan de Recuperación presentes de la compañía.

Los cambios en la aplicación deben fundamentarse en los resultados obtenidos de las actividades de retroalimentación al Plan de Contingencia, determinado si existen actividades que impacten directamente sobre el software. Dichos cambios deben realizarse planeadamente y buscando conservar la integridad de toda la aplicación.

Al realizar modificaciones al software, debe recordarse actualizar todos los documentos que giran en torno a él, como lo es el manual de usuario.

A continuación se enuncian las causas más relevantes que implican cambios en la aplicación:

- Resultados de simulacros. Posterior a la realización de un simulacro se presentan en ajustes a realizar dentro del Plan de contingencias; cuando el software no pueda cumplir con los cambios necesarios, entonces este debe modificarse.

- Fallas de operación. Al momento de registrarse una falla en la aplicación debe determinarse si se trata de un problema que pueda arreglarse manteniendo la funcionalidad original de la aplicación o esta deba ser modificada.

- Cambio en el Plan de Contingencia. El Plan de Contingencia puede verse afectado por diversas causas que puedan ser: Cambio en los objetivos de la

Empresa, modificación de procesos, reingenierías, etc., cuando esto suceda debe evaluarse si hay impacto en la aplicación.

- Mejora continua. Es válido modificar la aplicación para optimizarla o mejorar su funcionalidad aunque actualmente cubra los objetivos para lo que esta hecha.

Consideraciones de realizar modificaciones al software de Apoyo al Plan

Al realizar una modificación dentro del software se debe tomar en consideración los siguientes puntos:

- Análisis del cambio y autorización, el cambio debe ser propuesto por el personal involucrado en el Plan de Contingencias puesto que este es quién conoce las necesidades del caso y debe ser analizado por el responsable de la aplicación para determinar su impacto.

- Impacto de los cambios. El realizar una modificación a la aplicación comprende analizar los impactos que este pudiese tener en el resto del software, por ejemplo, al agregar un campo más a un reporte, si este no existe en la base de datos y no es resultado de un cálculo, es obligado que se agregue en la pantalla de captura.

- Consistencia de la documentación del Plan en relación a las modificaciones al las modificaciones solicitadas al Software.

- Dimensionar los tiempos de desarrollo que implicarán las modificaciones solicitadas.

- Notificación. Una vez realizada la modificación debe informarse al personal que tenga contacto directo con la aplicación y de ser un cambio mayor debe notificarse a los comités de recuperación.

Capítulo 7

Conclusiones

En la actualidad los avances tecnológicos son un factor determinante para el logro de las operaciones en un entorno empresarial, las empresas están comprometidas a ofrecer a sus clientes mayor calidad en sus servicios para lograr esto, realizan grandes inversiones en infraestructura tecnológica e informática. Ante este hecho es necesario incrementar nuestros conocimientos referentes a los temas de seguridad y vulnerabilidad de la información. Dada la dependencia creciente entre la empresa y los sistemas de información se deduce la importancia de contar con un Plan de Recuperación.

Un plan de contingencia o plan de recuperación en caso de desastres es una guía para la restauración rápida y organizada de las operaciones de cómputo después de una suspensión. Especifica quién hace qué y cómo. Los objetivos de dicho plan son los de restablecer, lo más pronto posible, el procesamiento de aplicaciones críticas, para posteriormente restaurar totalmente el procesamiento normal de la empresa.

Mediante el estudio realizado en el presente trabajo de investigación podemos concluir que el desarrollo de un Plan de Recuperación debe de cumplir con los siguientes puntos:

- Tomar en cuenta el objetivo de la empresa, esto nos permitirá conocer las partes más vulnerables a una contingencia.

- Analizar las aplicaciones automatizadas y su grado de dependencia con respecto a los procesos críticos de la compañía.

- Analizar los procesos críticos y los periodos críticos en los que se llevan a cabo dichos procesos.

- Definir el alcance y objetivo del Plan de Contingencia.

- Establecer los comités de recuperación así como su función dentro del Plan de Recuperación.

- Sensibilizar al personal directivo y al involucrado en el plan de contingencia, ya que sin su apoyo no se obtendrán los resultados esperados.

- Establecer los posibles escenarios de contingencia a los que se encuentra expuesta la organización. Estos van desde una pequeña falla en el sistema, hasta la perdida total del mismo, lo que implicará el tiempo que se necesitará para restaurar la operación normal.

- De acuerdo a las posibilidades económicas y a los resultados arrojados por el análisis efectuado se deberá elegir el Centro de Soporte Alterno óptimo

- Realizar simulacros de manera periódica a fin de evaluar la eficiencia del Plan de Recuperación.

- Retroalimentar y mantener actualizado el Plan de Recuperación.

El contar con un plan de Recuperación de Desastres representa las siguientes ventajas para una compañía:

- Tener un plan documentado con los procedimientos y acciones específicas a seguir en diferentes escenarios de desastre.
- Agilizar los procedimientos del proceso de recuperación para restablecer la operatividad de la empresa en el menor tiempo posible.
- Proporcionar lo más rápido posible soporte a las áreas críticas de la empresa.
- Registrar mínimas pérdidas económicas y/o de información en caso de desastre.
- Identificar los procesos y aplicaciones críticas dentro del portafolio de aplicaciones de la empresa y su prioridad a recuperar en caso de una situación de desastre.
- Tener documentados los recursos humanos, técnicos y materiales requeridos por la operación de los procesos y aplicaciones críticas en una situación de desastre.
- Contar con el personal capacitado para actuar en situación de desastre

Ahora bien existen en el mercado actualmente una variedad de herramientas que apoyan estos Planes de Contingencia con el fin de que las empresas obtengan un apoyo en la implementación de este tipo de Planes.

Por otra parte podemos concluir que la mejor forma de probar el Plan de recuperación, es creando una situación de contingencia en donde se apliquen y evalúen todos los procedimientos de recuperación, y de acuerdo a los resultados de esta prueba se harán las modificaciones requeridas al Plan de Contingencia.

Con respecto al caso práctico mencionado en el Apéndice A, desarrollado para la empresa Grupo Galaxy Mexicana S.A. de C.V. Podemos concluir que resulto de gran utilidad para la compañía contar con un sistema para la actualización y mantenimiento de su Plan de Recuperación.

Esperamos que el trabajo elaborado dé una visión del desarrollo de Planes de Contingencia, su importancia en la empresa de hoy y el importante papel que juega el departamento de sistemas en la implementación de éstos.

APENDICE A

CASO PRÁCTICO

GRUPO GALAXY MEXICANA DIRECTV™

CASO PRÁCTICO

Introducción

De acuerdo a la metodología mencionada en el capítulo 4, Desarrollo de Un Plan de Contingencia, cuyo objetivo es el de analizar, desarrollar e implementar un Plan de Recuperación de Desastres para empresas con información tecnológica, se presenta el siguiente caso practico el cual se llevo a cabo en base a la metodología propuesta en este trabajo de investigación.

Metodología Propuesta.

Se propone desarrollar un Plan de Recuperación de Desastres que contemple las siguientes características:

- Los riesgos y los porcentajes de factibilidad de estos, a los que esta expuesta la organización.
- La asignación de responsabilidades al personal, tanto en las actividades que se realizaran durante la emergencia como en las de preparación y las de recuperación de las aplicaciones críticas.
- La identificación de las aplicaciones (sistemas automatizados) de mayor importancia dentro del procesamiento de datos.
- La especificación de alternativas de respaldo.
- La definición de procedimientos y políticas a seguir durante el momento de la crisis.
- La integración de prácticas de mantenimiento, entrenamiento y pruebas del Plan de Recuperación.

Dentro del desarrollo del Plan de Recuperación se propone desarrollar un sistema que sirva como herramienta de apoyo al Plan de Recuperación, obteniendo así las siguientes ventajas:

- Contar con una guía para el desarrollo del Plan de Contingencia.
- Agilizar el proceso de documentación.
- Optimizar el manejo de información.
- Facilitar el mantenimiento y actualización.
- Brindar seguridad a la información.

Para el desarrollo del Plan fueron necesarias una serie de actividades las cuales se dividieron en las siguientes etapas:

1.- Información General de la Empresa en cuestión.
2.- Cuestionarios al Personal Directivo, Gerencial y Operativo.
3.- Análisis de Impacto al Negocio
4.- Alcance y objetivos del Plan de Recuperación de Desastres.
5.- Estructura de Comités.
6.- Determinación de Soporte Alterno.
7.- Seguridad Física.
8.- Seguridad Lógica.
9.- Logística del Plan de Recuperación.
10.- Plan de Pruebas.
11.- Procedimientos de Rehabilitación en Site Primario.

1.- Información General de la Empresa en cuestión.

GRUPO GALAXY MEXICANA, (DIRECTV™**)**, líder en servicios de comunicación y de entretenimiento vía satélite en México, ha mostrado en los últimos años un aprovechamiento importante de su infraestructura tecnología, incrementando fuertemente sus operaciones diarias.

Ante este hecho, DIRECTV™ no ha dudado en proteger sus operaciones más importantes así como los servicios de computo mas críticos, minimizando así el riesgo de una interrupción no programada de sus operaciones ocasionada por la ocurrencia de una contingencia.

Dado que cualquier interrupción podría inclusive afectar el cumplimiento de su operación comercial y causar grandes pérdidas monetarias, se requiere el desarrollo de un Plan de Recuperación de desastres para el área de Tecnología de Información.

Para el desarrollo del plan se formó un equipo especial de trabajo, el cual se encargo de elaborar y vigilar los detalles del plan, con el fin de garantizar el resultado esperado.

Este Plan de Recuperación de desastres es definitivamente el resultado de la aplicación de la metodología propuesta en este trabajo de investigación así como del esfuerzo conjunto de ideas y experiencias que ayudaron a enriquecer dicha metodología.

2.- Cuestionarios al Personal Directivo, Gerencial y Operativo.

Esta etapa de estudio, tuvo como objetivo conocer las necesidades particulares de cada una de las áreas, funciones y procesos críticos que, al no contar con una continuidad darían como resultados impactos negativos que afectarían considerablemente la operación de la empresa.

Se realizaron una serie de entrevistas con los gerentes de área y a los usuarios de los sistemas críticos a fin de identificar las aplicaciones mas criticas y así definir el alcance del Plan de Recuperación en conjunto con el personal Directivo de la compañía.

El resultado de esta serie de entrevistas se menciona en el siguiente punto.

3.- Análisis de Impacto en el negocio (Business Impact Análisis).

El BIA provee la base para las prioridades de planeación de la recuperación, así como de la selección de estrategias de recuperación que reflejen un balance óptimo entre las inversiones por la planeación de la recuperación, los riesgos y exposiciones potenciales.

El objetivo principal del BIA es proveer un análisis de los costos asociados con la interrupción de las operaciones en el centro de operación de DIRECTV.

Las actividades para lograr el análisis de Impacto en el Negocio son:

- Identificar las áreas que soportan las funciones críticas de la compañía.
- Identificar las funciones críticas del negocio.
- Detectar y clasificar las aplicaciones automatizadas.
- Estimar el impacto económico y operacional de un desastre en el centro de operación de DIRECTV™.

3.1 Áreas criticas específicamente de Directv™.

Atención a Clientes. El principal impacto en esta área se refleja en la calidad del servicio originado por no tener datos en línea, además de tener un impacto económico debido a la perdida de oportunidad de la actualización en línea de los datos de los subscriptores como domicilio actual, cambio de forma de pago, etc.

Esta área es de vital importancia para la compañía ya que es la encargada de satisfacer las necesidades de los suscriptores, además de ser el vinculo entre DIRECTV™ y los suscriptores.

Crédito y Cobranza. Esta área contempla el proceso de Recuperación de Cartera, el cual consiste en la programación de llamadas para recuperar saldos vencidos por clientes que no han cubierto sus adeudos, así como gestionar sus saldos.

Basados en el reporte de Recuperación de Cartera acumulado a Junio de 2003 el número de llamadas que realiza este centro de atención, es de aproximadamente 19,500 llamadas promedio por mes (Datos reales de Enero a Junio de 2003), lo que significa un promedio aproximado de 651 llamadas diarias. Si determinamos el número de llamadas por hora obtenemos un promedio aproximado de 47 llamadas.

Ventas y Activaciones. Es el área encargada de fortalecer los puntos de venta distribuidos en el territorio nacional, es el vinculo entre vendedores y DIRECTV™, su objetivo es el posicionamiento de la marca en el mercado.

En este proceso se registran todas las activaciones de nuevos subscriptores del servicio de DIRECTV por lo que representa la principal fuente de incremento en la participación de mercado de la empresa.

Basados en el reporte de Activaciones a Junio de 2003, el número de llamadas que realiza este centro de atención es de aproximadamente 8,000 llamadas promedio por mes (Datos reales de Enero a Junio de 2003), lo que significa un promedio aproximado de 269 llamadas diarias. Si determinamos el número de llamadas por hora obtenemos un promedio aproximado de 19 llamadas.

Distribución y Logística. Es el área encargada de la importación, distribución, control de inventario, instalación y reparación de equipos receptores.

Sistemas. Es el área encargada de suministrar la infraestructura tecnológica para soportar la operación de la compañía.

Broadcast Center. Área encargada de la recepción vía satélite de señales de los canales de programación, por sus necesidades de operación necesita la comunicación con las oficinas centrales de DIRECTV™

Una vez identificadas las áreas criticas dentro de DIRECTV ™, se procedió a identificar los procesos y aplicaciones de mas alto riesgo por su naturaleza y por su relación con otros.

ANALISIS DE IMPACTO EN EL NEGOCIO DIRECTV™

Área	Proceso	Aplicación Critica
Atención a Clientes	Activación de programación	**I B S**
	Atención de problemas técnicos	
	Explicación de saldos y ajustes	
	Disminución o Aumentos en paquetes de programación	
	Información y venta de pagos por eventos (PPV)	
	Gestión de cancelaciones	
	Información general	
	Venta del servicio	
	Aplicación de pagos	
Crédito y Cobranza	Recuperación de cartera	
	Facturación	
	Administración de Cuentas (Métodos de Pago)	
	Gestión de archivos bancarios	
	Desconexiones	
	Cancelaciones	
	Suspensiones	
Ventas	Administración de pagos de comisiones	
	Administración de vendedores	
	Capturas de nuevos suscriptores	
	Configuración de Campañas de venta	
Distribución	Requisición de Equipo	
	Activaciones	
	Gestión y Administración de equipos receptores	
	Administración de ordenes de servicio	
Información y Tecnología	Administración de acceso a usuarios al sistema IBS	
	Configuración y mantenimiento del sistema IBS	
	Administración y Mantenimiento de la Base De Datos de IBS	
	Administración de equipo de comunicaciones	
Brodcast Center	Recepción de señales vía satélite de los canales de programación	
	Gestión de información recibida vía MODEM de los equipos receptores (PPV)	
	Administración de equipos de Comunicación	

Por este motivo se analizo el nivel de impacto negativo que sufriría la organización si no se contara con dichas funciones, descritas en la tabla anterior.

De acuerdo a la metodología propuesta en este trabajo de investigación se deberán clasificar los procesos de negocio en función de los impactos que se enlistan a continuación:

- Impacto Operacional.
- Impacto Legal y Fiscal.
- Impacto de Imagen.
- Impacto de pérdida del negocio.
- Impacto Económico.

3.2 Calificación del grado de Criticidad de los Procesos.

De acuerdo a lo que se menciono en el capítulo 4.2 referente a la calificación que se le deberá asignar a las aplicaciones de acuerdo a su factor de criticidad. Clasificándolos en base a los siguientes criterios

3 Crítica.
2 Vital.
1 Sensibles.
0 No críticas.

La alta dirección en conjunto con los gerentes de área de DIRECTV ™ definieron el factor en porcentaje de los impactos operacional, económico, legal, de pérdida del negocio e imagen. Además este mismo equipo calificó el grado el grado de importancia de los procesos de acuerdo a los procesos de negocio.

Esta decisión es importante ya que es aquí en donde se determina el impacto de las aplicaciones así como el alcance del Plan de Recuperación.

De acuerdo a lo mencionado anteriormente se obtuvieron los siguientes resultados:

Factor (%)	20	10	40	10	20	100
Proceso	Operativo	Imagen	Económico	Legal Fiscal	Pérdida del Negocio	Valor Total
Activaciones	3	3	3	2	3	2.90
Atención de problemas técnicos.	3	2	3	2	2	2.6
Explicación de saldos y ajustes	2	2	1	1	1	1.3
Gestión de cancelaciones	2	2	1	1	1	1.3
Información general	2	2	2	1	1	1.7
Ventas	3	3	3	2	3	2.9
Recuperación de cartera	2	2	3	1	2	2.3
Facturación	3	2	3	2	3	2.8
Administración de Cuentas (Métodos de Pago)	2	1	2	1	2	1.8
Gestión de archivos bancarios	3	2	3	1	2	2.5
Desconexiones	2	1	2	1	1	1.6
Cancelaciones	2	1	2	2	1	1.7
Suspensiones	2	1	2	1	1	1.8
Administración de pagos de comisiones	3	2	3	1	2	2.5
Administración de vendedores	2	1	1	1	2	1.4
Capturas de nuevos suscriptores	3	2	3	1	3	2.7
Configuración de Campañas de venta	3	1	2	1	2	2
(Importación de Equipo)	2	1	3	2	2	2.3
Gestión y Administración de equipos receptores	3	2	3	2	2	2.6
Administración de ordenes de servicio	3	2	2	2	2	2.4
Administración de acceso a usuarios al sistema IBS	2	1	1	0	1	1.1
Configuración y mantenimiento del sistema IBS	3	3	3	3	3	3
Administración y Mantenimiento de la Base De Datos de IBS	3	3	3	2	3	2.9
Administración de equipo de comunicaciones	3	2	3	2	3	2.8
Recepción de señales vía satélite de los canales de programación	3	3	3	2	3	2.9
Gestión de Información recibida vía MODEM de los receptores (PPV)	3	2	3	1	2	2.5

Fórmula:

$$\textbf{Valor Total} = \frac{\sum \textbf{Grado de Criticidad (Factor)}}{\textbf{100}}$$

Ejemplo:

Valor Total Activaciones = 3(.20) + 3(.10) + 4(.30) + 2(.10) + 3(.20)

Valor Total Activaciones = **2.90**

Criticidad de los Procesos de Negocio Directv ™.

Nombre del Proceso	Grado de Criticidad
Configuración y mantenimiento del sistema IBS	3
Administración y Mantenimiento de la Base De Datos de IBS	2.9
Activaciones	2.9
Ventas	2.9
Recepción de señales vía satélite de los canales de programación	2.9
Facturación	2.8
Administración de equipo de comunicaciones	2.8
Capturas de nuevos suscriptores	2.7
Atención de problemas técnicos	2.6
Gestión y Administración de equipos receptores	2.6
Gestión de Información recibida vía MODEM de los receptores (PPV)	2.5
Administración de pagos de comisiones	2.5
Gestión de archivos bancarios	2.5
Administración de ordenes de servicio	2.4
Recuperación de cartera	2.3
Importación de Equipo	2.3
Configuración de Campañas de venta	2.0
Suspensiones	1.8
Administración de Cuentas (Métodos de Pago)	1.8
Información General	1.7
Cancelaciones	1.7
Desconexiones	1.6
Administración de vendedores	1.4
Explicación de saldos y ajustes	1.3
Gestión de cancelaciones	1.3
Administración de acceso a usuarios al sistema IBS	1.1

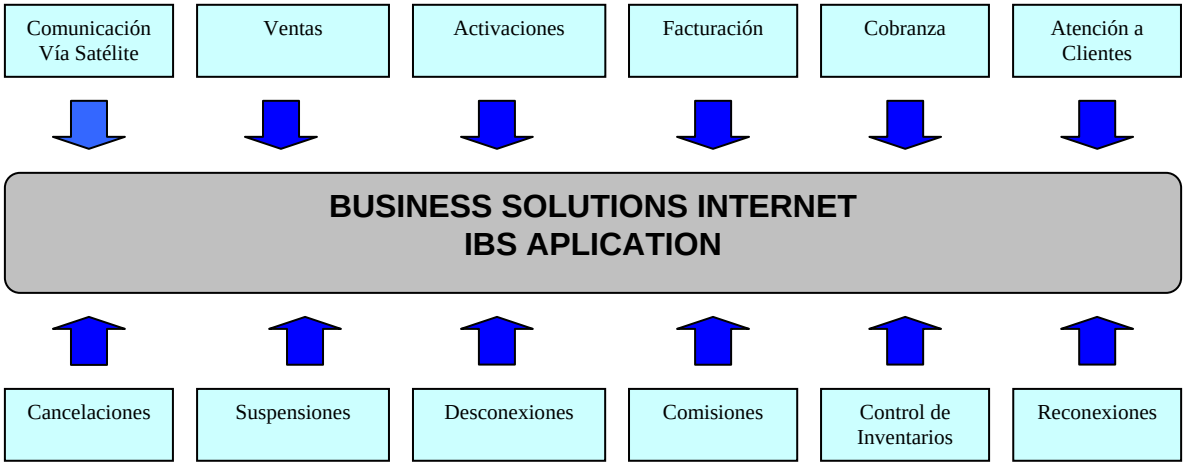
Dada la información anterior podemos observar que si estos procesos no estuvieran disponibles por una falla en el sistema ocasionaría grandes impactos como operacionales, económicos, legales y en general un impacto en la pérdida del negocio. Además podemos observar que en todos los procesos críticos interviene la aplicación IBS.

El proceso de más impacto es la configuración y mantenimiento del sistema IBS. Dicho sistema es el mas critico ya que provee de la facturación de los clientes, es el encargado de enviar los comandos de activación de nuevos canales de TV vía satélite, además de ser el sistema CRM (Customer Relationship Managment de DIRECTV™).

Sistema IBS

La alta dirección así como los gerentes de área conocen que la aplicación crítica para la compañía es el sistema IBS. Este sistema es de origen Holandés creado por la empresa Mindport es un sistema especialmente diseñado para compañías proveedoras de servicio de TV vía satélite.

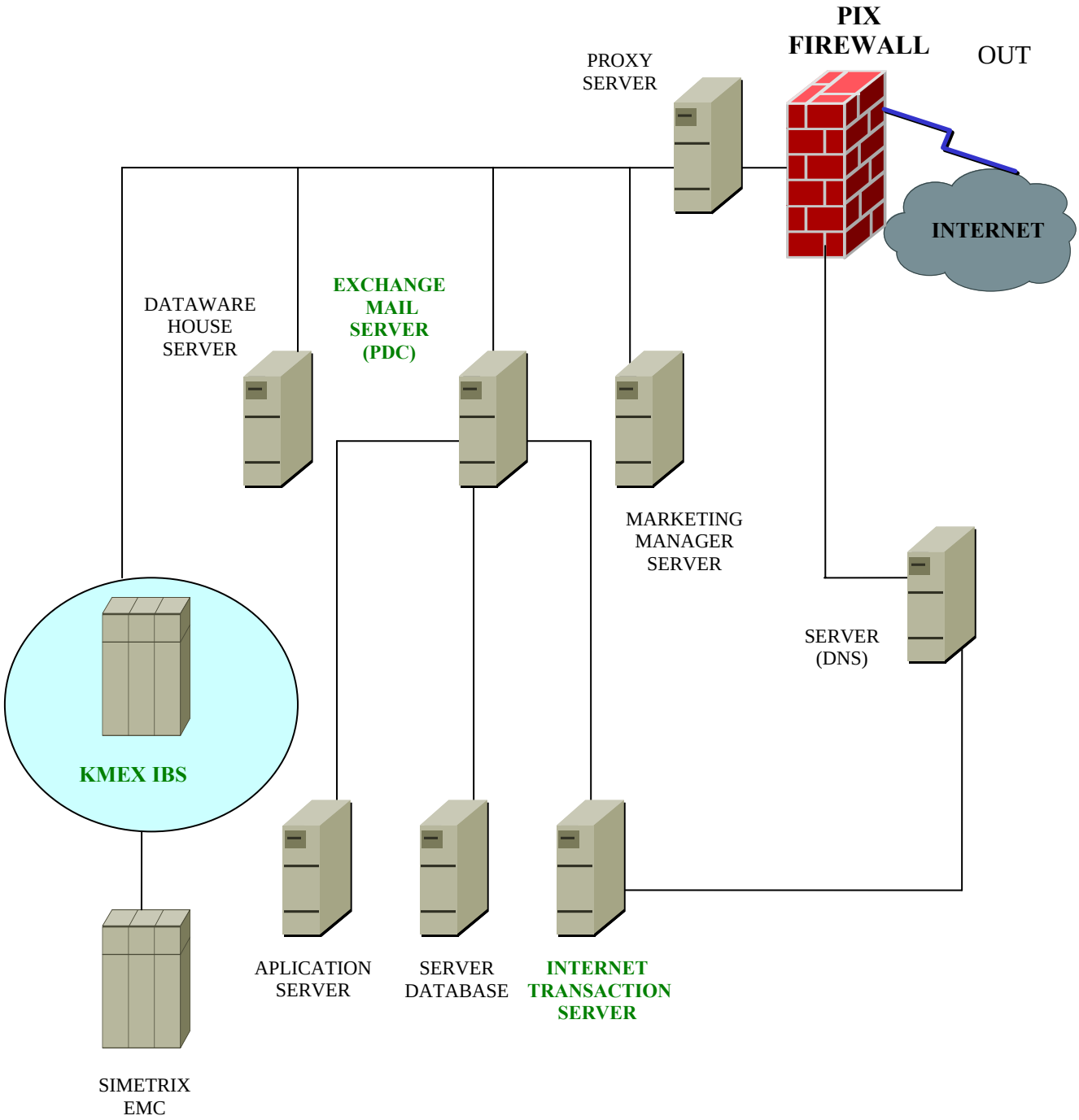
A continuación se presenta un diagrama para observar la relación de procesos de negocio vs el sistema IBS de DIRECTV™



Debido a que este sistema es el más critico de la compañía el alcance del Plan de Recuperación de Desastres esta basado en la disponibilidad de este sistema.

3.3 Infraestructura Tecnológica Actual

A continuación se muestra un diagrama en el cual se muestra como están integrados los servidores de impacto en el centro de operación de DIRECTV™



En el diagrama anterior, se muestran los servidores que son críticos para la compañía, no obstante este trabajo se enfocara al Plan de Recuperación de Desastes del sistema IBS, ya que como se menciono en puntos anteriores resulta ser el sistema más critico de la empresa.

4.- Alcance y Objetivos del Plan de Recuperación de Desastres.

Los objetivos del Plan de Recuperación de Desastres, están enfocados a prevenir y corregir la interrupción de las aplicaciones que más impacto tienen para el negocio.

Definición del Alcance del Plan de Recuperación de Desastres para Directv™

Dado el análisis de los puntos anteriores en este punto se debe de definir el alcance del Plan de Recuperación.

El comité Directivo, en conjunto con el de Sistemas y el Operativo definieron que el objetivo principal del Plan de Recuperación de Desastres (DRP), es por lo tanto, la recuperación de la aplicación IBS después de que un desastre ha sido declarado.

Directv™ ha establecido que las funciones soportadas por la aplicación IBS son críticas para la operación del negocio por lo que desde un principio se determino la aplicación IBS como la única critica.

Así como también el objetivo de este Plan esta concebido exclusivamente para el área de Tecnología de Información.

Para un mejor entendimiento del alcance del Plan de Recuperación de Desastres diseñado para **GRUPO GALAXY MEXICANA, (Directv™)**, es necesaria una breve descripción de sus centros de operación.

TELETECH

Este centro de operación es una empresa de outsourcing la cual es contratada por Directv™, para su centro de atención al cliente, en ella se llevan a cabo funciones criticas y especificas relacionadas a operaciones con los clientes, además de ser el punto de contacto entre DIRECTV™ y el cliente o suscriptor.

CENTRO DE TRANSMISIONES TELEPUERTO

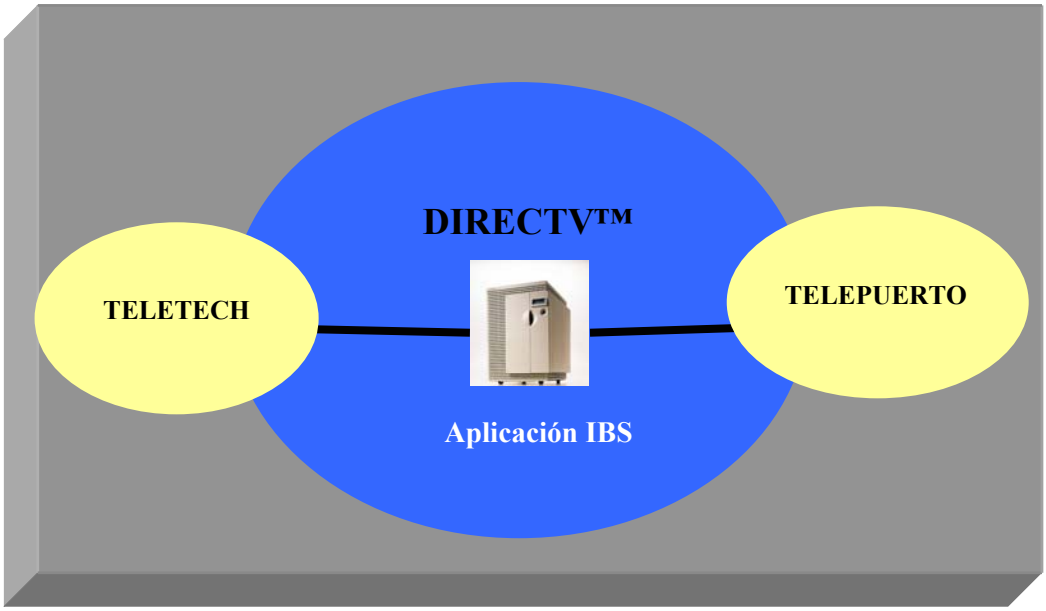
En este centro operacional radica la funcionalidad de la empresa, en ella se llevan a cabo los procesos de recepción de señales para su transmisión a los decodificadores de los subscriptores, además de ser en ese lugar en donde se concentra la información que los decodificadores transmiten referente a sus compras de pagos por evento.

OFICINAS CENTRALES DIRECTV™

En estas oficinas se encuentran las siguientes áreas administrativas siguientes:

- Distribución y Logística
- Ventas
- Compras
- Recursos Humanos
- Finanzas
- Sistemas
- Mercadotecnia
- Finanzas
- Crédito y Cobranza
- Departamento Legal

Estructura Operacional Actual DIRECTV ™

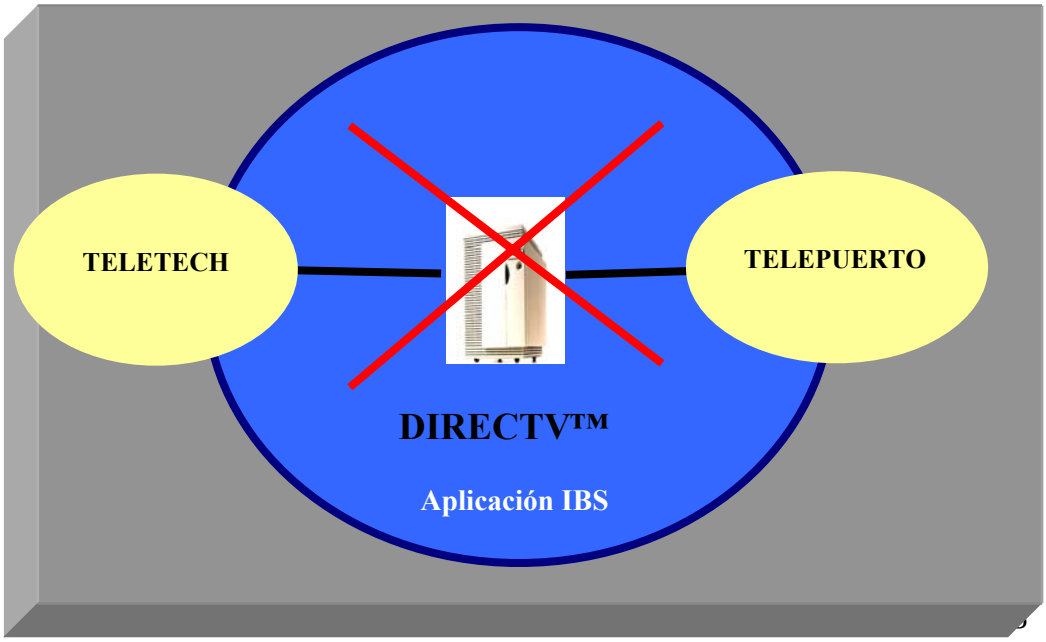


Como se observa en el diagrama anterior las oficinas de Teletech que es el centro de atención a clientes debe tener comunicación hacia las oficinas centrales de Directv™, para hacer uso de la aplicación IBS.

Por otro lado en las oficinas de Directv ™ reside la base de datos de la aplicación IBS, y es aquí en donde se lleva el procesamiento de información de las áreas administrativas.

Las oficinas de Telepuerto necesitan tener comunicación de tipo full dúplex hacia las oficinas centrales de Directv ™, con el objetivo de hacer uso de la aplicación IBS.

Escenario de Desastre de DIRECTV ™

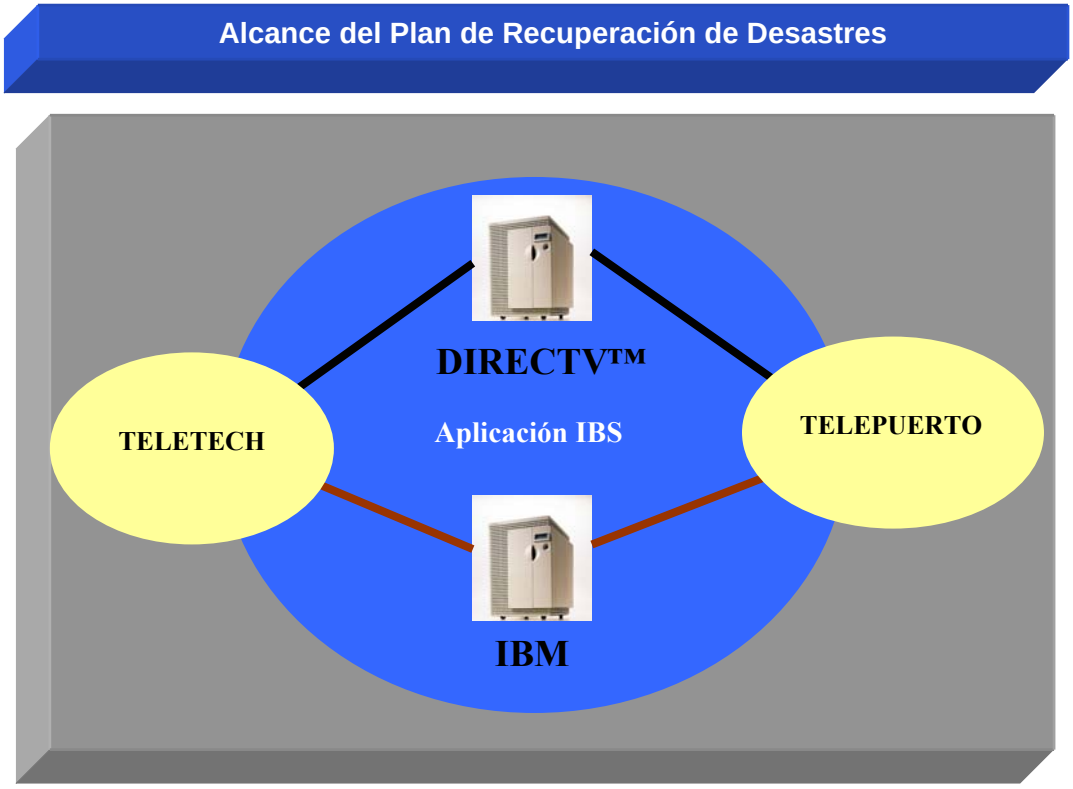


4.1 Identificación de Riesgo.

Se identifico que el punto de alto riesgo son las oficinas centrales de **DIRECTV™,** ya que es aquí donde se lleva el centro de procesamiento de información, además de ser el punto de comunicación entre los 2 centros operativos importantes para el negocio de esta empresa. En el esquema anterior se muestra la situación no deseada y por la cual este Plan de Recuperación tiene a bien cubrir.

4.2 Alcance del Plan de Recuperación de Desastres.

Este plan de recuperación de desastres esta desarrollado para cubrir el alcance que muestra el siguiente diagrama:



Como resultado de este análisis, la estrategia de recuperación ha sido identificada y se espera que reduzca el impacto en la continuidad de las operaciones de DIRECTV™ en caso de desastre.

4.3 Objetivos del Plan de Recuperación

1) Restaurar el sistema IBS y la recuperar sus datos.
2) Recuperar el centro de computo principal de DIRECTV™, ubicado en Blvd. Manuel Ávila Camacho No. 1-101, edificio “INVERLAT”, Piso 1, Colonia Lomas de Chapultepec, México DF.
3) Utilizar el centro operativo de respaldo de IBM en modalidad de Hotsite, ubicado en Calzada Legaria 853 Col. Irrigación en México DF. Delegación Miguel Hidalgo.
4) Recuperar los enlaces de comunicación de DIRECTV™ con TELETECH y TELEPUERTO, con líneas de respaldo independientes entre IBM y TELETECH e IBM y TELEPUERTO.
5) Designar a la gente para la logística y operación del plan de la recuperación.

5.- Estructura de Comités.

A continuación se mencionan las actividades que tendrán a bien cubrir los participantes en el desarrollo del Plan de Recuperación:

- Administrar el Plan.
- Coordinar de la Recuperación.
- Comunicar el estado de la situación con el Exterior.
- Reconfigurar los Equipos.
- Recuperar las Operaciones.
- Restaurar las Comunicaciones.
- Administrar los equipos personales.
- Apoyar e Interactuar con los Usuarios de los sistemas automatizados.

El correcto funcionamiento del Plan de Recuperación de Desastres, requiere de la oportuna participación de todas sus partes. El equipo DRP, líderes y miembros, junto con otros participantes, deben conocer bien su papel y responsabilidad en el plan. Su tarea deberá ser ejecutada con ejemplar dominio y exactitud, para garantizar el éxito del plan.

El procedimiento para la distribución del plan debe informar de dicho plan a los equipos participantes y al resto de la organización. La adecuada distribución y promoción del plan determinarán finalmente el éxito, es por ello indispensable, que el líder de cada uno de los equipos debe asegurarse de que todo su equipo, esté perfectamente enterado de la visión global del plan, de su papel y de la responsabilidad que se le esta encomendando.

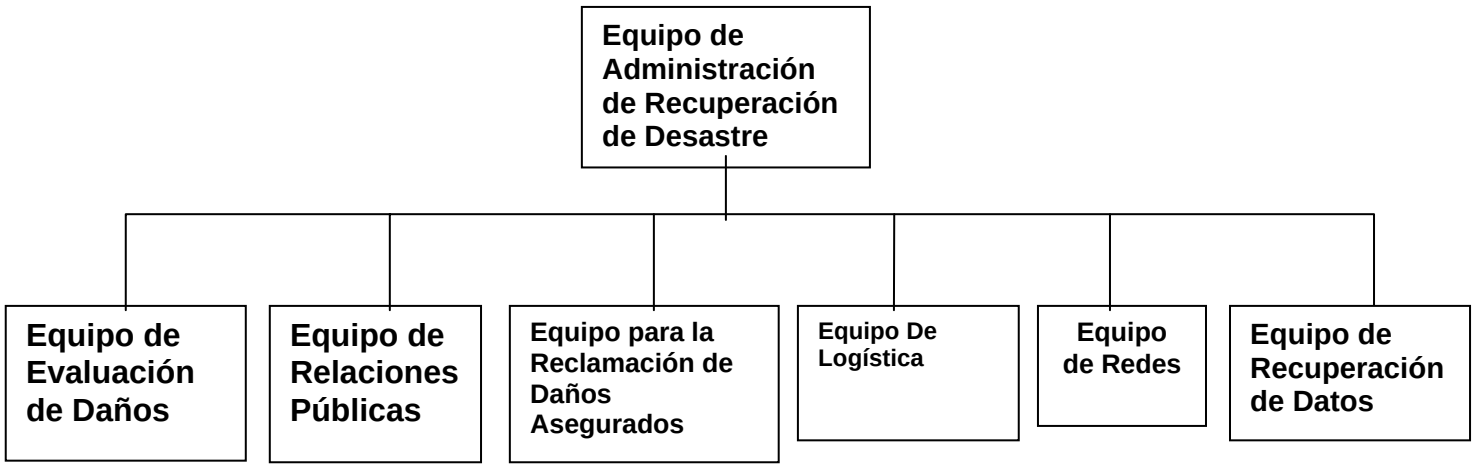
5.1 Estructura de comités de seguridad para Directv™.

Organización en la recuperación de desastres Centro de Procesamiento de datos de DIRECTV ™

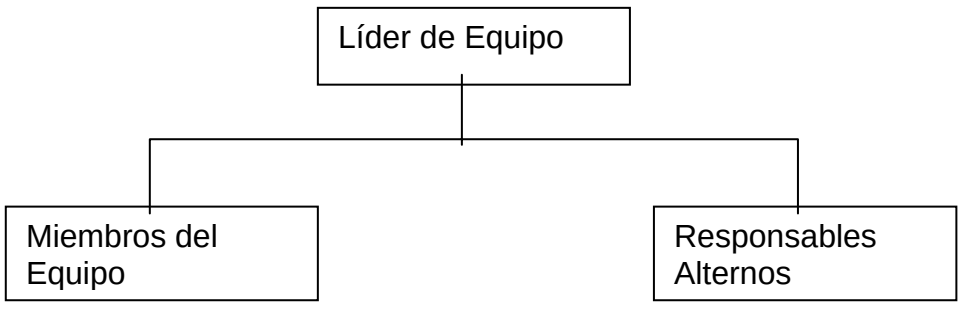
Objetivos

Definir las responsabilidades, y deberes de los miembros cada uno de los equipos de Recuperación del Plan de Recuperación de Desastres.

Estructura organizacional



A su vez para cada Equipo de Recuperación se debe cumplir la siguiente estructura:



Perfil de los integrantes de los Equipos de Recuperación

Líder de equipo:

El líder deberá estar totalmente familiarizado con todo el DRP, formar un equipo de apoyo con los miembros más adecuados de acuerdo a la experiencia y desarrollo de cada uno, entrenar constantemente al equipo en la ejecución del plan y mantener siempre actualizada y al alcance de todos, una lista con todos los datos generales, necesarios para la localización oportuna del equipo.

Miembros del equipo:

Son todos aquellos individuos que participan directamente en la ejecución del DRP. Tienen la responsabilidad de ejecutar una tarea especifica, de acuerdo al plan, y de hacerlo en el momento exacto, es decir, ajustar su intervención a la sincronía propia del plan, indicada por el líder, con el fin no actuar a destiempo en comparación con el resto del equipo.

Responsables alternos:

Para cada miembro del equipo, incluyendo al líder, se debe buscar un sustituto que tome la responsabilidad de asumir la función que resulte vacante por ausencia o incapacidad. La recomendación en este sentido, es “rolar” a los miembros del equipo durante los entrenamientos y pruebas, en todas y cada una de las actividades y responsabilidades, de manera que, al estar familiarizado, mantengan un buen control sobre la función heredada, en caso de requerir su participación al presentarse un desastre.

Nuevos miembros:

Toda persona, que por su función o actividad deba agregarse al equipo, será sometida a entrenamiento y evaluación, por parte del líder del equipo, que entregará copia del plan. Una vez autorizada y firmada su colaboración, será identificada y reconocida por todo el equipo, para su participación en el plan.

5.2 Descripción de los equipos de DRP.

Los equipos de recuperación de desastre se han identificado para administrar y desempeñar todas las operaciones de recuperación de desastre. Los equipos siguientes dirigirán el proceso de recuperación y apoyaran para la ejecución del Plan de Recuperación:

Equipo de Administración de Recuperación de Desastre:

Responsabilidad

El equipo de Recuperación de Desastre es responsable de la administración y control global de las operaciones de Recuperación de Desastre que comienzan con evaluar el daño y termina hasta que el sistema de cómputo esté operando normalmente y los empleados hayan recuperado totalmente las operaciones normales de negocio.

El equipo de Administración de Recuperación de Desastre se compone de un líder de equipo y un líder de cada uno de los otros equipos de recuperación.

Autorizar los gastos necesarios de la puesta en marcha del Plan de Recuperación. El objetivo preciso de este equipo es la restauración del centro operativo principal.

El equipo Administrativo de Recuperación de Desastre también será responsable de dar la notificación inicial a los equipos de usuarios (tanto el grupo clave como a los usuarios que no constituyan parte del grupo clave) así como la constante comunicación durante el proceso de recuperación de las operaciones.

En este caso nuestro Equipo de Administración de Recuperación de Desastre esta formado por la alta Dirección, y el Director de Sistemas, como suplente se encuentra el Subdirector de Sistemas.

Equipo de evaluación de daños:

Responsabilidad:

El equipo de Evaluación de Daños será responsable de complementar los informes de evaluación de daños. Su responsabilidad incluye determinar:

- La condición del Site de operaciones de Directv™, a través de complementar un informe preliminar de la situación una vez que se ha declarado una contingencia;

- La magnitud del daño a la máquina en donde reside la base de datos de IBS y los sistemas de la red afectados por el desastre, a través del llenado de una lista de comprobación de evaluación de daños.

- El estado del procesamiento al momento del desastre a través de la identificación de documentación que se haya podido rescatar.

- La condición del equipo y las facilidades de oficina, evaluar el alcance inicial de daños.

- Un informe completo, preciso y rápido de la situación del desastre.

Equipo de Redes y Comunicaciones:

La importancia de este equipo de recuperación es alta ya que como lo mencionamos en el objetivo de este Plan de Recuperación resulta fundamental contar con la comunicación entre los centros operativo de Directv ™ (Oficinas en Directv ™), (Operaciones Telepuerto) y (Atención a Clientes Teletech)

Responsabilidad

Coordinar con el centro de operaciones de Teletech y Telepuerto el direccionamiento de los servicios de red hacía el centro alterno de IBM.

Equipo Logística:

El Equipo de Logística es responsable de todos los asuntos administrativos tales como:

- Proveer abastecimiento al Centro de Soporte Alterno como papelería, Mobiliario etc.
- El establecimiento de un fondo de caja chica.
- Notificar al servicio postal de la dirección del Centro de Soporte Alterno.
- Coordinar el acceso a las cintas de respaldo.
- Desempeñar deberes secretariales, tales como notificar al personal cómo comunicarse con el Equipo de Administración de Recuperación de Desastres al Centro de Soporte Alterno y tomar mensajes telefónicos para cada uno de los miembros del Equipo de Recuperación de Desastres;
- Coordinar el transporte y cualquier alojamiento necesario para los miembros del Equipo de Recuperación de Desastre.
- Proveer otros servicios incidentales al Equipo de Administración de Desastre tales como comidas, servicios de fotocopiado y otros deberes administrativos.

Equipo de Relaciones Públicas:

El equipo de Relaciones Públicas es responsable del manejo de la comunicación, a factores externos como prensa, proveedores, etc.

Notificación y Plan de Acción para los socios de Negocio de DIRECTV™

Equipo para la reclamación de Daños Asegurados:

El equipo para la Reclamación de daños es responsable de determinar el alcance del daño, complementar y presentar la reclamación contra la póliza de seguros existente.

Equipo para la Recuperación de Datos:

Responsabilidad:

Este equipo es responsable de recrear la plataforma, así como la restauración del sistema IBS en las ubicaciones alternas. Además son responsables de la seguridad de la información así como del hardware transportados del centro de operaciones central de DIRECTV™ a las instalaciones alternas.

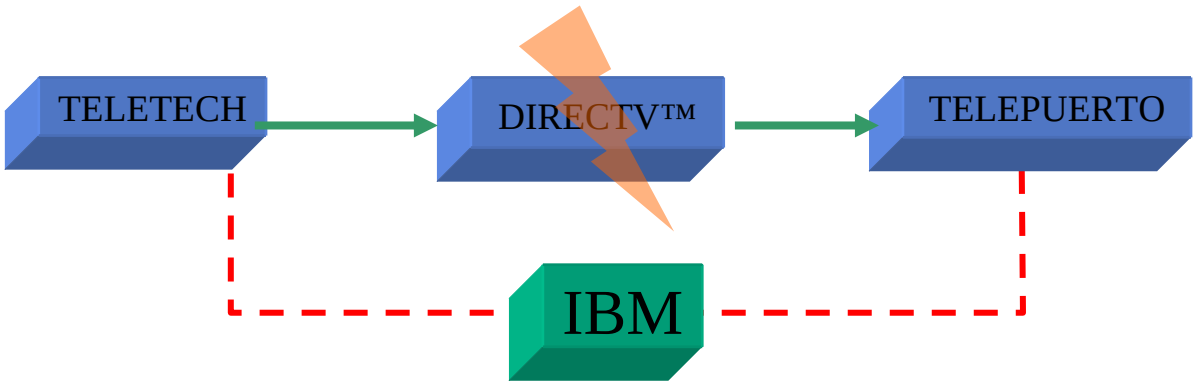
Recuperar los datos de los sitios de almacenamiento, acudir al centro operativo de respaldo, recuperar el servidor de respaldo (Sistema operativo, manejador de base de datos, magic e **IBS**) y actualizar los datos del último respaldo disponible.

6.- Determinación de Centro de Soporte Alterno.

Como se ha observado es de suma importancia la implantación de un Plan de Recuperación de Desastres que contemple la disponibilidad del sistema IBS que se encuentra ubicado en el centro de operaciones de Directv™, ya que sus centros de operación deben de estar comunicados de manera permanente dadas las características propias de negocio.

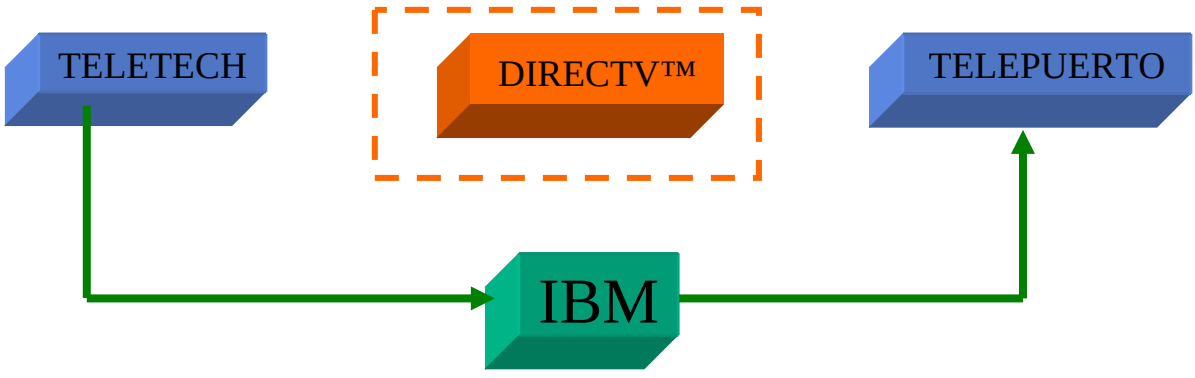
De esta manera fue necesaria la implementación de un centro de soporte alterno el cual tiene como objetivo ser el centro de operación de emergencia entre:

TELETECH - DIRECTV™ - TELEPUERTO.



Se tomo la decisión de tener una maquina en la modalidad de HOTSITE, con características similares al servidor KMEX de Producción.

Escenario de Recuperación de Comunicaciones



6.1 Requisitos Contractuales.

Es responsabilidad del Equipo de Administración del Plan de Recuperación de Desastres, definir las características del centro de soporte alterno de tal manera que cumpla con la infraestructura tecnológica para qué soporte los alcances del Plan, en este caso se definió que el centro de soporte alterno debería cumplir los siguientes puntos

- Un Servidor HP 9000 K460 con 756 Mb. de memoria RAM y 35Gb. en disco duro.
- Unidad de cinta 8 mm.
- Impresora 3930
- Dos líneas conmutadas, dos tarjetas de red.
- Un MODEM dinámico
- Cinco Computadoras Personales
- Cinco Lugares de oficina
- Soporte operativo para montaje de cartuchos, cintas y papelería
- Acceso a fax y copiadora

Este plan de recuperación de desastres funciona bajo las siguientes condiciones:

a) Cuando el perímetro de desastre afecte únicamente la operación el centro de computo en Directv™, y no afecte la operación normal de los centros IBM, Teletech y Telepuerto.

b) Cuando el desastre no impida al equipo de gente encargado de la recuperación de desastres de Directv ™ estar disponible para ejecutar el plan.

c) Cuando el personal de sistemas que conforma los equipos de recuperación de desastres pueda recopilar las cintas de respaldo almacenadas en Teletech y las cintas se encuentren en buen estado.

d) Cuando los sistemas y aplicaciones sean compatibles con el año 2000.

e) Cuando los enlaces de comunicación de respaldo entre IBM y Telepuerto, e IBM y Teletech operen normalmente.

6.2 Lista de vulnerabilidades y amenazas.

Basados en los supuestos anteriores las vulnerabilidades y amenazas que contempla este Plan son las siguientes:

CONTEMPLA
♦ Rayos y/o truenos ♦ Huelgas y/o paros sindicales (que afecten el edificio o instalaciones de Directv™) ♦ Interrupciones de suministro eléctrico (que afecten el edificio o instalaciones de Directv™) ♦ Choque de aeronave cerca o en el edificio. ♦ Amenaza de bomba o explosivo (que afecten el edificio o instalaciones de Directv ™) ♦ Derrame y/o fuga de químicos ♦ Desalojo sorpresivo de edificios u oficinas ♦ Robo de equipo (Robo del servidor Kmex) ♦ Disturbios sociales y/o manifestaciones (que afecten el edificio o instalaciones de Directv™) ♦ Fuego y/o Incendio ♦ Inundaciones (que afecten el edificio o instalaciones de Directv ™) ♦ Fugas de agua ♦ Fuga de gas o material Tóxico ♦ Sabotaje externo (Hackers, ciberterrorismo) ♦ Sabotaje interno de empleados disgustados ♦ Líneas dedicadas defectuosas ♦ Accidentes en construcciones vecinas ♦ Explosión cerca o en el edificio ♦ Fallas en Hardware que el proveedor no pueda resolver en tiempos pactados

Basados en los supuestos anteriores las vulnerabilidades y amenazas que NO contempla este plan son las siguientes:

NO CONTEMPLA
➢ Epidemias y/o enfermedades (que afecten el edificio o instalaciones de Directv ™) ➢ Nevada / Tormenta de hielo ➢ Sequía ➢ Tormenta de arena ➢ Terremoto ➢ Temperaturas extremas ➢ Hambruna ➢ Huracán ➢ Paro masivo de tráfico ➢ Accidente nuclear ➢ Tornado ➢ Tifón ➢ Erupción volcánica ➢ Derrame de desperdicios

El siguiente listado menciona amenazas, las cuales se esperan sean solucionadas a través de procedimientos normales de operación y no requieren ser incluidos dentro de un Plan de Recuperación de Desastres.

NO CONTEMPLA

➢ Humedad extrema
➢ Error humano
  ➢ Uso indebido de usuarios finales
  ➢ Errores de procedimientos
  ➢ Errores en la programación
  ➢ Utilización de datos erróneos
➢ Disfunción de software.
➢ Virus de software
➢ Acceso no autorizado a los datos
➢ Acceso no autorizado para el manejo del respaldo de datos

7. Seguridad Física.

Resguardo de Información en Caja de Seguridad y Sitio Externo

Los respaldos de los registros vitales son obtenidos diariamente llevando una bitácora de registro en el site de operación, son obtenidos en cintas magnéticas las cuales son resguardadas en una caja de seguridad blindada ubicada en el centro de operaciones de TELETECH.

Actualmente el área de sistemas cuenta con los siguientes sistemas de protección:

- Lector de tarjetas magnéticas y teclado numérico para tener acceso al área de sistemas, ya sea con gafete o con la introducción de una clave personal.

- Teclado numérico para acceder al Site de Directv™.
- Sistema de seguridad contra incendio Gas FM-200.

- Sistema de aire acondicionado, que consiste de 2 contenedores con capacidad (15 tons.c/u).
- Se cuenta con un Generador de planta de emergencia.
- Se cuentan con sistema de energía sin interrupciones.

Los medios son verificados con el proveedor de servicios mínimo 2 veces al año, se lleva bitácora de revisión de medios por parte del proveedor de servicios.

8.-Seguridad Lógica.

La seguridad Lógica implementada por Directv™, esta dividida en las siguientes partes:

Seguridad de Servidores.

Es responsabilidad del administrador de los equipos NT, las siguientes actividades:

Respaldos de los Servidores.

Mantenimiento y Actualización de los Servidores en Producción.

Seguridad en equipos HP-UX Unix.

Administración de Usuarios.

Seguridad y Control de accesos.

Mantenimiento de Servidores HP-UX Unix.

Respaldo del Sistema Operativo Unix.

Respaldar la aplicación IBS.

Seguridad De Base de Datos.

Administración de Usuarios a nivel de Base de Datos.

Respaldo de Software de Informix.

Administración de Perfiles de Usuarios.

Crear procedimientos para monitorear la actividad de la Base de Datos.

Administración del espacio en disco de acuerdo al crecimiento del volumen de la información.

Aplicar políticas de respaldos de la Base de Datos IBS.

Respaldos de los Logs de transacciones de la Base de Datos.

Adicionalmente las cuentas del sistema IBS, se entregan al usuario final de manera personal, y a este se le hace llenar un formato de confidencialidad de la información. Dichas cuentas expiran mensualmente.

Seguridad de Comunicaciones.

Verificar que los accesos sean autorizados de red.

Administración de Usuarios Remotos.

Identificación de Puntos Vulnerables de accesos no autorizados.

Identificación de Transmisión de Datos sobre demanda en la Red Corporativa.

Planeación estratégica del crecimiento de la Red.

Verificar la conectividad entre los centros de operación Teletech-Directv™-Telepuerto.

Seguridad Help Desk.

Creación y la Ejecución de Políticas de Seguridad a nivel usuario.

Los empleados de la organización deberán cambiar su password de acceso a su estación de trabajo en un periodo de 1 mes.

Administración de software autorizado.

Se cuenta con una herramienta llamada Altiris la cual es capaz de detectar software ajeno a la compañía, y una vez detectado es posible desinstalarlo, protegiendo así la información de la compañía.

8.1 Identificación de registros vitales

Los registros vitales de la aplicación IBS son aquellos datos indispensables para la operación, respaldo y recuperación de la aplicación, y son los siguientes:

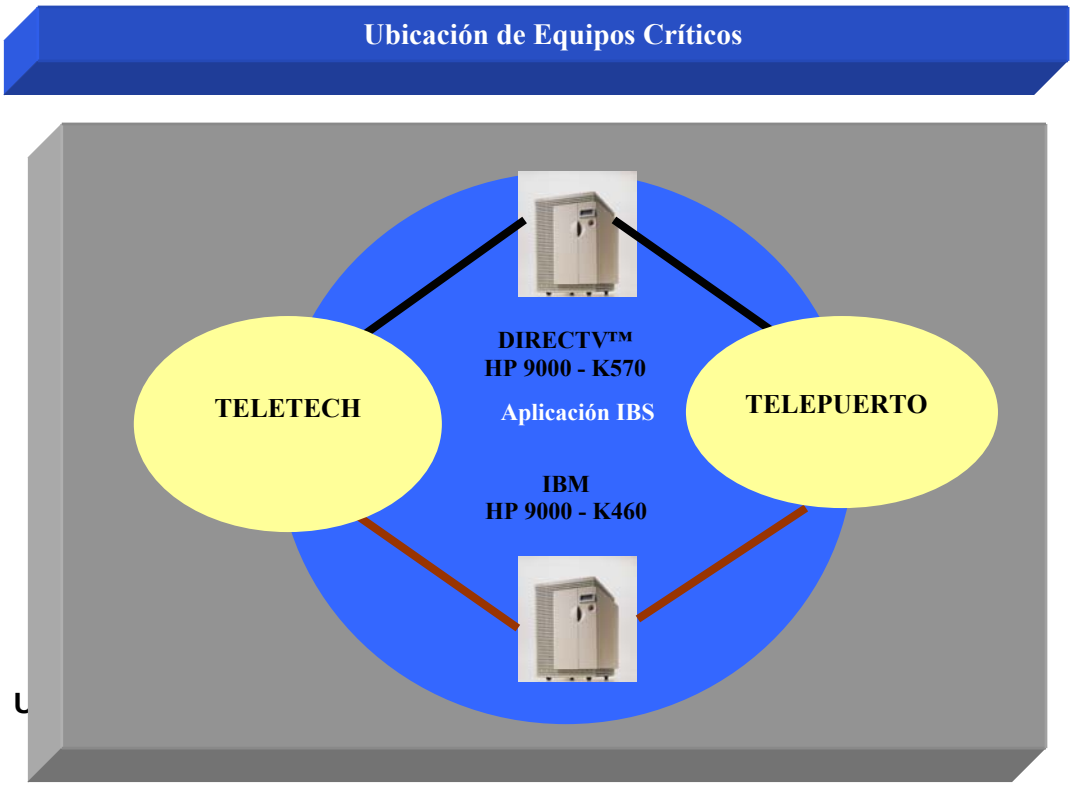
a) Sistema Operativo UNIX HP-UX.

b) Manejador de base de datos INFORMIX.

c) Aplicación IBS.

d) Cintas de Respaldo de la Base de Datos de IBS.

9.2 Hardware y Software Críticos



Equipo	Ubicación
Servidor "kmex" HP 9000-K570	Centro de computo principal: Blvd. Manuel Ávila Camacho # 1-101, 1er Piso
Servidor "Respaldo IBM" HP 9000- K460	IBM: Calzada Legaria # 853, Col. Irrigación. Delegación Miguel Hidalgo. C.P. 11500 México, D.F.

Especificaciones técnicas y de configuración de los equipos principales.

Servidor "Kmex" HP – K570	**IP ADDRESS:**	172.16.XX.XX
	PROCESADORES	4 de 280Mhz
	MEMORIA RAM	3 Gb
	ARREGLO DE DISCOS	75 Gb
Servidor de "Respaldo IBM" HP – K460	**IP ADDRESS:**	172.16.XX.XX
	PROCESADORES	2 de 180 Mhz
	MEMORIA RAM	756 Mb RAM
	ARREGLO DE DISCOS	35 Gb

Especificaciones técnicas y versiones actualizadas de las aplicaciones críticas (IBS).

SOFTWARE	VERSIÓN
UNIX	10.20
INFORMIX	7.31uc3
MAGIC	5.62
IBS	52ª20

8.3 Respaldos de registros vitales.

Se requiere tener almacenados en sitio y fuera de sitio los respaldos de los registros vitales.

Los respaldos que se guardarán en sitio son los siguientes:

- Respaldo de Informix Base de Datos
- Respaldo de HP-UNIX.
- Respaldo de logs de Informix.

Plan de retención de respaldos

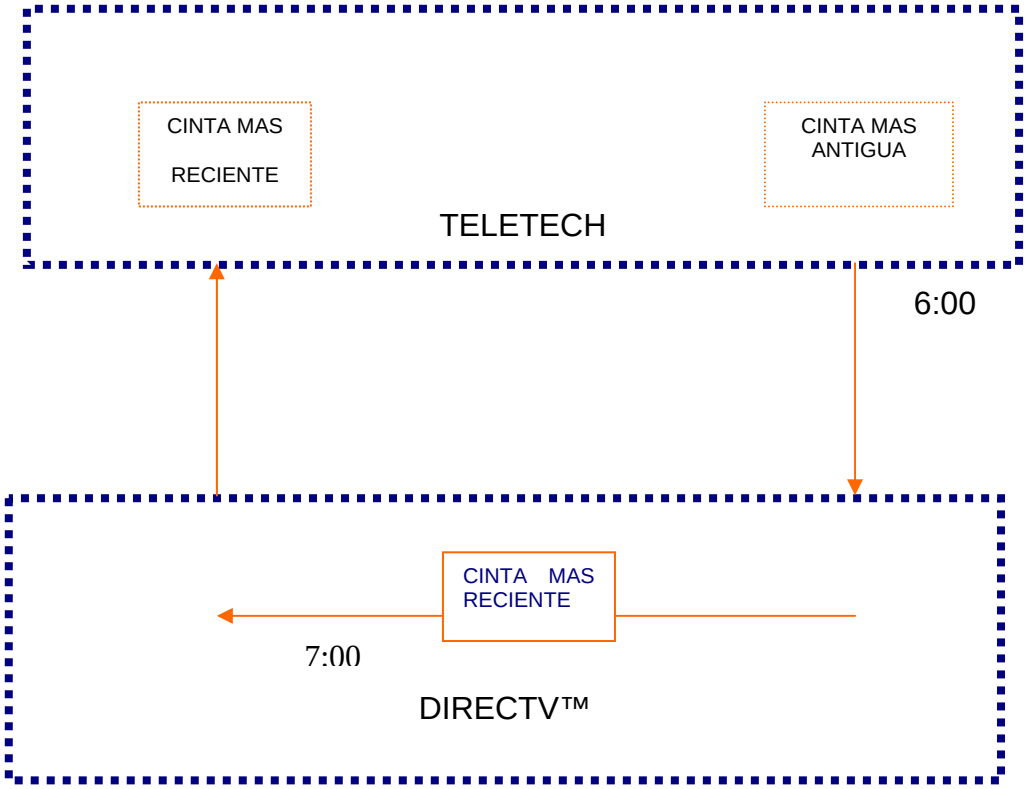
Los respaldos de a nivel de Base de Datos son efectuados diariamente a las 3:00 am, en las oficinas centrales de Directv™

El almacenamiento de estas cintas de respaldo son almacenadas en una caja de seguridad dentro y fuera del centro de operaciones de Directv™ en donde solo el personal autorizado tiene acceso.

Los respaldos fuera del site son almacenados en las oficinas de Teletech.

Logística de Respaldos

Diagrama de rotación de respaldo en Site Alterno.



9.- Logística del Plan de Recuperación de Desastre.

Declaración de Desastre.

La declaración de desastres es el primer aviso formal dirigido a un grupo especifico de personas, informándoles sobre el evento o grupo de eventos que han causado daño considerable en alguna o en todas las aplicaciones críticas del negocio, afectando o poniendo en riesgo su funcionamiento y cuya recuperación requiere de la ejecución inmediata del Plan de Recuperación de Desastres.

En un desastre, se considera que el centro de operaciones principal de Directv™, se encuentra en estado inoperante, y que los medios definidos de comunicación puedan estar seguramente averiados, por lo que es menester, definir un centro de comando, fuera de las instalaciones, desde donde se indique y giren instrucciones precisas de recuperación.

Es conveniente que este centro de comando esté precisamente donde se recupera la operación, es decir, el centro de cómputo de respaldo en IBM.

Dado que es muy probable que la comunicación con los miembros del equipo sea difícil, es necesario que los miembros de los equipos se mantengan en comunicación constante con el equipo de administración en este centro de comando.

La comunicación hacia el centro de comando es muy importante ya que con ello sé esta asegurando la coordinación de las actividades a la par de los demás miembros del equipo.

Se deberá contar con la lista actualizada de direcciones, teléfonos, nombres de contacto etc; de todos los integrantes de los equipos de recuperación de desastres, así como de proveedores.

El almacenamiento de respaldos fuera de sitio se encuentra en Teletech, ubicado en Av. Paseo de la Reforma No. 76 – Piso 2. Col. Juárez, C.P. 06600 en México D.F.

9 .1 Procedimiento a seguir en caso de declaración de Desastre.

Al ocurrir un desastre, es muy importante hacer su declaración siguiendo los pasos definidos para ello, en nuestro caso la secuencia es la que se muestra a continuación.

Paso	Equipo o Responsable	Actividad	Descripción
1	Operador o Vigilante en turno	Notifique desastre	Localice en la lista de contactos los datos del equipo de administración. Intente hasta tener comunicación. Avise el desastre al equipo de administración.
2	Administración	Solicite evaluación de daños	Avise el desastre al equipo de evaluación de daños y solicite al equipo de evaluación diagnostico del desastre en el centro de computo.
3	Recuperación	Evalúe daños	Revise daños del desastre. Reporte al equipo de administración los daños del centro de cómputo. Mencione tiempo estimado de recuperación del centro de cómputo.
4	Administración	Declare o cancele desastre	Localice equipos de recuperación. Declare o cancele declaración de desastre.
*** 5**	Administración	Reúne equipos	Pida a los equipos de recuperación se presenten en centro de comando IBM.
*** 6**	Administración	Declare contingencia en Hot Site IBM.	Avise centro de cómputo de respaldo, notifique desastre. Proporcione nombre de empresa, número de contrato y desastre.
*** 7**	Recuperación	Recopile los respaldos.	Recopile respaldos de sitios de almacenamiento fuera de sitio. Ejecute procedimientos de recopilación de respaldos fuera de sitio.
*** 8**	Redes	Notifique a Teletech.	Avise desastre a Teletech que ejecute plan de Recuperación de red de respaldo.
*** 9**	Redes	Notifique a Telepuerto.	Avise desastre a Telepuerto que ejecute plan de Recuperación de red de respaldo.
*** 10**	Administración	Notifique a Proveedores.	Contacte proveedores y solicite soporte si lo requiere.
11	Administración	Organice centro de comando	Organice centro de comando. Comience estrategia de recuperación.
12	Recuperación	Recupere servidor de respaldo	Recupere servidor de respaldo, si requiere recupere respaldo con aplicaciones. Recupere base de datos más reciente.
13	Recuperación	Notifique a Teletech y Telepuerto	Avise a Teletech y Telepuerto inicio de operación desde sitio de respaldo
14	Recuperación	Inicie operación En sitio de respaldo.	Comience operación de IBS.

Nota:

Las actividades marcadas con el signo (*) son actividades que pueden hacerse en paralelo. Cuando se habla de actividades de equipos, se refiere actividades que deben de ser realizadas por el líder de ese equipo o su suplente.

9.2 Notificación de Desastre.

Pasos para notificar un desastre a medios externos de la compañía:

Paso	Equipo o Responsable	Actividad	Descripción
1	Administración	Notifique a directores	Avise a la Alta Dirección.
2	Relaciones Públicas	Publique Notificación	Prepare publicación a medios de información. Publique en medios de información y prensa el desastre y su recuperación.

9. 3 Procedimientos de Recuperación de Datos.

A continuación se presentan los procedimientos que se deberán de llevar a cabo una vez declarada una contingencia en el centro de operaciones en las oficinas centrales de Directv™

Centro de Operaciones de Directv™

Procedimientos en el Centro de Operaciones DIRECTV™	Descripción
Baja de la Aplicación IBS	Dar de baja los procesos activos del sistema IBS
Baja del manejador de la base de datos INFORMIX	Proporciona la baja de la base de datos de IBS
Apagado físico del equipo HP9000 K570	Procedimiento para el apagado físico

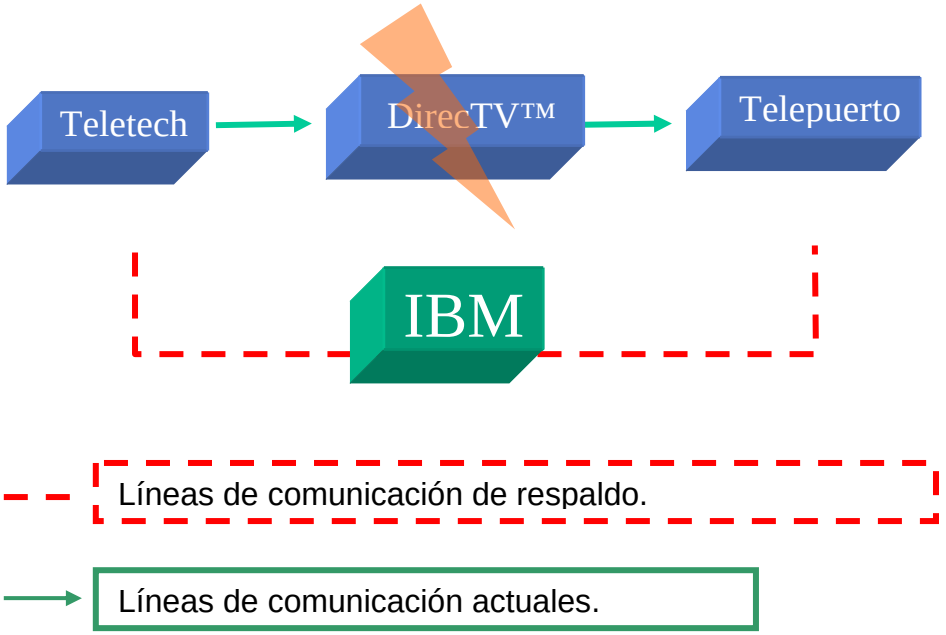
Centro de Soporte Alterno

Procedimientos en el Centro de Soporte Alterno (IBM™)	Descripción
Encendido físico del equipo HP 9000- K460	Proporciona las tareas a realizar para el encendido del equipo
Alta del manejador de la base de datos INFORMIX	Genera el ambiente para la base de datos de la aplicación IBS
Restauración de cintas de Respaldo	Restaura las cintas de respaldo
Alta de la Aplicación IBS	Iniciar los procesos del sistema IBS

9.4 Procedimientos de Restauración de Comunicaciones.

Teletech y Telepuerto respectivamente, cuentan con enlaces de comunicación de respaldo hacía el centro de computo de respaldo en IBM. Estos enlaces deberán utilizarse en lugar de los enlaces normales en caso de desastre.

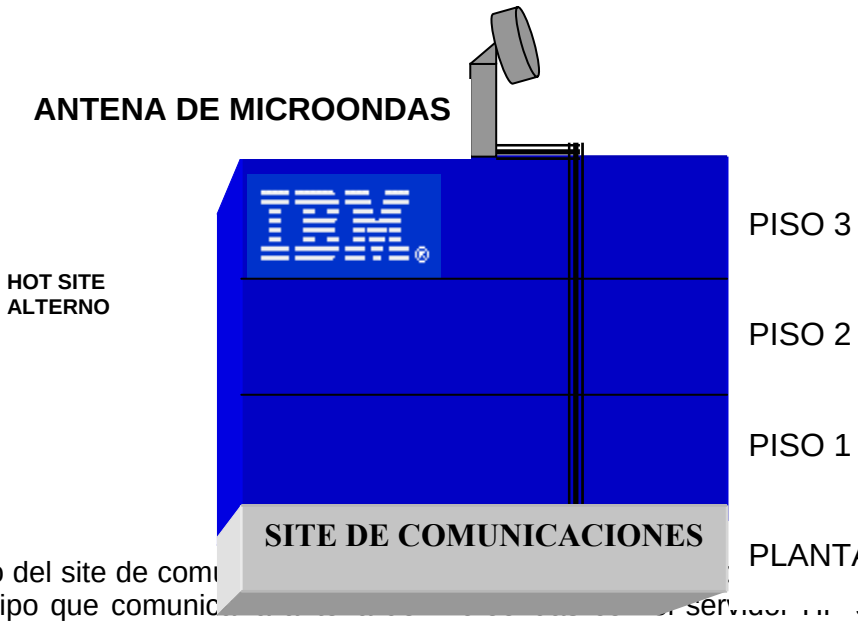
Ver figura:



El centro de operaciones de respaldo IBM, cuenta con 2 líneas de comunicación por microondas hacía Teletech y Telepuerto respectivamente.

La antena de transmisión de microondas de IBM, se encuentra montada en la parte superior del edificio.

Ver figura.



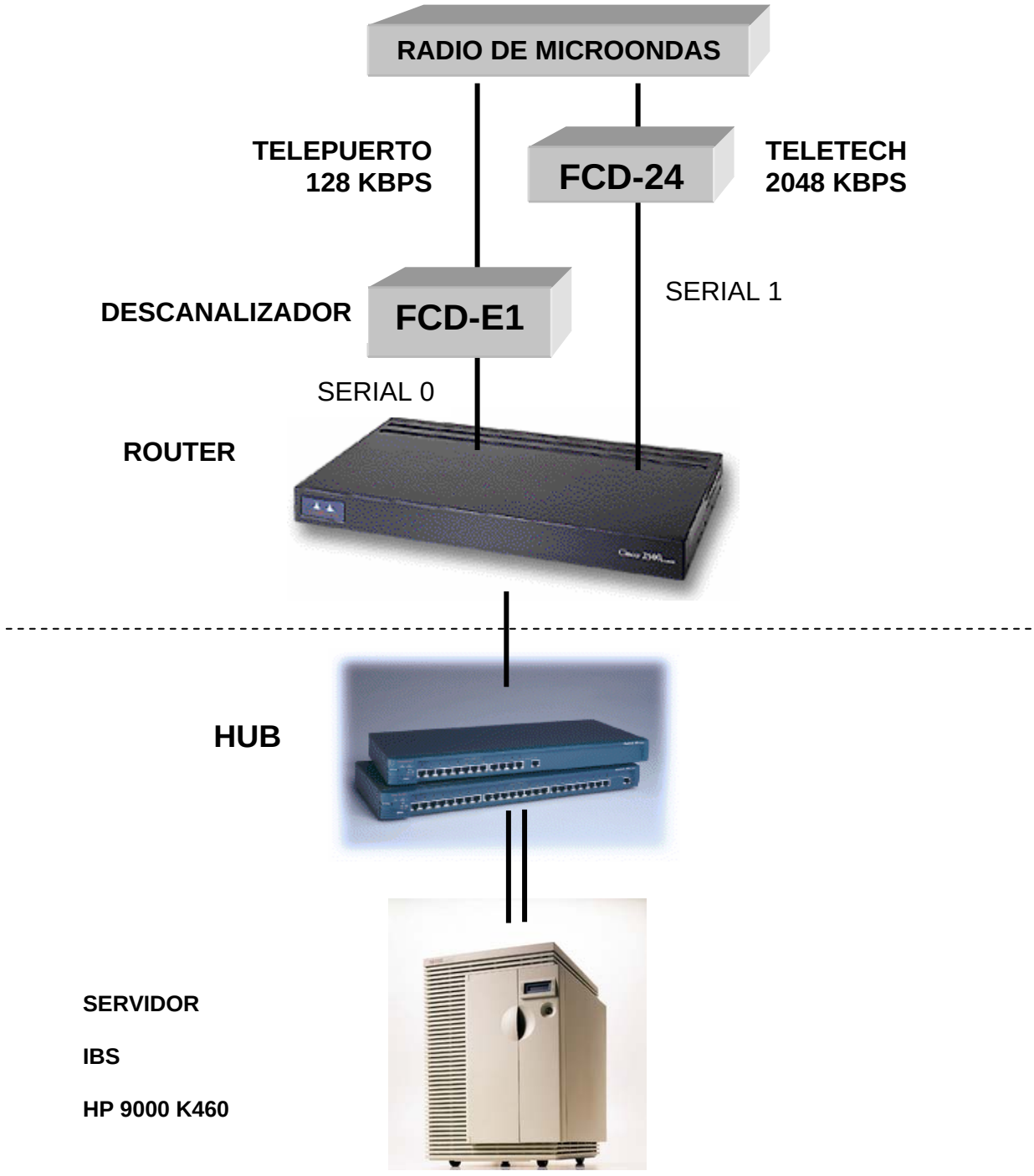
Dentro del site de comu ra el equipo que comunic servidor [illegible] de IBS y que esta estructurado de la siguiente manera:

FDC-24

ROUTER

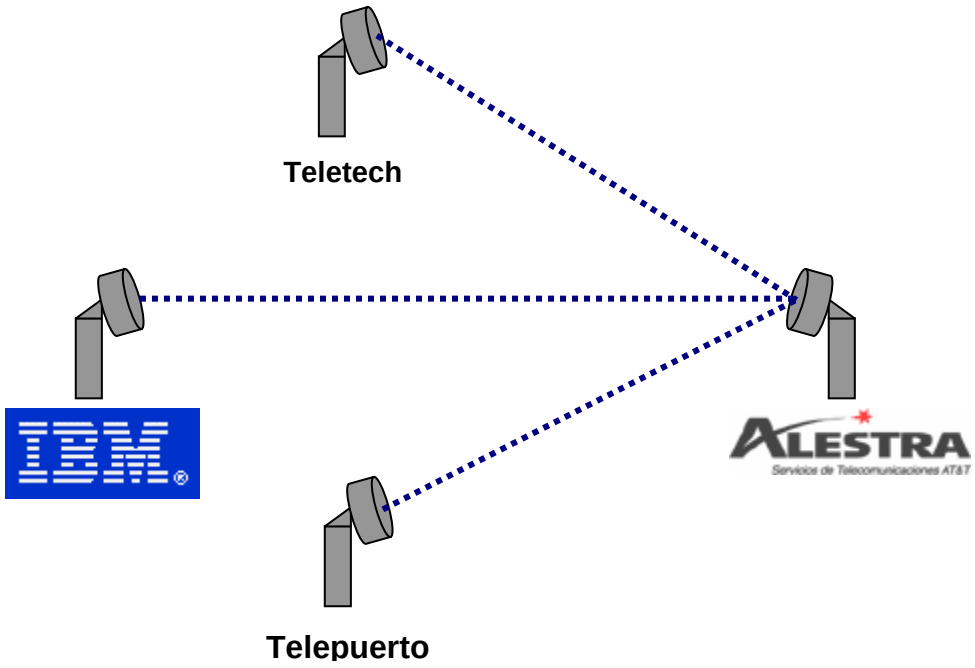
RADIO DE MICROONDAS

El equipo del site de comunicaciones arriba descrito, se encuentra conectado a su vez con el equipo HP9000 en el centro de respaldo:



Esta misma línea de comunicación por microondas en IBM corre hacia Teletech y Telepuerto, pasando por Alestra para la retransmisión de señal.

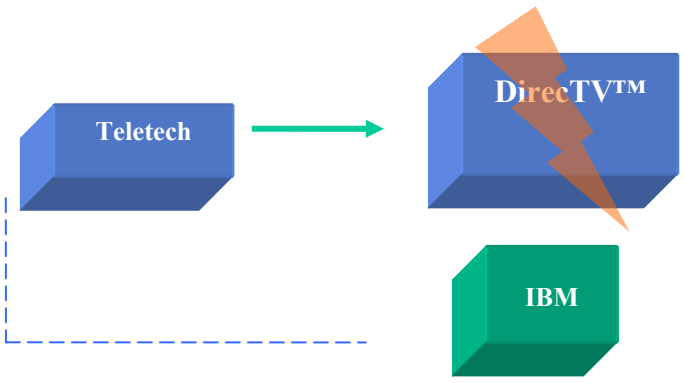
Ver figura:



En caso de un desastre, se deben ejecutar los siguientes procedimientos, tanto en Teletech como en Telepuerto:

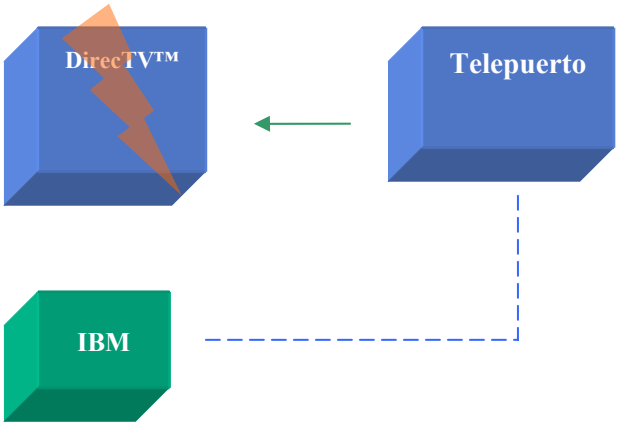
Estrategia de recuperación de redes en Teletech:

- ✓ El equipo de administración notifica el desastre al equipo de redes de Teletech.
- ✓ El equipo de redes de Teletech inicia el procedimiento de restauración de la red de respaldo IBM y Teletech.
- ✓ El equipo de redes de Teletech termina el procedimiento.
- ✓ El equipo de redes de Teletech avisa al equipo de redes en IBM, la finalización del procedimiento de restauración.
- ✓ El equipo de redes de Teletech e IBM prueban la comunicación.
- ✓ El equipo de redes de Teletech da por concluido el procedimiento.
- ✓ El equipo de redes de Teletech notifica al equipo de administración la conclusión del procedimiento de restauración.



Estrategia de recuperación de redes en Telepuerto:

- ✓ El equipo de redes de Telepuerto inicia el procedimiento de restauración de la red.
- ✓ El equipo de redes de Telepuerto termina el procedimiento de restauración de la red.
- ✓ El equipo de redes de Telepuerto avisa al equipo de redes en IBM la finalización del procedimiento de restauración.
- ✓ El equipo de redes de Telepuerto da por concluido el procedimiento.
- ✓ El equipo de redes de Telepuerto notifica al equipo de administración la conclusión del procedimiento de restauración.



10. Plan de Pruebas en Situaciones Específicas.

El DRP debe ser consistente con los procedimientos de respaldo y recuperación, por lo que deben efectuarse pruebas de eficacia, durante periodos programados de tiempo.

Existen varios niveles en los que deben efectuarse las pruebas.

Nivel 1. Pruebas en aplicaciones, bases de datos y sistemas operativos.
Descripción.
Este nivel de prueba debe consistir en la recuperación de aplicaciones y/o software de las funciones críticas que considere el plan (DRP). Se debe contar con la aprobación del usuario.

Nivel 2. Pruebas de comunicaciones.
Descripción.
Este nivel de prueba se debe medir la comunicación de respaldo entre IBM y Teletech e IBM y Telepuerto.

Nivel 3. Pruebas de contactos.
Descripción.
Revisar la vigencia de la lista de contactos que se tenga.

Nivel 4. Prueba de integridad de los respaldos en las ubicaciones fuera de sitio.
Descripción.

Debe probarse que los respaldos almacenados en las ubicaciones fuera de sitio puedan ser recuperados y los datos estén íntegros.

Nivel 5. Reuniones periódicas de equipos de recuperación de desastres.
Descripción.
Realizar juntas periódicas con los integrantes de los equipos del DRP para analizar las alternativas de acción en diferentes casos de desastre.

11.- Procedimientos para la Rehabilitación en el Site Primario.

Los procedimientos incluidos en esta sección del manual son la dirección de las acciones a ser tomadas para la rehabilitación de las nuevas instalaciones (sitio primario), el traslado a éste sitio y recuperar al procesamiento del negocio y sistemas de aplicación críticos.

Inspección de las instalaciones

1. Cuando la rehabilitación de las nuevas instalaciones se haya completado o el estado de peligro haya terminado y las instalaciones de aire acondicionado, eléctricas, etc., estén probadas, se deben de desempeñar las siguientes tareas:

- Notificar al equipo de administración del Plan de Recuperación de la ubicación alterna.

Un día antes del traslado al Site primario.

- Respaldar la base de datos de IBS
- Validar el contenido del respaldo.
- Colocar las cintas en recipientes apropiados junto con una lista impresa de la información que contienen.
- Empacar las cintas y cualquier otra propiedad (debidamente inventariada en la lista de transporte)

Responsabilidad: **El equipo de recuperación de instalaciones y sistemas de datos**

2. En las instalaciones del Site primario, recibir los materiales debidamente empacados.

Verificar contra la lista de transporte que se están recibiendo todos los artículos que allí aparecen y que se encuentren en buenas condiciones. Si faltara cualquier cinta de respaldo pida su reenvió desde las instalaciones alternas.

Responsabilidad: **El equipo de recuperación de instalaciones y sistemas de datos.**

Hardware y comunicaciones

- Entrega de las Instalaciones principales.

A través del intercambio de ideas con el encargado de las instalaciones principales y la inspección del mismo, asegurar que todas las utilidades necesarias están funcionando, es decir:

- Aire acondicionado.
- Energía eléctrica.
- Comunicaciones.

Informar de cualquier problema para ser solucionado lo antes posible.

Responsabilidad: **El equipo de recuperación de Instalaciones y sistemas de datos.**

- La instalación y prueba del equipo.

Si el equipo no ha sido ya instalado por el personal de emergencia, monitorear la entrega, instalación y prueba de equipo.

Verificar el equipo ordenado, ha sido instalado y probado adecuadamente en las instalaciones principales.

Actuar como enlace entre los proveedores y la administración del sitio alterno sobre cualquier problema de instalación.

Responsabilidad: **El equipo de recuperación de Instalaciones y sistemas de datos.**

- La recepción de materiales de respaldo

Revisar el contenido de los materiales de respaldo recibidos, y verificar el contenido uno por uno de la relación de empaque.

- Cintas de respaldo del sistema operativo y base de datos.
- La documentación que describe los procedimientos de restauración para las aplicaciones críticas del HP 9000 “Kmex”.

Responsabilidad: **El equipo de recuperación de Instalaciones y sistemas de datos.**

Procesos para el levantamiento de los equipos y comunicaciones.

Se deberán de llevar a cabo los procedimientos de restauración de comunicaciones para establecer la comunicación en el centro de operaciones de Directv de acuerdo a su esquema original es decir la comunicación entre las oficinas centrales, Teletech y Telepuerto.

Responsabilidad: **El equipo de recuperación de Comunicaciones.**

Sistemas operativos y aplicaciones.

Los sistemas operativos y aplicaciones se restauraran del modo que es descrito en el punto 10.3.- Procedimientos de Recuperación de Datos.

Responsabilidad: El equipo de recuperación de Instalaciones y sistemas de datos.

Registros vitales.

Se refiere a las cintas necesitadas para restaurar el sistema operativo.

1. Cinta: respaldo del file system contiene el sistema operativo HPUX, e INFORMIX.
2. Cinta: DDS (4mm) contiene los Log's del sistema IBS

Toda la información del sistema IBS esta contenida en estas cintas, en la primera cinta se encuentra el sistema operativo HP-UX, en la segunda cinta se encuentra la base de datos INFORMIX.

Si cualquier material se pierde, llamar al centro de comando de emergencia ubicado en el site alterno y solicitar una copia reenvío del mismo.

Responsabilidad: **El equipo de recuperación de instalaciones y sistemas de datos.**

11.1 PROCESOS OPERACIONALES.

- Actualizar las aplicaciones a su estado actual.

Notificar a los usuarios que todos los sistemas y las aplicaciones se han movido al site primario informándoles de la fecha del último respaldo.

Responsabilidad: **El equipo de recuperación de facilidades y sistemas de datos.**

- Liberación de los sistemas a los usuarios.

1. Notifique a los usuarios que todos los sistemas de producción fueron recuperados y que están listos para su utilización.

Tomar nota en particular que:

- Las plantillas normales del personal de producción se reanudan.
- Los procedimientos normales de respaldo se reanudan.
- La distribución normal de operaciones se reanuda.

Responsabilidad: **El equipo de administración de recuperación de desastre.**

- Regresar al proceso de operativo normal.

1. Para la primera semana siguiente a la liberación a usuarios de los sistemas recuperados, monitorear cuidadosamente los problemas de usuario y corregir cualquier problema encontrado.

El equipo de recuperación de sistemas deberá permanecer en alerta durante este periodo.

Responsabilidad: **El equipo de recuperación de instalaciones y sistemas de datos y el equipo de administración.**

2. Cuando los problemas se hayan resuelto al final de la primera semana, se considerará como terminado el estado de alerta para todos los equipos de recuperación.

Responsabilidad: **El líder del equipo de administración.**

- Conducir una revisión posterior al desastre.

1. Tan pronto como sea posible, después de que se ha realizado toda la recuperación, programar una serie de reuniones para cada equipo de recuperación de desastre y finalmente con el equipo de administración de recuperación de desastre.

Responsabilidad: **El equipo de administración de recuperación de desastre.**

2. En las reuniones individuales de equipo, discutir los logros y fracasos de los esfuerzos de recuperación con los miembros del equipo y con referencia a los minutas de las reuniones del equipo de recuperación. Obtener recomendaciones de cómo el plan podría o debe mejorarse.

Responsabilidad: **Los líderes del equipo de recuperación de desastre.**

3. El equipo de administración de recuperación de desastre discute los puntos mencionados por los equipos individuales y decidir qué puntos deben ser redirigidos.

Responsabilidad: **El equipo de administración de recuperación de desastre.**

APENDICE B

METODOLOGIA DE DESARROLLO SOFDRP

METODOLOGÍA DE DESARROLLO APLICACIÓN SOFDRP

En el siguiente apartado se menciona las fases de la metodología empleada para la realización del sistema de administración del Plan de Recuperación.

Análisis
- Estudio Preliminar
- Planeación
- Propuesta

Diseño
- Diccionario de Datos
- Diagrama Entidad Relación

Desarrollo
Implementación
Plan de Pruebas
Documentación Técnica
Manual de Usuario

En base a las etapas de desarrollo previamente mencionadas se llevo a cabo el desarrollo del sistema con el fin de que se cumpla con los requerimientos planteados.

ESTUDIO PRELIMINAR

Primer Acontecimiento del Problema

Grupo Galaxy Mexicana (Directv™), líder en servicios de comunicación y de entretenimiento vía satélite, ha mostrado en los últimos años un aprovechamiento importante de su infraestructura tecnológica, incrementando fuertemente sus operaciones diarias.

Los directivos de Directv™, han planteado la necesidad de contar con un sistema de información el cual tenga como objetivo el de administrar eficientemente la información necesaria para la toma de decisiones oportuna durante una situación de contingencia.

El no contar con una herramienta de este tipo con lleva a no tener actualizados los procedimientos que involucran el Plan de Recuperación de la compañía. En este sentido se convierte en una necesidad la creación de este sistema.

Objetivos.

Como resultado de una primera fase de análisis se obtuvieron los siguientes objetivos:

- Proporcionar una guía para el desarrollo del Plan de Contingencia.
- Agilizar los procesos de documentación
- Optimizar el manejo de información
- Facilitar el mantenimiento y actualización del Plan de Contingencia
- Brindar seguridad a la información
- Administrar de manera centralizada la información

PLANEACIÓN

Para que nuestro sistema proporcione los elementos suficientes para facilitar la administración de la información necesaria para un Plan de Recuperación en caso de contingencia se requiere que se consideren los siguientes puntos:

- Procesos Críticos
- Comités de Recuperación
- Aplicaciones Criticas
- Proveedores
- Empleados involucrados en Aplicaciones Criticas
- Acciones del Plan a tomar durante una contingencia
- Visualización e Impresión de documentos Relacionados al Plan de Recuperación
- Software
- Documentos relacionados al Plan de Recuperación
- Registros Vitales y Líneas de comunicación.
- Adquisiciones de Activos
- Módulo de Consulta
- Módulo de Reportes

PROPUESTA

Tomando en cuenta los requerimientos detectados durante el análisis se decidió desarrollar los módulos que a continuación se describen, la información completa de los campos que incluye cada uno, se detalla en la documentación técnica del sistema que más adelante se proporciona.

Pre Plan

Este módulo contendrá información acerca de lo que es un Plan de Contingencia y su importancia, se mencionara el perfil de Grupo Galaxy Mexicana S.A. de C.V. así como el directorio de empleados y proveedores relacionados al Plan, es decir que sus funciones tienen que ver con la continuidad del negocio.

Procesos Críticos

El objetivo de este módulo es poder almacenar un catalogo de los procesos operativos más críticos que la empresa tiene, alimentando información de prioridad de recuperación para cada proceso, ingresando los niveles de impacto como son: Impactos Legal y Fiscal, Operativo, Económico, de Imagen y de pérdida del negocio. Lo anterior se determina en base al Análisis de Impacto al Negocio.

Empleados involucrados en Aplicaciones Criticas

En este módulo se visualizaran, los usuarios de aplicaciones criticas, lo cual permite conocer en todo momento quienes son los afectados al fallar uno de estos sistemas críticos para la compañía.

Comités

El objetivo de este módulo es poder dar de alta los comités de recuperación, así como la responsabilidad de éstos dentro del Plan de Contingencia, una vez ingresados los comités en el sistema se podrán vincular a los empleados.

Usuarios por Comité

En este módulo el usuario podrán identificar a los empleados por comité, para una rápida visualización de estos.

Acciones del Plan

En este módulo se describen las acciones que se deben realizar antes de que la contingencia se suscite, así como las actividades a desarrollar durante la contingencia y finalmente que se debe hacer para llevar a cabo la reinstalación de los procesos normales. Lo anterior tiene como objetivo principal disminuir el impacto que la contingencia provoca.

Aplicaciones Críticas

Además de ingresar información referente a las aplicaciones criticas de la empresa, en este módulo también se registran los requerimientos mínimos para procesar cada una de las estas aplicaciones. Lo cual permite conocer el equipo mínimo necesario para la operación de dicha aplicación así como los enlaces de comunicaciones requeridos, etc.

Diseño del Manual

El objetivo de este módulo es visualizar detalladamente el Plan de Recuperación por escrito y en caso de existir una modificación a éste, el sistema deberá de ser capaz de reflejar estos cambios con el fin de distribuir a los integrantes de los comités la versión más actualizada del Plan de Contingencia.
Simulacros

El sistema proporcionara información relativa a los simulacros realizados, presentando los resultados obtenidos. El administrador del sistema contara con este módulo para el fácil mantenimiento y distribución de dichos documentos.

Adquisiciones de Activos

En este módulo el usuario podrá ingresar las adquisiciones realizadas, con el fin de que en caso de contingencia se pueda determinar la factura enlazada a dicha adquisición, por ejemplo un equipo, un dispositivo de Red, equipos de seguridad, etc y a su vez identificar al proveedor correspondiente para futuras aclaraciones. Este módulo tendrá información importante para el equipo de reclamación de daños en caso de una contingencia. El tener esta información es vital para recuperar la operatividad normal durante la etapa de reinstalación después de la contingencia.

Inventario de documentos relacionados al Plan de Contingencia

En este módulo se registraran los documentos críticos para la operación de la compañía y se determinará a que proceso critico definido esta ligado, así como su periodicidad de reemplazo, esto con el fin de estar preparados en caso de una discontinuidad prolongada de operaciones.

Registros Vitales

En este módulo el usuario ingresara información respecto a los registros vitales como por ejemplo: respaldos de bases de datos, archivos de seguridad, archivos de configuración, etc. Se deberá especificar la periodicidad del respaldo, así como el medio de almacenamiento utilizado y además a que aplicación critica pertenece.

Administración

En este módulo el usuario encontrara una serie de pantallas para que en caso de ingresar nuevos elementos al Plan de Recuperación, el sistema tenga la funcionalidad de ingresarlos, como por ejemplo: Un nuevo centro de negocio, un medio de almacenamiento adicional, una nueva fase dentro del Plan, etc.

Software

En este módulo el usuario podrá ingresar información acerca del software utilizado en la compañía ya que en caso de una contingencia lo pueda rápidamente identificar.

Ayuda

Este módulo proporcionara ayuda en línea para aprender a utilizar el sistema y como navegar dentro del mismo.

DISEÑO

DICCIONARIO DE DATOS

Cuadros de entidades

Una entidad es una componente claramente identificable que se puede distinguir y definir por sus características particulares. A continuación se definen para cada uno de los formularios

ENTIDAD: Empleados
DESCRIPCIÓN: Tabla para la captura, modificación y baja de todos los empleados de la empresa.

NO. CAMPO	NOMBRE	TIPO DE DATOS	LONGITUD	DESCRIPCIPON	KEY
1	id_emp	int	4	Cadena de caracteres única para identificación de los Empleados	SI
2	nom_emp	varchar	80	Nombre completo del usuario.	
3	Tel_oficina	varchar	50	Números telefónicos dentro de la empresa donde se le pueda localizar.	
4	Puesto	varchar	60	Nombre del puesto del empleado.	
5	Localidad	varchar	50	Nombre de la localidad ala que pertenece.	
6	Área	varchar	60	Nombre del departamento o área de la que forma parte.	
7	Cel_bipper	varchar	50	Número telefónico del celular o bipper.	
8	Dir_casa	varchar	50	Nombre de la calle y número exterior e interior del domicilio particular del empleado.	
9	cod_postal	numeric	9	Código postal al que pertenece su domicilio.	
10	Colonia	varchar	80	Nombre de la colonia ala que pertenece su domicilio particular.	
11	telefono_casa	varchar	50	Número telefónico de su casa.	
12	Delegacion	varchar	80	Delegación política a la que pertenece su domicilio particular.	
13	Comité	varchar	80	Nombre del comité de recuperación al que pertenece el empleado.	
14	Procesocritico	varchar	100	Proceso critico del que se encarga	
15	Observaciones	Text	16	Observaciones	
16	Aplicación	varchar	25	Aplicación critica a la que pertenece	
17	nom_emp_res	varchar	80	Nombre de la persona que lo puede sustituir en caso de que este ausente.	
18	Email	varchar	60	Dirección de correo del empleado	

ENTIDAD: Comités de Recuperación
DESCRPCIÓN: Datos de los grupos de Comités de recuperación en caso de una contingencia

NO. CAMPO	NOMBRE	TIPO DE DATOS	LONGITUD	DESCRIPCIPON	KEY
1	id _ comité	Int	4	Cadena de caracteres única para identificación de los Comités	SI
2	nombre _ comité	varchar	80	Nombre de los comités	
3	Descripción _comité	Text	16	Descripción de las táreas que se realizara el grupo en conjunto	

ENTIDAD: Proveedores
DESCRIPCIÓN: Relación de todos los datos de los proveedores de la empresa.

NO. CAMPO	NOMBRE	TIPO DE DATOS	LONGITUD	DESCRIPCIPON	KEY
1	id_proveedor	Int	4	Cadena de caracteres única para identificación Proveedores	SI
2	nom_proveedor	varchar	80	Nombre completo del proveedor	
3	Dirección	varchar	100	Calle y Número interior y exterior donde se localiza la oficina del proveedor	
4	Pagweb	varchar	60	Pagina de web de la empresa del proveedor	
5	Ciudad	varchar	50	Nombre de la ciudad o estado donde se localiza la empresa del proveedor	
6	Cod_postal	numeric	9	Número del código postal correspondiente al domicilio de la empresa	
7	tel1	varchar	50	Número de teléfono	
8	tel2	varchar	50	Número de un segundo teléfono (sí existe)	
9	tel3	varchar	50	Número de un tercer teléfono (si existe)	
10	fax1	varchar	50	Número del fax	
11	fax2	varchar	50	Segundo número fax (si existe)	
12	Representante	varchar	80	Nombre de la persona con que se contacta.	
13	Sub Representante	varchar	80	Nombre de una segunda persona con quien se contacta	
14	Cargo	varchar	60	Puesto al que pertenece el empleado	
15	Email	varchar	60	Dirección de correo del empleado o empresa	

ENTIDAD: Procesos Críticos
DESCRIPCIÓN: Datos del catalogo de procesos críticos

NO. CAMPO	NOMBRE	TIPO DE DATOS	LONGITUD	DESCRIPCIPON	KEY
1	id_proc	Int	4	Cadena de caracteres única para identificación de los procesos críticos	SI
2	nom_proc	varchar	100	Cadena que identifica al proceso	
3	desc_proc	text	16	Descripción breve del proceso	
4	imp_lf_proc	varchar	50	Afectación del proceso en los aspectos fiscal y legal de la empresa. Cuatro opciones: Alta, Medio, Bajo o Nulo.	
5	imp_ec_proc	varchar	50	Afectación del proceso en el aspecto económico de la empresa. Cuatro opciones: Alta, Medio, Bajo o Nulo.	
6	imp_op_porc	varchar	50	Afectación del proceso en el aspecto funcional de la empresa. Cuatro opciones: Alta, Medio, Bajo o Nulo.	
7	imp_img_proc	varchar	50	Afectación del proceso en cuanto ala imagen de la empresa. Cuatro Opciones: Alta, Medio, Bajo o Nulo.	
8	imp_perdida_neg	varchar	50	Afectación del proceso en la salida del mercado de la empresa. Cuatro opciones: Alta, Medio, Bajo o Nulo.	
9	imp_total	Float	8	Evaluación total de los impactos	
10	Aplicación	varchar	50	Aplicación critica a la que pertenece	
11	Área	varchar	50	Área a la que pertenece	
12	Documento	varchar	40	Documento relacionado	

ENTIDAD: Acciones del Plan
DESCRIPCIÓN: Descripción de las actividades y acciones que se llevaran a cabo en cada una de las fases en que se divide el Plan de Contingencia.

NO. CAMPO	NOMBRE	TIPO DE DATOS	LONGITUD	DESCRIPCIPON	KEY
1	id_acción	Int	4	Cadena de caracteres única para identificación del Plan	SI
2	Nombre	varchar	100	Nombre del Plan	
3	Descripción	text	16	Resumen detallado de las actividades a realizarse en esta etapa.	
4	Fase	varchar	40	Nombre de una de las tres fases en que se divide en plan de recuperación: Preparación, operación o Preinstalación	
5	nom_comité	varchar	80	Nombre de los comités	

ENTIDAD: Adquisiciones
DESCRIPCIÓN: Control de Adquisiciones de equipo en general.

NO. CAMPO	NOMBRE	TIPO DE DATOS	LONGITUD	DESCRIPCIPON	KEY
1	id_ad	real	4	Cadena de caracteres única para identificación de las Adquisiciones	SI
2	nombre_ad	varchar	50	Nombre del material adquirido	
3	desc_ad	text	16	Resumen detallado de las compras	
4	nom_proveedor	varchar	80	Proveedor al que se realizo la compra	
5	fecha_compra	smalldatetime	4	Fecha de adquisición	
6	no_factura	varchar	50	Número de folio de la factura	
7	Monto	varchar	50	Costo total de la compra	

ENTIDAD: Líneas de Comunicación
DESCRIPCIÓN: Relación de las diferentes líneas de comunicación existentes.

NO. CAMPO	NOMBRE	TIPO DE DATOS	LONGITUD	DESCRIPCIPON	KEY
1	id_línea	int	4	Registro único de las líneas de Comunicación	SI
2	Nombre	varchar	80	Nombre de la línea de comunicación	
3	Descripción	text	16	Descripción breve de la línea de comunicación	
4	Velocidad	varchar	50	Velocidad con la que trabaja la línea	
5	Localidad	varchar	50	Nombre de la localidad a la que pertenece	
6	Medio	varchar	50	Medio de transmisión del enlace	
7	Localidaddestino	varchar	50	Localidad destino	

ENTIDAD: Áreas
DESCRIPCIÓN: Nombre de todas las áreas en que esta organizada la empresa

NO. CAMPO	NOMBRE	TIPO DE DATOS	LONGITUD	DESCRIPCIPON	KEY
1	id_área	int	4	Cadena de caracteres única para identificación de las áreas	SI
2	Nombre_área	varchar	60	Nombre del área	

ENTIDAD: Registro de Software
DESCRIPCIÓN: Relación del software contenido y sus características.

NO. CAMPO	NOMBRE	TIPO DE DATOS	LONGITUD	DESCRIPCIPON	KEY
1	id	int	4	Cadena de caracteres única para identificación del Software	SI
2	nombre	varchar	80	Nombre del Software	
3	versión	varchar	50	Especificación de la versión del Software	
4	plataforma	varchar	50	Plataforma operativa del Software.	
5	licencia	varchar	50	Número de licencia del Software	
6	observaciones	text	60	Descripción breve y / o comentarios	
7	Proveedor	varchar	50	Proveedor	

ENTIDAD: Inventario de Documentos
DESCRIPCIÓN: Relación de aquellos papeles para la operatividad de la empresa

NO. CAMPO	NOMBRE	TIPO DE DATOS	LONGITUD	DESCRIPCIPON	KEY
1	id_forma	Int	4	Cadena de caracteres única para identificación de los Inventarios de Documentos	SI
2	nom_forma	varchar	50	Nombre del documento	
3	Desc_forma	text	16	Comentarios del documento	
4	cantidad	Int	4	Cantidad adquirida	
5	reemplazo	Int	4	Periodo de renovación o nueva adquisición	
6	Localidad	varchar	50	Nombre de la localidad a la que pertenece.	
7	Nom_proc	varchar	60	Proceso critico al que se destina	

ENTIDAD: Registros Vitales
DESCRIPCIÓN: Relación de aquellos documentos, cintas y disquetes que contienen la información necesaria para recuperar la operatividad de los procesos.

NO. CAMPO	NOMBRE	TIPO DE DATOS	LONGITUD	DESCRIPCIPON	KEY
1	id_respaldo	Int	4	Cadena de caracteres única para identificación de los Registros Vitales	SI
2	Nombre	varchar	60	Nombre Registro Vital	
3	Descripción	text	16	Descripción	
4	Localidad	varchar	50	Localidad	
4	Aplicación	varchar	50	Aplicación critica a la que pertenece	
5	Frecuencia	varchar	50	Periodo de tiempo fijo en que se realiza el respaldo	
6	Medio	varchar	50	Tipo de dispositivo de almacenamiento	
7	Cantidad	Int	4	Números de dispositivos en que se almacena un solo respaldo.	
8	Tipo	varchar	50	Tipo de respaldo	
9	fecha_realización	smalldatetime	4	Fecha con que se realizo el respaldo	
10	Comité	varchar	80	Nombre del comité responsable.	
11	Hora	varchar	50	Hora aproximada del respaldo	

ENTIDAD: Aplicación Critica
DESCRIPCIÓN: Registro de las aplicaciones más importantes con las que opera la empresa y los requerimientos mínimos necesarios para su funcionamiento

NO. CAMPO	NOMBRE	TIPO DE DATOS	LONGITUD	DESCRIPCIPON	KEY
1	Inaplica	int	4	Cadena de caracteres única para identificación de la Aplicación Critica	SI
2	Nombreaplica	varchar	25	Nombre de la aplicación critica	
3	Descaplica	text	16	Descripción detallada de la operatividad de la aplicación critica	
5	req_equipo	varchar	100	Dispositivos necesarios (Pc, impresora, etc.)	
6	req_fimpresas	varchar	50	Documentos que necesitara	
7	req_enlaces	varchar	50	Dispositivos o periféricos por el cual se llevara a cabo la comunicación	
8	req_loficina	int	4	Número de lugares de oficina donde se requiere	
9	req_misceláneos	varchar	100	Dispositivos extras (calculadoras, impresoras, etc.)	
10	Observaciones	text	16	Descripción breve, acerca de la aplicación	

ENTIDAD: Centros de Negocio
DESCRIPCIÓN: Instalaciones con la que cuenta la empresa.

NO. CAMPO	NOMBRE	TIPO DE DATOS	LONGITUD	DESCRIPCIPON	KEY
1	id_localidad	Int	4	Cadena de caracteres única para identificación del Centros de Negocio	SI
2	nom_localidad	varchar	50	Nombre del centro de negocio	
3	Dirección	text	16	Ubicación ó dirección completa del centro de negocio	

ENTIDAD: Tipos de Respaldos
DECRIPCIÓN: Dispositivos por medio del cual se realizaran los respaldos de la información en caso de contingencia

NO. CAMPO	NOMBRE	TIPO DE DATOS	LONGITUD	DESCRIPCIPON	KEY
1	id_tipo	int	4	Cadena de caracteres única para identificación de los tipos de respaldos	SI
2	Nombre	varchar	50	Nombre del respaldo	
3	Descripción	text	16	Descripción detallada del respaldo	

ENTIDAD: Medios de Transmisión
DESCRIPCIÓN: Forma por el cual se llevara a cabo la comunicación de una a otra instalación en caso de una emergencia de contingencia.

NO. CAMPO	NOMBRE	TIPO DE DATOS	LONGITUD	DESCRIPCIPON	KEY
1	id_mt	Int	4	Cadena de caracteres única para identificación de los Medios de Transmisión	SI
2	nombre	varchar	50	Nombre del tipo de medio de transmisión	

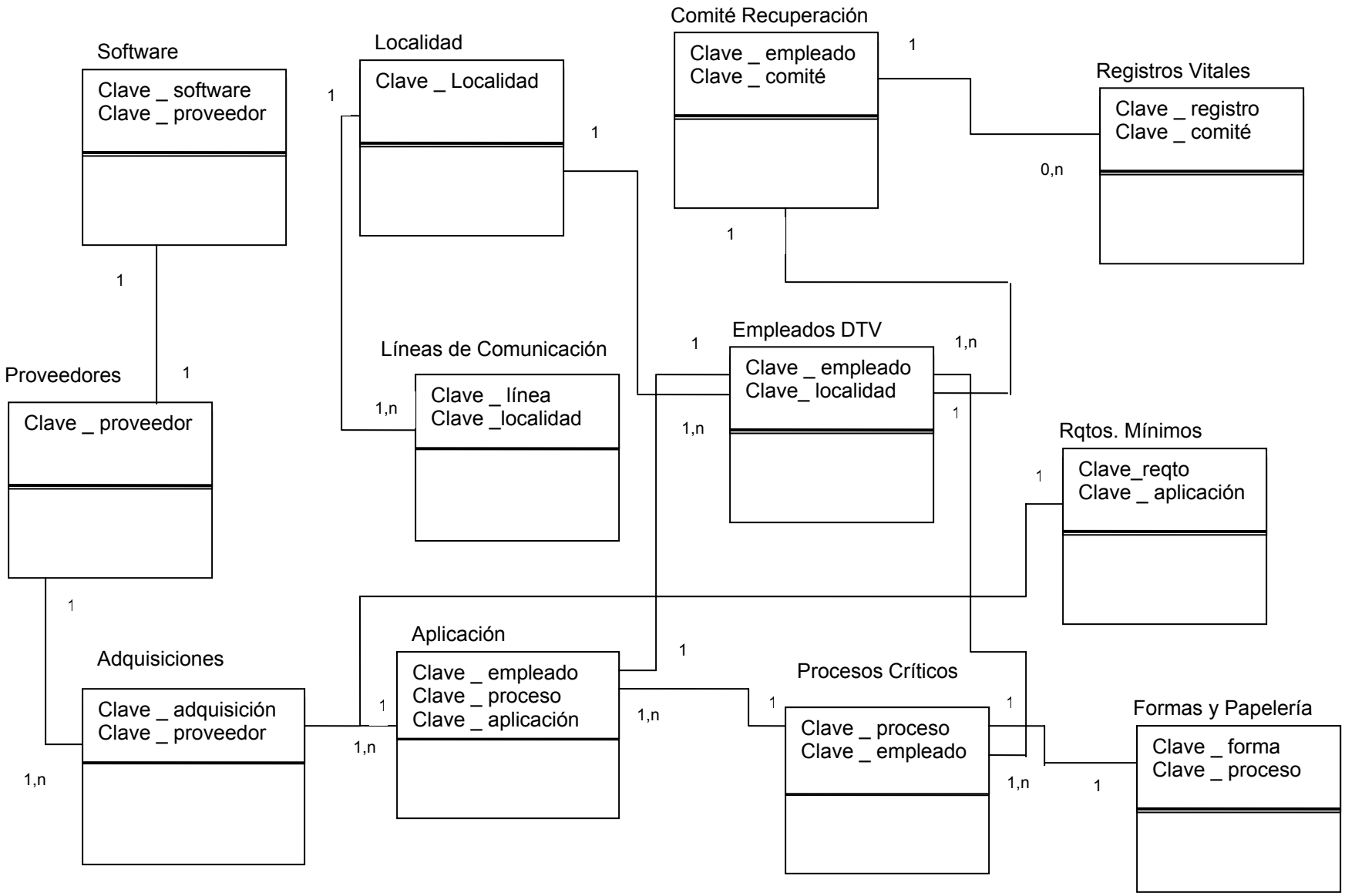
ENTIDAD: Medios de Almacenamiento
DESCRIPCIÓN: Dispositivos por medio del cual se realizaran los respaldos respectivos en caso de una contingencia

NO. CAMPO	NOMBRE	TIPO DE DATOS	LONGITUD	DESCRIPCIPON	KEY
1	id_medio	int	4	Cadena de caracteres única para identificación de los Medios de Almacenamiento	SI
2	Nombre	varchar	80	Nombre del dispositivo	
3	Descripción	text	16	Descripción breve del dispositivo	

ENTIDAD: Fases
DESCRIPCIÓN: División del plan de recuperación para operar en caso de una contingencia

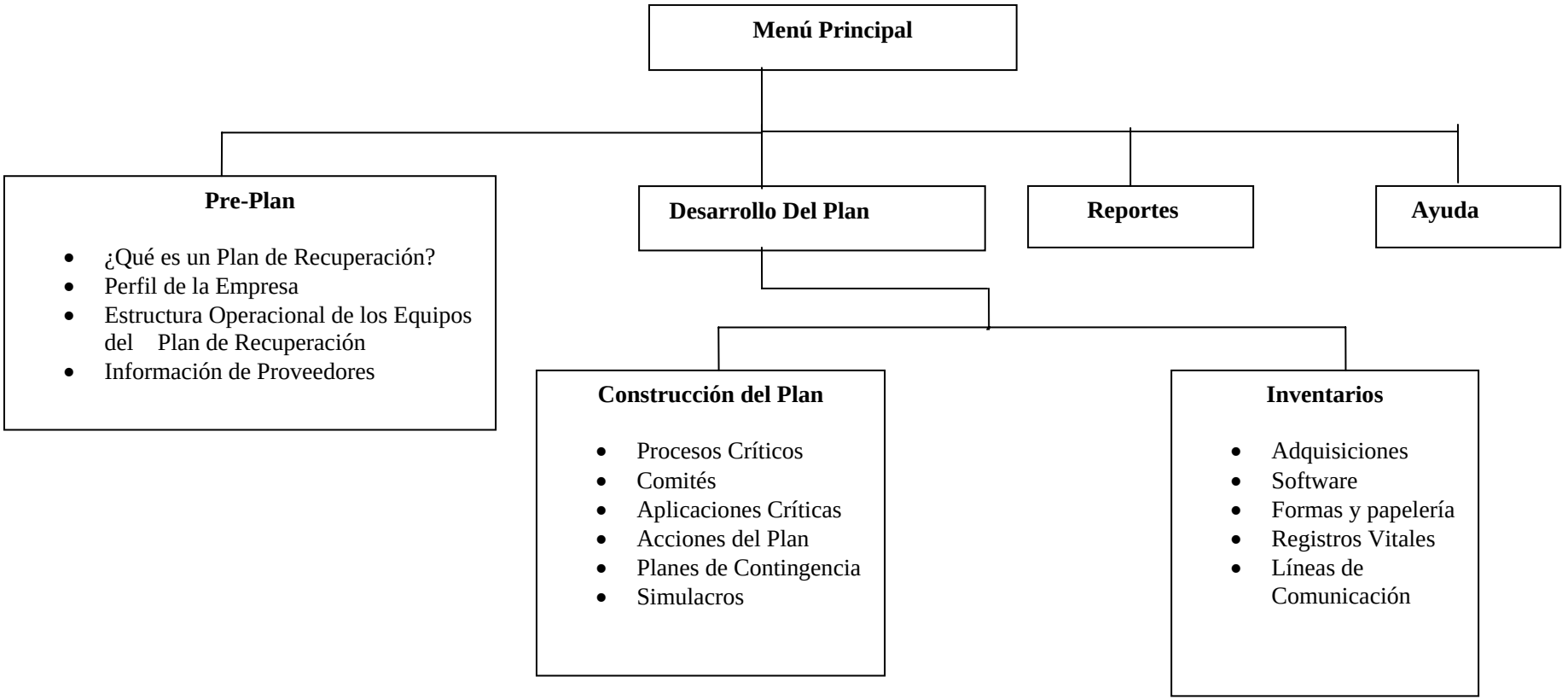
NO. CAMPO	NOMBRE	TIPO DE DATOS	LONGITUD	DESCRIPCIPON	KEY
1	id_fase	Int	4	Cadena de caracteres única para identificación de las fases	SI
2	fase	varchar	35	Nombre de las en plan de recuperación: Preparación, operación o Preinstalación	
3	descripción	Text	16	Descripción breve de la fase	

DIAGRAMA ENTIDAD RELACION


Software
Clave _ software
Clave _ proveedor
Localidad
Clave _ Localidad
Comité Recuperación
Clave _ empleado
Clave _ comité
Registros Vitales
Clave _ registro
Clave _ comité
Proveedores
Clave _ proveedor
Líneas de Comunicación
Clave _ línea
Clave _localidad
Empleados DTV
Clave _ empleado
Clave_ localidad
Rqtos. Mínimos
Clave_reqto
Clave _ aplicación
Adquisiciones
Clave _ adquisición
Clave _ proveedor
Aplicación
Clave _ empleado
Clave _ proceso
Clave _ aplicación
Procesos Críticos
Clave _ proceso
Clave _ empleado
Formas y Papelería
Clave _ forma
Clave _ proceso
1
1,n
0,n

ESQUEMA DE LA APLICACIÓN

Módulos



PROTOTIPO

Una vez indicadas las necesidades de los usuarios del Plan de Recuperación de Desastres para Directv™, y siguiendo las fases de la metodología empleada en el desarrollo del proyecto, se realizo un prototipo mostrándole al usuario el esquema de las pantallas de captura, el acceso y el ingreso de información al sistema, así como los módulos de reportes y de consulta.

Una vez obtenida la aprobación de los usuarios con respecto al alcance del sistema se procedió a la etapa del desarrollo del sistema.

DESARROLLO

Las características principales del sistema SOFDRP son las siguientes:

- Es un sistema desarrollado para computadoras personales
- Integridad de información
- Interfaz gráfica
- Fácil Mantenimiento
- Adaptabilidad

Como manejador de la Base de Datos del Sistema SOFDRP, se opto por SQL-Server 2000, ya que es de fácil mantenimiento y porque se adecua a las necesidades del sistema. Sin embargo el sistema cuenta con la capacidad de que cuando se realiza la instalación por primera ocasión se le pregunta al usuario sobre el repositorio de datos es decir el usuario, podrá elegir entre Access 2000 o si lo prefiere por SQL-Server 2000.

Se determino realizar el desarrollo de este sistema en el Lenguaje de Programación de Visual Basic 6.0 Enterprise Edición, por poseer una interfaz grafica de desarrollo, por ser un lenguaje de programación orientado a eventos, de fácil mantenimiento y actualización.

La aplicación SOFDRP al haber sido desarrollado bajo ambiente Windows, proporciona las facilidades graficas de este ambiente, lo que hace sencillo su uso y manejo, pues se utiliza de forma similar a cualquier otra aplicación Windows.

En cuanto al módulo de Repotes, se decidió utilizar la herramienta Crystal Reports v.7.0, por ser una herramienta completa en el desarrollo de Reportes de tipo OLAP, Cross tab etc.

En los apartados siguientes: manual técnico y el manual de usuario, se especifica en detalle la alimentación de información mediante las pantallas de captura, así como el módulo de reportes.

IMPLEMENTACIÓN

La aplicación se desarrolló en una computadora personal fuera de red, para la implementación del sistema se requirió crear la base de datos en un servidor de Base de Datos SQL-Server. Para realizar esta tarea, el administrador de la Base de Datos, deberá ejecutar los archivos del tipo .dts (Data Transformation Services), en el administrador corporativo de SQL Server.

Para una mejor compatibilidad se recomienda usar SQL Server 2000, como se menciona en las siguientes líneas:

Creación de la Base de Datos

En el CD de instalación del sistema el usuario encontrara en la siguiente directorio los archivos que se enlistan a continuación:

Y:\SOFDRP\DATA

En donde Y representa la unidad de cd-room

1.- EspCreaBase**BDSOFDRP**.dts (Ejecutar este archivo si la versión de SQL se encuentra en español)

2.- EngCreateDataBase**BDSOFDRP** (Ejecutar si la versión de SQL esta en el idioma Ingles)

Los archivos anteriormente mencionados son script´s, cuya función es crear la base de datos en el ambiente de SQL-Sever, el usuario deberá elegir la ejecución de uno de estos dependiendo de la versión de SQL que este instalado en el servidor de base de datos.

Cargar información de SEPOMEX

El sistema cuenta con la funcionalidad de que en el momento que se capturan los empleados dentro del sistema, se propone de manera automática la colonia y la delegación en base al código postal digitado previamente.

El script que realizara la transferencia de información de las tablas de sepomex es el que se menciona a continuación:

3.- TransferenciaTablasSEPOMEX.dts

El dts mencionado anteriormente tiene el objetivo de cargar los datos de las tablas de Sepomex. El administrador de la base de datos, podrá ejecutar este dts, para actualizar la información de códigos postales al sistema.

Para lograr esto, el archivo de origen deberá ser un archivo con extensión mdb, deberá ubicarse en la siguiente carpeta, y la información actualizada deberá encontrarse en dicha base de datos.

C:\SOFDRP\DATA\BDSOFTDRP.MDB

Después de verificar que este archivo exista solo basta con correr el dts llamado TransferenciaTablasSepomex, este proceso actualizara las tablas:

Municipi (Municipios)
Ciudades
TodoCP (Códigos Postales)

Nota.- El sistema cuenta con la funcionalidad de proponer la colonia y delegación, si estas tablas no se encontraran, el usuario podrá ingresar los datos manualmente.

PLAN DE PRUEBAS

El objetivo de estas pruebas consistió en verificar que la aplicación funcionara de manera correcta, a continuación mencionamos en que consistieron dichas pruebas.

Se identifico el servidor de base de datos en donde residiría la Base de Datos obteniendo las siguientes características:

Equipo Pentium con procesador de 1.80 Ghz con 512 MB RAM, y HD de 40 GB.

Se identifico que la versión de SQL SERVER estaba en ingles, así que se procedió a ejecutar el dts de creación de la Base de Datos en dicha versión.

Una vez realizada esta tarea, la siguiente fue ejecutar el dts TransferenciaTablasSEPOMEX.dts Para actualizar la información de los Códigos Postales.

Se procedió a realizar la conectividad entre el equipo cliente y el equipo de servidor de base de datos, obteniendo un buen tiempo de respuesta en el medio físico.

Se realizo a manera de prueba la configuración de un ODBC utilizando el usuario que crea el dts que genera la base de datos, denominado **adminsofdrp** con igual contraseña.

Una vez validados los pasos anteriores se procedió a instalar la aplicación cliente, después de esta actividad, se ingreso por primera vez al sistema y ya una vez en él, se estableció el origen de datos, que finalmente utilizaría la aplicación.

El usuario administrador del Plan después de ejecutar los pasos anteriores descritos se encontró en posibilidad de trabajar con la herramienta

DOCUMENTACION TECNICA

En este apartado se describen los requerimientos para la instalación de la aplicación SOFDRP.

1.- Requerimientos Mínimos

Los requerimientos mínimos que deberá cumplir el sistema de cómputo en donde se instalara la aplicación SOFRDP son los siguientes:

Equipo:

Procesador Pentium I a 366 MHz
Monitor vga 19”
Drive de 3 ½ “
Tarjeta de video de 4MB
64 MB de RAM
Disco duro de 1GB

Software

Office 2000 o posterior

Servidor de Base de Datos
SQL VERSION 7.0 o posterior, preferentemente 2000

2.- Configuración de Aplicación

Estructura de Directorios

Directorio C:\SOFDRP\PLAN

En este directorio se almacenará la información correspondiente a los planes de recuperación, y de igual forma podemos ver el detalle de ese manual dando clic. La extensión de dichos archivos deberá ser ***.doc.**

El equipo en donde se desea instalar el sistema deberá contar con un directorio en donde se encontraran los siguientes componentes del sistema:

C:\SOFDRP\PLAN**PerfilEmpresa.rtf**

Adicionalmente en el documento llamado PerfilEmpresa.rtf deberá contener una breve descripción del perfil de la compañía, en nuestro caso se ingreso en este documento información de Directv™

Directorio C:\SOFDRP\SIMULACROS

Con el objetivo de mostrar los resultados obtenidos en la realización de los simulacros, el sistema tendrá la funcionalidad de mostrarlos, para que con esto se concentre la información en un solo lugar, los archivos deberán ser de tipo .**doc**.

DOCUMENTACION DE USUARIO

A continuación se presentará el manual de usuario de la aplicación SOFDRP, esta ayuda se complementara con la ayuda en línea que presenta el sistema.

Para ingresar al sistema el usuario lo encontrara en el menú de Programas→SOFDRP

Al iniciar la aplicación por primera vez el sistema mostrará una pantalla de configuración referente a la base de datos, deberá indicar el nombre del servidor de base de datos, un nombre a su origen de datos y opcionalmente una descripción.

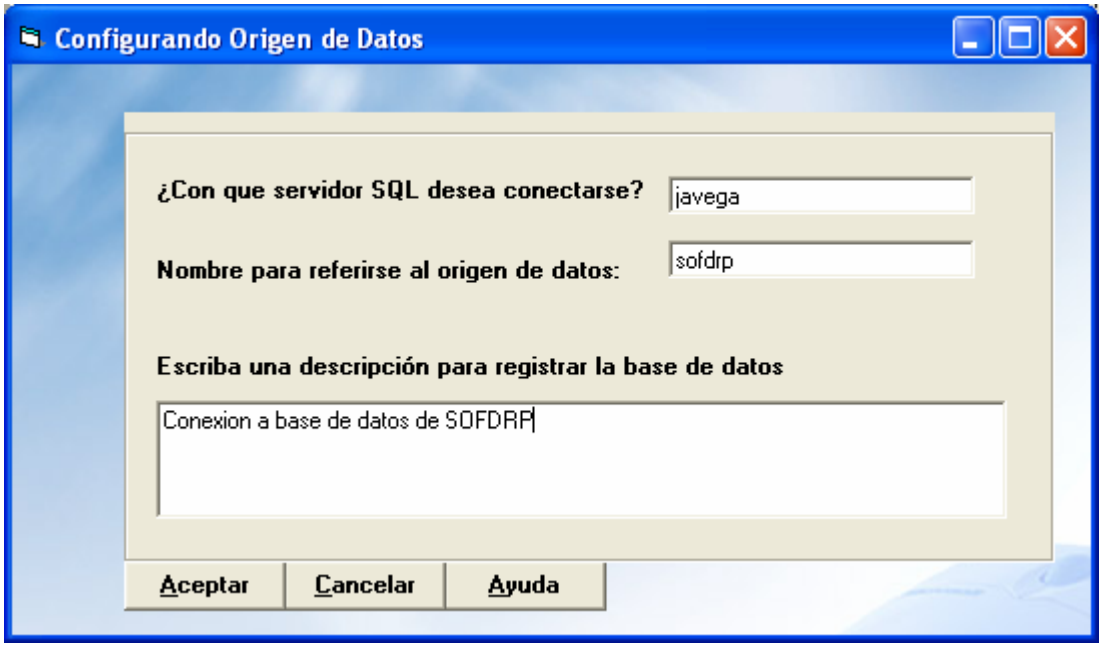
Al ejecutar por primera vez la aplicación, el sistema nos pedirá cierta información referente a la conectividad de los datos.

El sistema cuenta con la funcionalidad de que el repositorio de datos se pueda establecer en base a las necesidades del negocio, es decir que el sistema le agrega esa flexibilidad a la empresa de poder elegir su repositorio de datos si es en SQL –Server o en Access 2000, si elegimos la primera opción el sistema nos pedirá la información necesaria para establecer el origen de los datos.

En el caso de que el usuario decida que su repositorio de datos sea Access 2000, solo deberá validar que el archivo de base de datos BDSOFDRP.MDB, se encuentre en el directorio mencionado a continuación, C: \SOFDRP\DATA, el cual se anexa en el disco de instalación.

A continuación en la siguiente figura se ilustra, la parte de la configuración cuando se elige que el origen de datos se SQL-SERVER

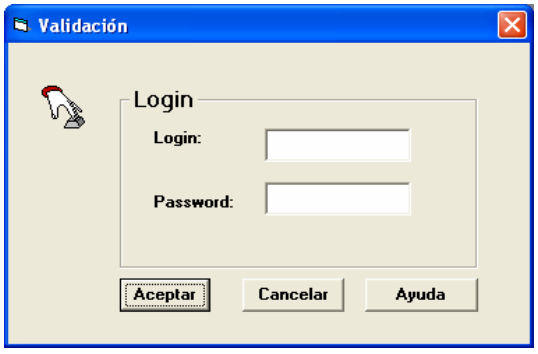
Configuración de la conexión de acceso a datos de SQL-Server



Una vez ingresada la información anterior, debemos de digitar el login y el password en la Pantalla que se nos mostrara a continuación.

Nota.- Dentro de la ejecución del script de la base de datos se crea el usuario **adminsofdrp**, con password de igual manera. Si después si así lo requiere lo podrá cambiar.

Pantalla de Inicio Al iniciar la aplicación el usuario deberá ingresar una clave para acceder al sistema.



Pantalla Principal

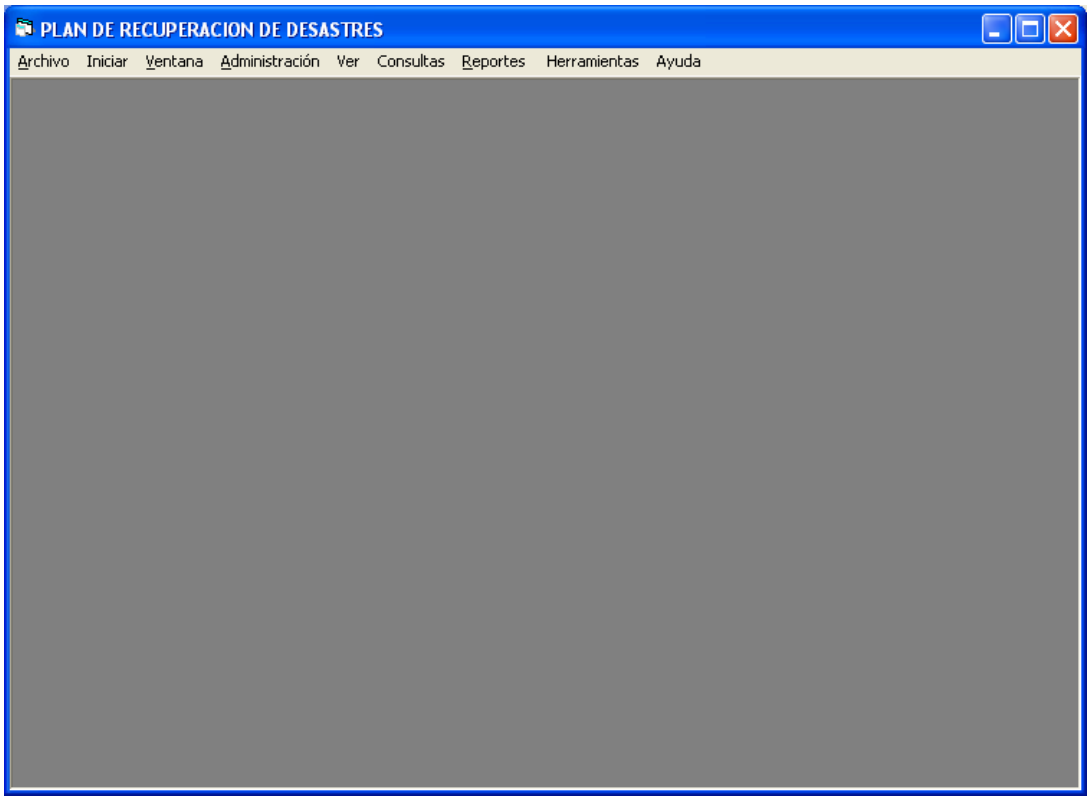
Al iniciar el sistema SOFDRP encontrara una pantalla principal desde donde se podrá acceder a los diferentes menús con los que cuenta el sistema.

Esta es la pantalla en donde el administrador del Plan de Recuperación, ingresara la información global involucrada en el Plan de Recuperación.

Mediante esta pantalla, el usuario podrá acceder a una pantalla adicional de manera directa desde el menú ventana o bien seguir el flujo de las pantallas presionando el menú Iniciar.

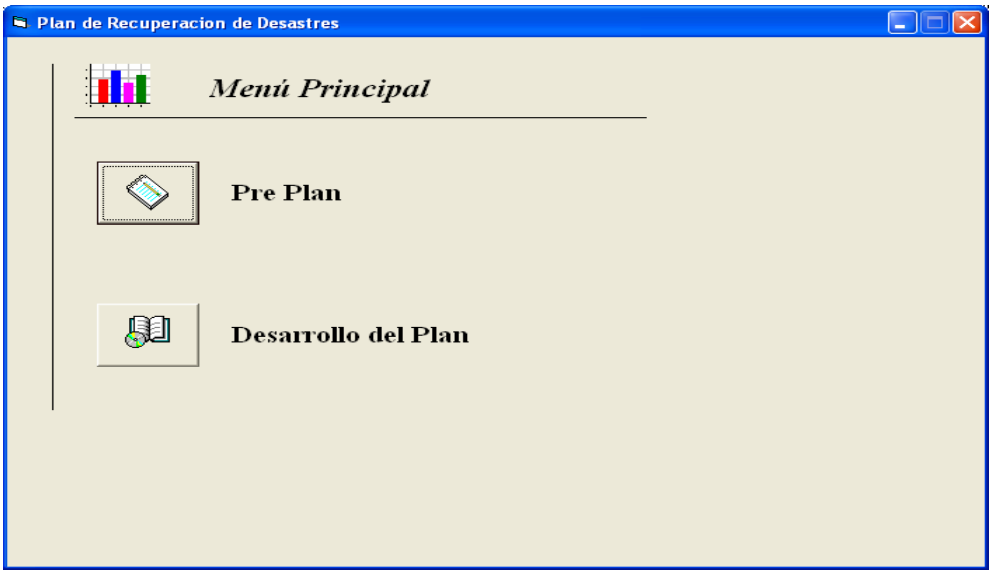
El usuario cuenta con una ayuda en línea, la cual podrá acceder a esta, presionando en el menú superior → Ayuda, o bien presionando la tecla F1.

A continuación se presenta dicha forma:



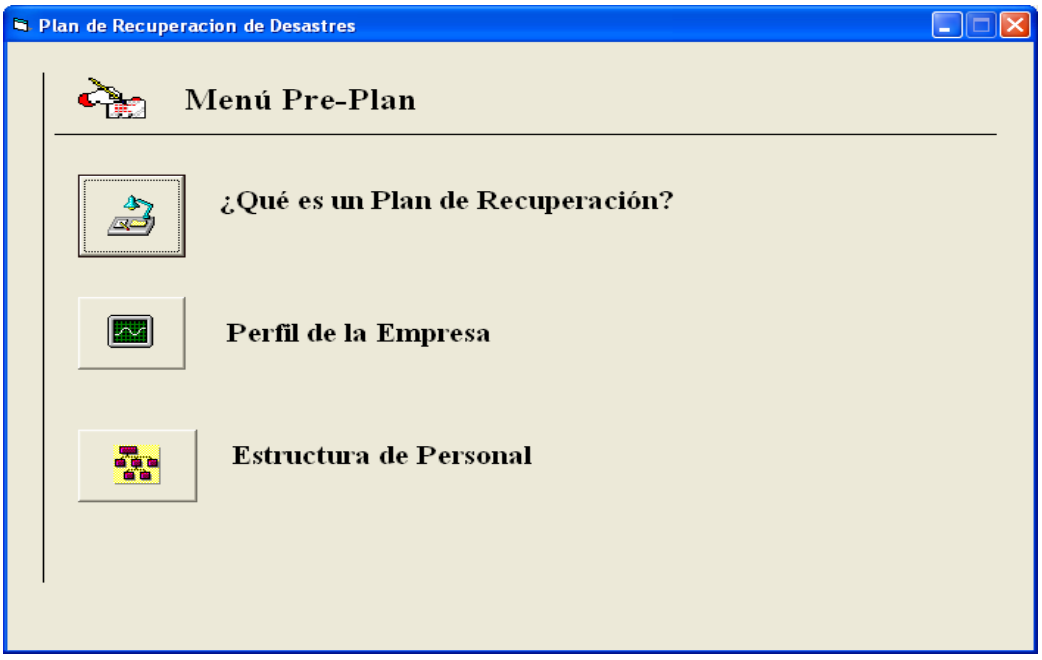
Menú Principal

Esta pantalla consiste en dos botones, llamados Pre Plan y Desarrollo del Plan. Al dar clic sobre cualquiera de estos dos botones, se obtiene un submenú correspondiente. Si no se desea continuar, entonces cierre esta ventana para pasar a la pantalla principal de la aplicación.



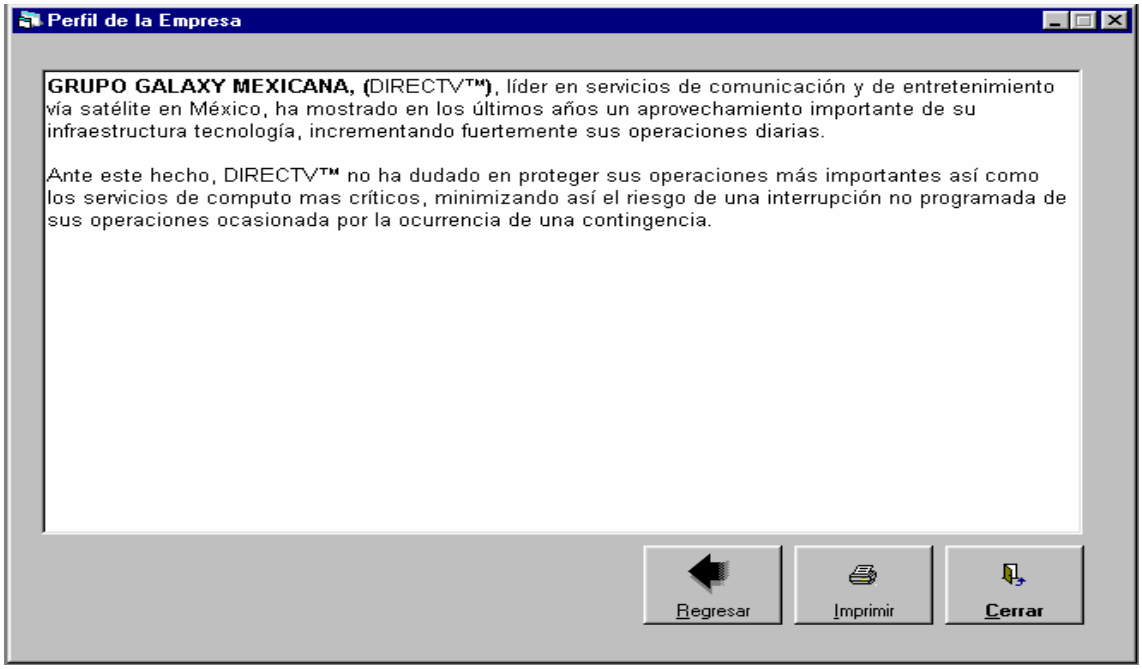
Pre Plan

La primera fase del plan de contingencia es la que se denomina Pre-Plan. En ella se menciona la definición de Plan de Recuperación y su importancia de éste dentro de la empresa.



Si elegimos la primera opción denominada que es un Plan de Recuperación nos lleva a una descripción acerca de lo que es un Plan de Recuperación.

En la siguiente opción denominada Perfil de la Empresa, se da una breve descripción de la compañía en cuestión.



Estructura Operacional de la Empresa

Al seleccionar esta opción nos aparece una segunda pantalla, la cual indica si se desea ir al directorio de empleados o de proveedores, dependiendo de la selección se presentara una pantalla de captura de personal involucrado en el Plan.

Directorio de Empleados

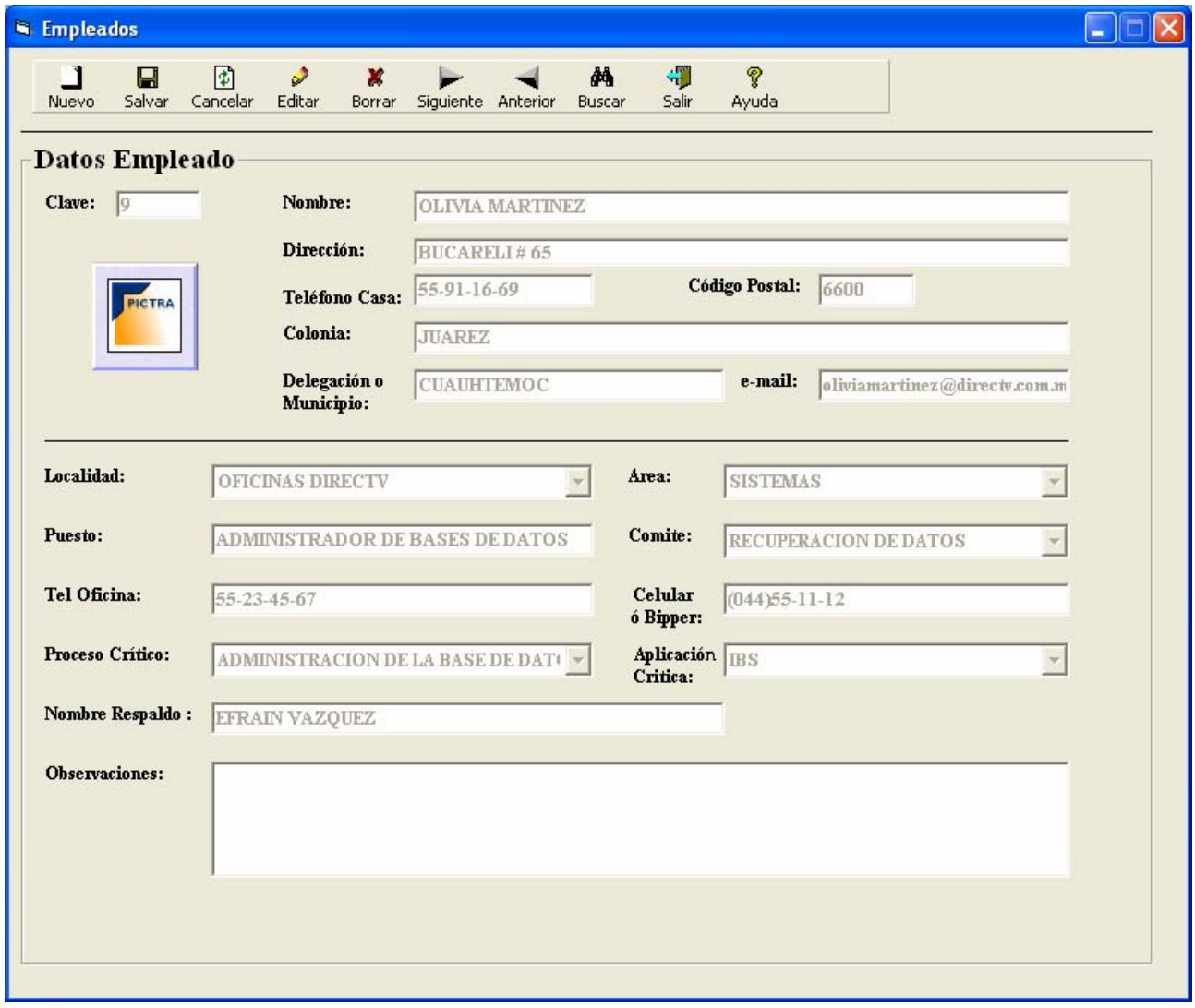
Al seleccionar esta opción, aparece la forma de empleados; en ella se podrá consultar los datos personales de cada uno de los empleados, así como aspectos que intervienen en el Plan de Recuperación.

La pantalla siguiente solicita la información de la siguiente manera:

En la primera sección se enumeran los datos personales del empleado como son:

Clave: Clave del Empleado dentro de la organización
Nombre: Nombre completo del empleado
Dirección: Domicilio particular
Teléfono casa: teléfono particular
Código Postal:
Colonia:
Delegación o municipio:
Email

Pantalla de Empleados



El sistema cuenta con la funcionalidad de que al proporcionar el campo CODIGO POSTAL el sistema automáticamente agrega la información de la colonia y de la delegación correspondiente, o bien se podrá ingresar manualmente dicha información.

En la sección de datos del empleado con respecto al Plan de Recuperación se deberá ingresar los siguientes datos:

Centro de Negocio: Centro de Negocio al que pertenece el empleado.
Área:
Puesto: El cargo que desempeña
Comité: Se deberá elegir el comité al cual el empleado pertenece
Tel. de oficina:
Celular o bipper: Teléfono móvil
Proceso Crítico: Proceso Critico al cual el empleado esta ligado
Aplicación Crítica: Aplicación Crítica a la cual se le vincula

Nombre de respaldo: Persona suplente en caso de no contar con el empleado titular
Observaciones: indica algún dato especial como puede ser horario, habilidades, etc.

Instrucciones en la captura de la información

Básicamente la funcionalidad de la barra de herramientas se encuentra en la mayoría de los formularios, por lo que se explicara en este momento esta funcionalidad con la pantalla de captura de Empleados.

Nuevo

- Presione el botón NUEVO si desea dar de alta un empleado. Al terminar presione SALVAR
- Si se esta dando de alta a un empleado, se captura los datos correspondientes y se da un clic en el botón SALVAR.

Editar

- Por el contrario, si se desea modificar los datos de un empleado ya existente, solo desplácese o proporcione la clave en el botón buscar. Una vez situado en el registro deseado dar un clic en el botón EDITAR y estará listo para poder realizar cambios, al realizar su cambio presione nuevamente el botón SALVAR para que se actualicen los datos.

Siguiente y Anterior

Navegación por los registros.

Buscar

Busca un registro de un empleado, ingresando como parámetro, la clave del Empleado

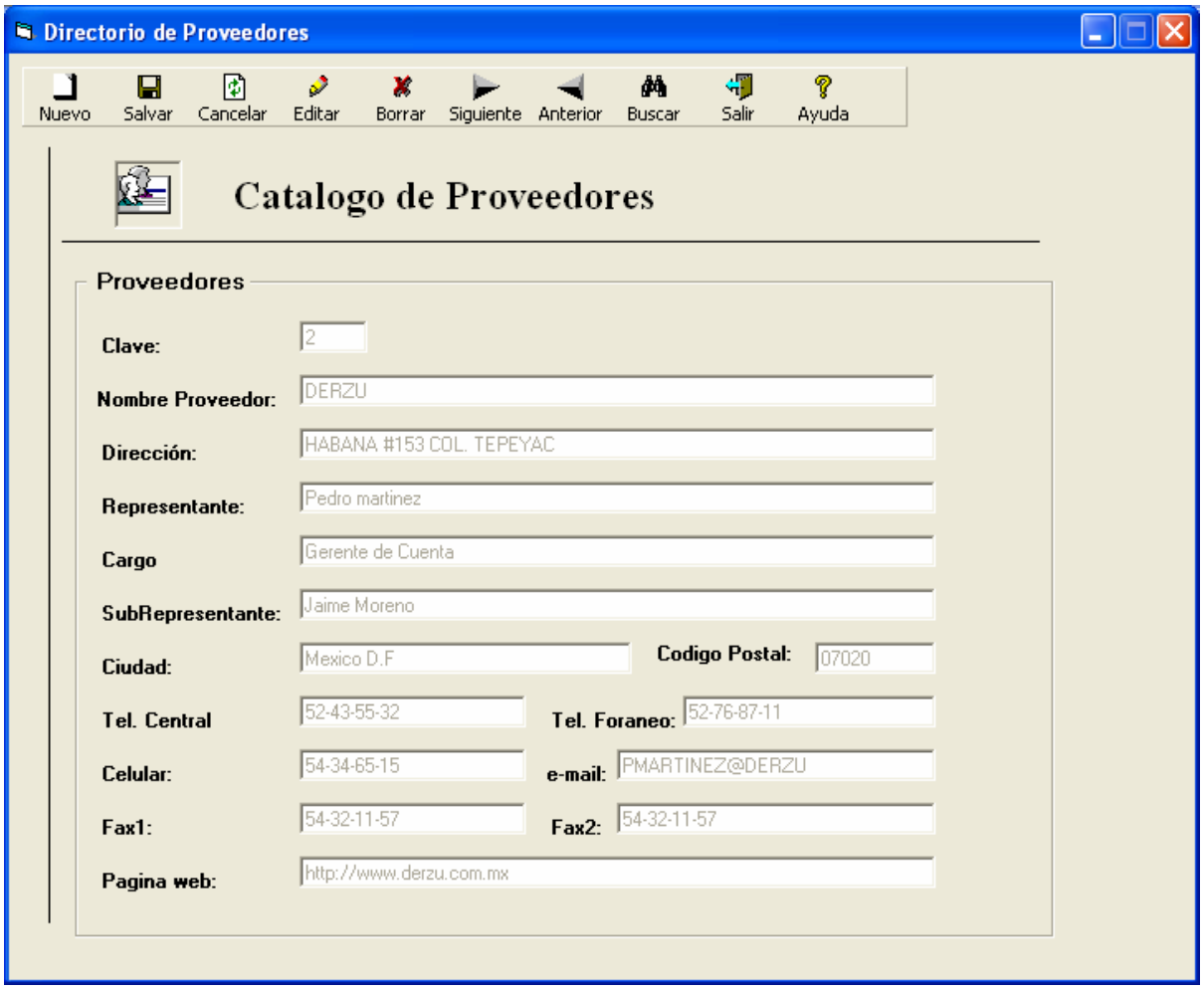
Ayuda

Presenta la ayuda en línea.

Directorio de Proveedores

En esta pantalla de captura se definen los datos de los proveedores involucrados en el Plan de Recuperación que la compañía posee.

Pantalla de Proveedores



En esta pantalla se deberá ingresar información referente a los proveedores como lo indica la forma de captura. Se deberá especificar el nombre del ejecutivo de cuenta, así como un responsable alterno con el fin de asegurar un contacto en el momento de la contingencia.

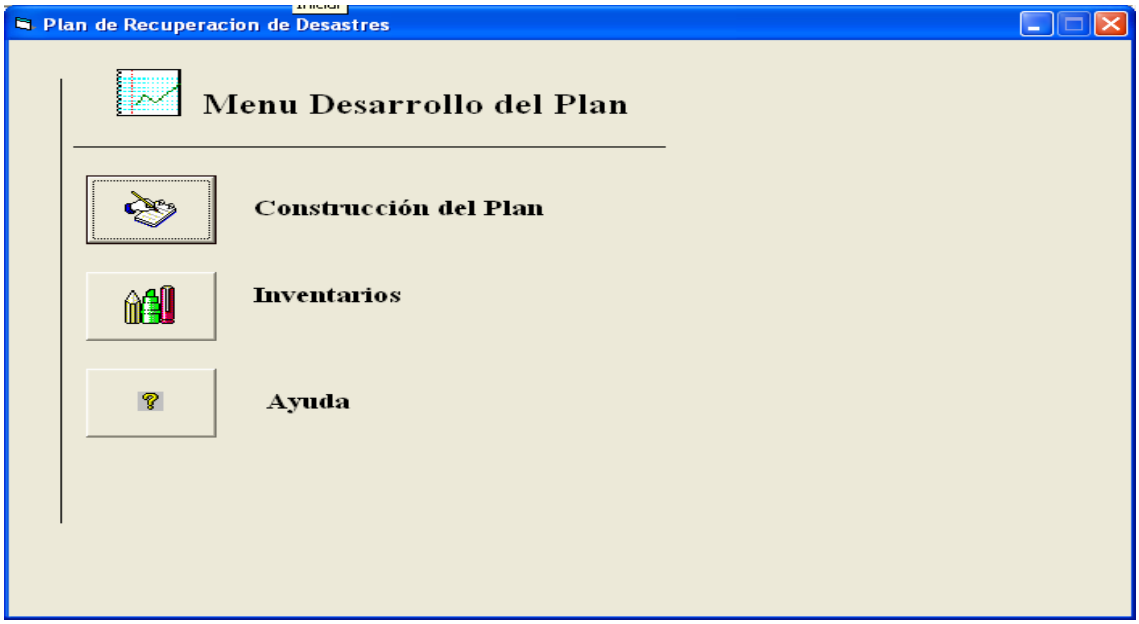
Información adicional

e-mail: Dirección de correo del empleado.
Pagina Web Donde proporciona el formato http://www. Al empezar a escribir su dirección de la pagina

Para obtener un documento impreso con los datos necesarios seleccione REPORTES del menú de la pantalla principal y en la opción proveedores dar un clic. Se presentaran los datos más necesarios.

Desarrollo del Plan

El menú que se presenta al seleccionar esta fase aparece como se muestra a continuación:



Dar clic en cualquiera de las opciones para tener acceso al submenú correspondiente:

Construcción del Plan

En esta sección se hace referencia a todos aquellos elementos necesarios para llevar a cabo el Plan de Recuperación. Los datos obtenidos son resultado de un análisis de todos aquellos procesos que se llevan a cabo dentro de la compañía, su impacto al negocio, los requerimientos del personal, equipo y comunicaciones para llevarlos a cabo, así como los procedimientos a seguir en caso de presentarse una contingencia, los documentos y respaldos necesarios para llevar a cabo la recuperación y el personal que llevara a cabo estos procedimientos.

Al dar clic en el botón correspondiente, se presenta la siguiente pantalla:

Procesos Críticos

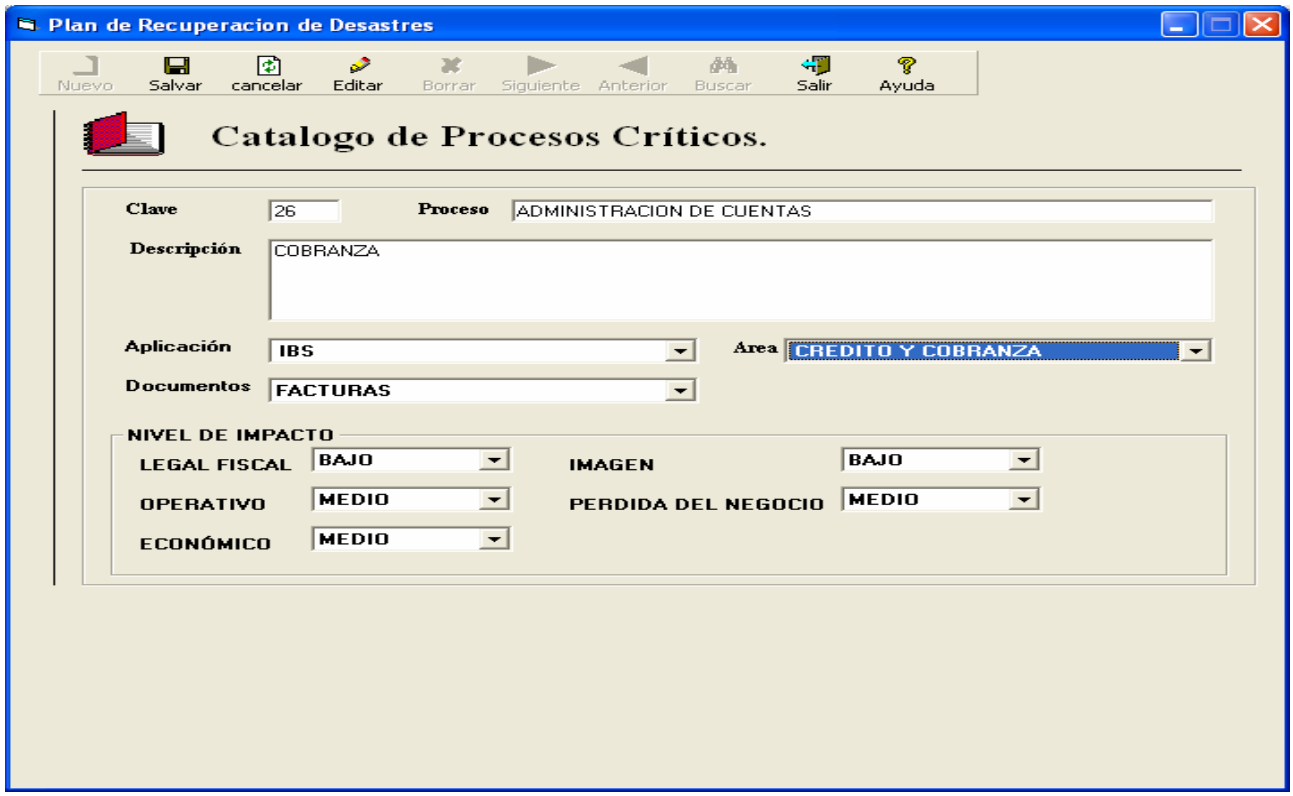
Se considera como proceso Crítico a aquel que es fundamental para la operación de la empresa, ya que al faltar este puede ocasionar grandes consecuencias, como no contar con la información oportuna para la toma de decisiones, afectar su operatividad a aquellos procesos a que dependa de él, paralizar algunas operaciones de la empresa, etc.

Se deberán ingresar los niveles de impacto para ese proceso de acuerdo a factores como Operativos, Legales, de Imagen, Económicos y de perdida del negocio.

Las variables se describen a continuación:

Alto = 3 Describe que el impacto es critico dentro de la compañía
Medio = 2 Se refiere a que el nivel de impacto es vital.
Bajo = 1 Implica un impacto sensible a la operación de la compañía
Nulo = 0 No afectara en nada las operaciones de la empresa.

La pantalla de Procesos Críticos es la siguiente:



La pantalla de Procesos Críticos Requiere de los siguientes datos:

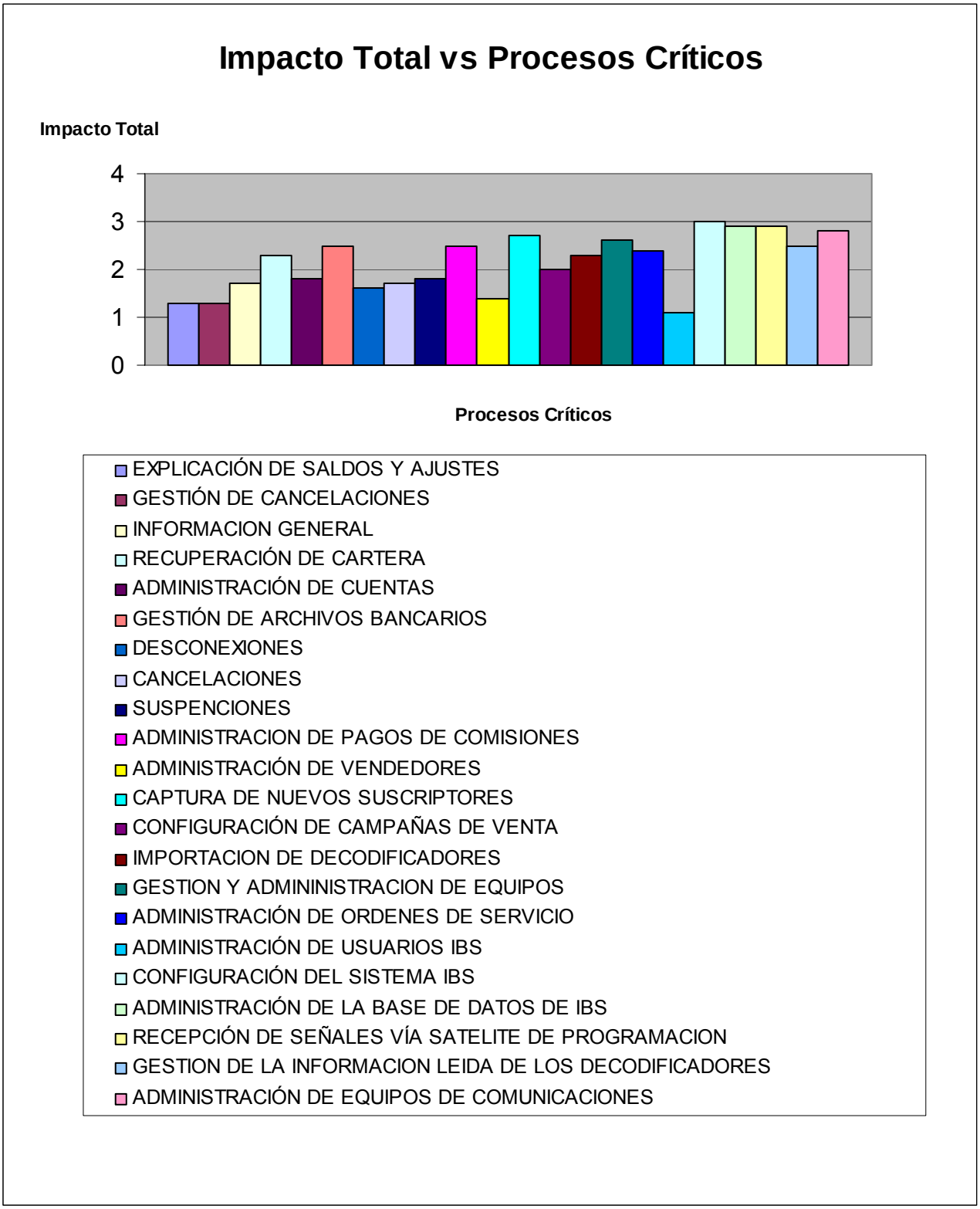
Clave: Este campo el sistema lo proporciona automáticamente al dar clic en el botón **NUEVO**
Proceso: Nombre del Proceso Crítico
Descripción: En este campo se deberá describir brevemente, el proceso y su relación con los otros procesos de la empresa, las tareas principales, etc.
Aplicación: Aplicación ligada al proceso critico en particular.
Área: Es al grupo de trabajo en el que se aplica
Nivel de Impacto: En este menú el usuario deberá calificar al proceso de acuerdo a su nivel de impacto, de acuerdo al Análisis de Impacto al Negocio se definen los niveles de riesgo desde 0 a 3 y toma los siguientes valores:

Se puede obtener un reporte impreso de los procesos críticos de la empresa y su prioridad, accediendo a la forma principal y después de seleccionar la opción reportes. Adicionalmente existe un reporte en donde se nos muestran los empleados ligados a cierto proceso crítico.

Grafica de procesos críticos

La grafica corresponde a todos los procesos críticos de sistema de respaldo SOFDRP, en la cual aparecen representados todos los impactos que determinan la criticidad para cada uno de los procesos; De esta forma se puede tener un panorama visual de cada aplicación critica con respecto a las demás. Cabe señalar que si cambiaran alguno de los criterios que determinan la criticidad de los procesos, la grafica se modifica automáticamente. Para obtener dicha grafica basta seleccionar desde el menú principal Reportes →procesos críticos→grafica.

La grafica es la siguiente:

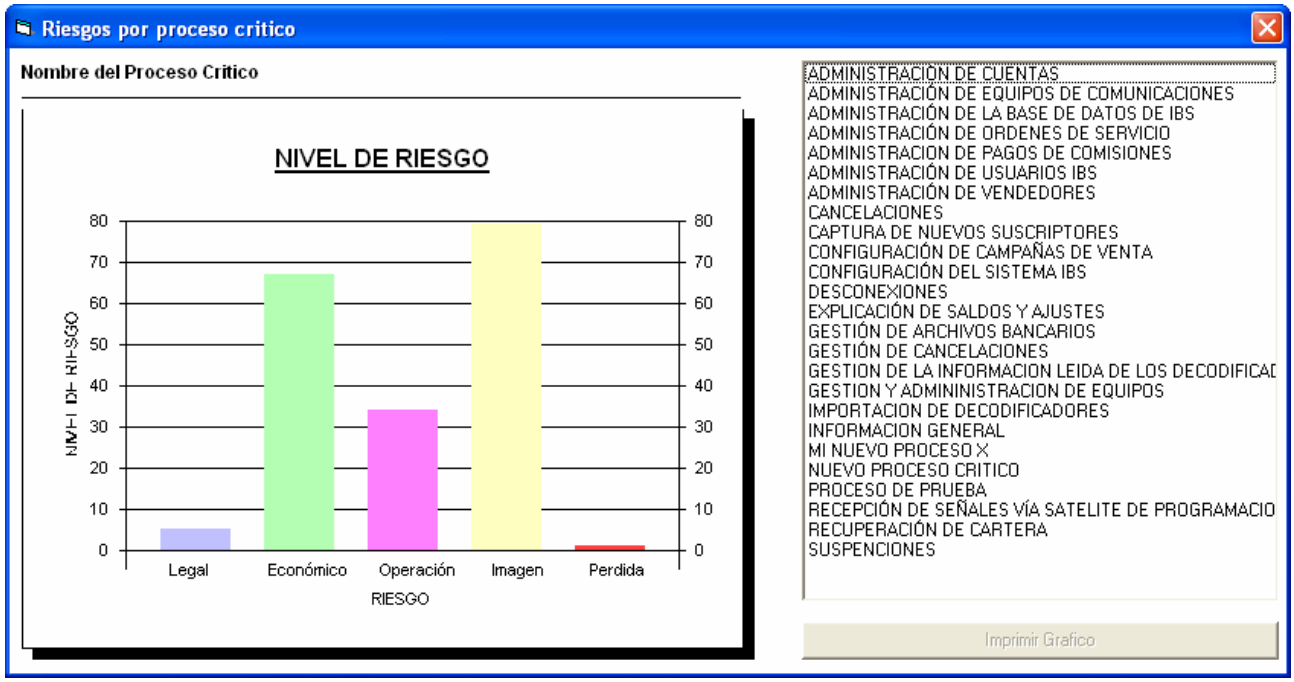


Gráfica por Proceso Crítico.

Adicionalmente el sistema cuenta con otra gráfica en la cual se puede observar las características de los Procesos Críticos analizándolos de manera individual, para identificar para cada uno de los procesos su valor de impacto, por los diferentes criterios como son:

- Impacto Legal/Fiscal
- Impacto en Imagen
- Impacto Operacional
- Impacto de Pérdida del Negocio
- Impacto Económico

La gráfica se presenta a continuación:



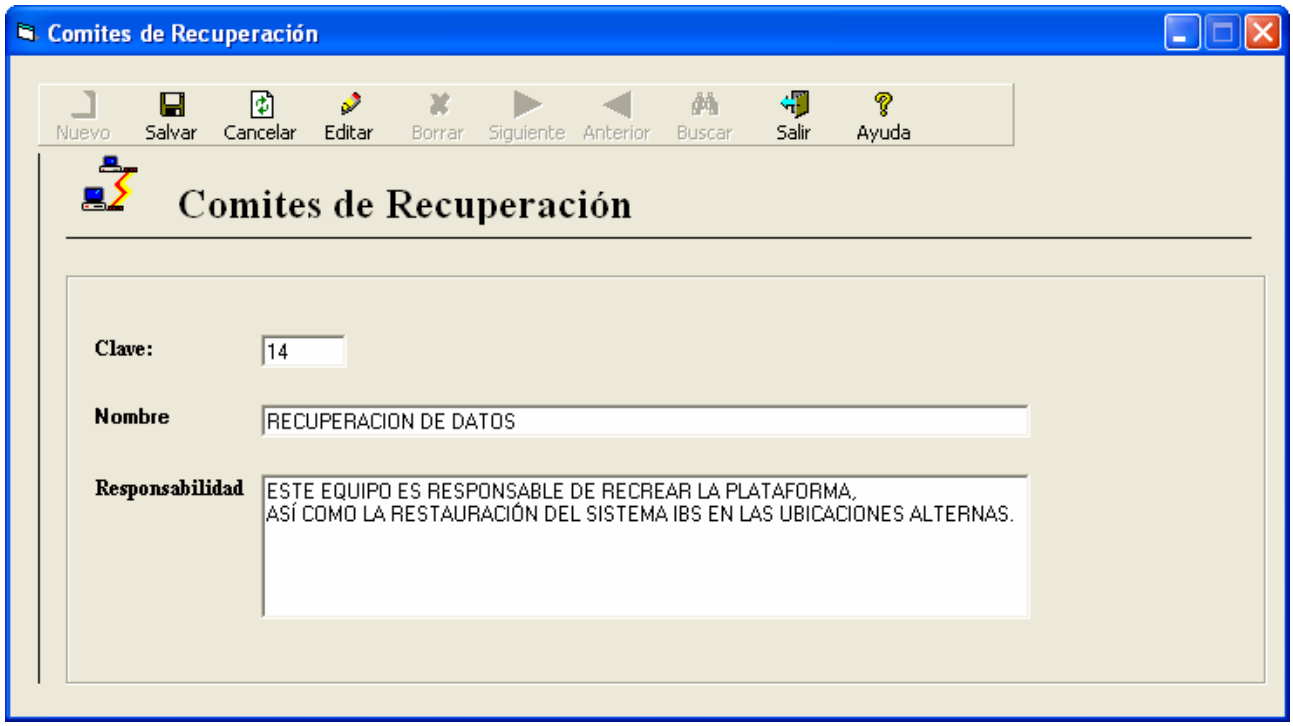
Para cada proceso seleccionado se muestra su nivel de riesgo definido por el comité administrativo del Plan de Recuperación.

Comités de Recuperación

Para lograr el objetivo del plan de recuperación se determino la formación de comités de recuperación. Un comité esta formado por un grupo de personas, las cuales realizan una serie de actividades interdependientes con miras a lograr un objetivo común: Recuperar la operatividad de en el menor tiempo posible.

Los datos requeridos en la forma de comités de recuperación son los siguientes:

Comités de Recuperación



Clave: Se refiere a la clave del comité
Nombre del comité: La identificación con que se hace referencia a este comité
Responsabilidad: Las actividades o tareas que debe de contemplar el comité.

Para proceder a registrar a los integrantes respectivos del comité, se debe dirigir a la pantalla de los empleados. Para obtener un reporte de comités el usuario deberá referirse al menú de reportes dentro de la pantalla principal.

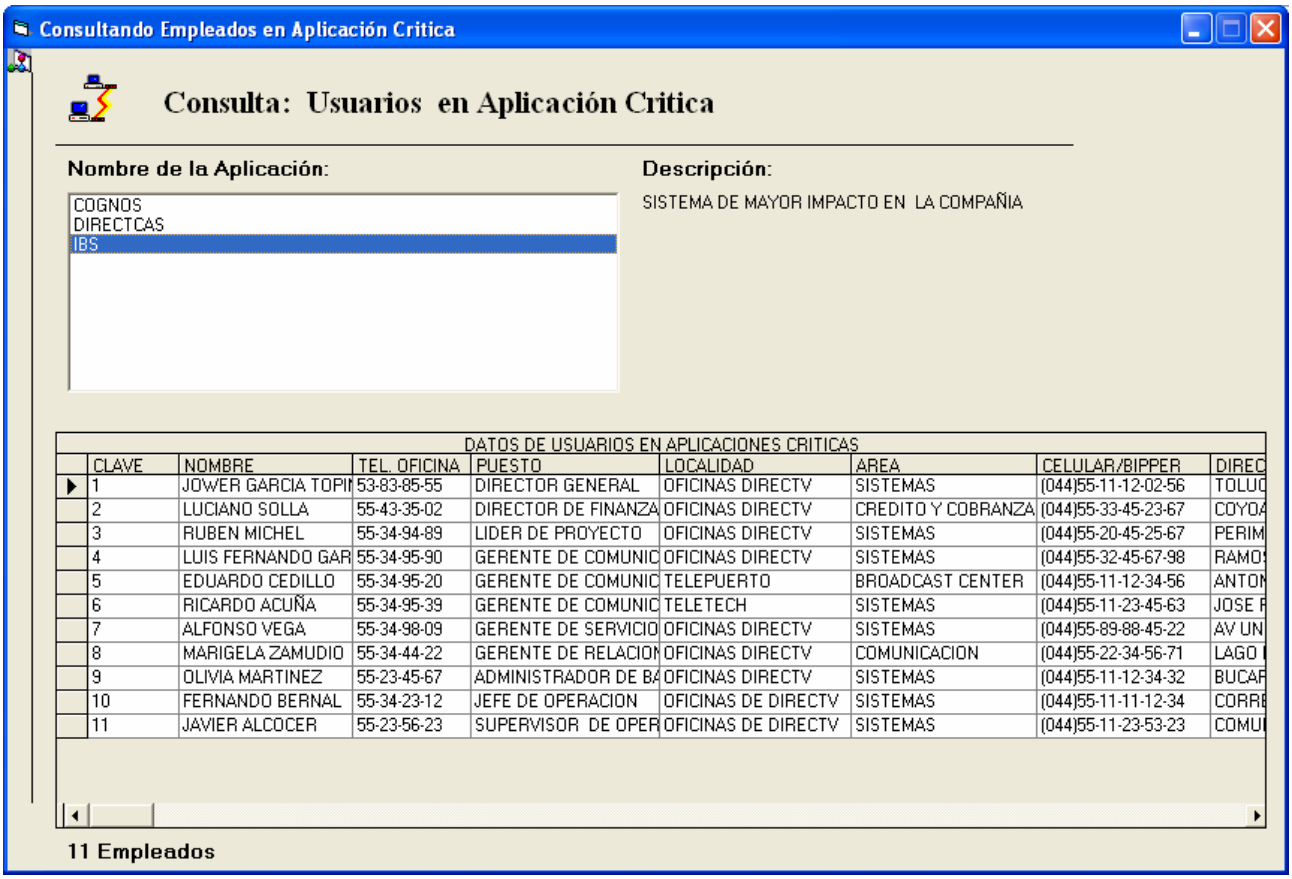
Usuarios aplicaciones criticas

Es muy importante tener el directorio de las personas que por sus funciones diarias están relacionados con las aplicaciones más críticas dentro de la compañía, esto para que en caso de una contingencia con alguna de estas aplicaciones se puedan identificar de manera rápida los

empleados que utilizan dichas aplicaciones para que se sepa en caso de activarse el plan de recuperación a que usuarios recurrir e informar para poder lleva a cabo el Plan de Recuperación.

La siguiente pantalla nos muestra lo mencionado anteriormente:

Usuarios Aplicaciones críticas



Para obtener un reporte impreso de los empleados por aplicación crítica, el usuario deberá seleccionar el menú principal, reportes, empleados, aplicación critica.

Acciones del Plan

El plan de acción es el conjunto de actividades a seguir para lograr el objetivo. Las actividades que se contemplan en el plan de acción a seguir son:

Actividades que se van a realizar antes de un desastre, por ejemplo mantener actualizados los requerimientos de usuarios para laborar en un centro de soporte alterno, los datos necesarios para comunicar el desastre y la evaluación de la criticidad de las aplicaciones.

Actividades a realizar en el momento en que ha ocurrido un desastre. Esta fase abarca desde la evaluación de la disponibilidad del personal, el estado del equipo, el estado de los sistemas de información y de la red de comunicaciones hasta declarar la contingencia

Actividades a realizar una vez activado el plan, para reinstalar las operaciones en un centro de soporte alterno. Entre las principales actividades a realizar en esta fase se encuentran: contactar con el centro de soporte alterno, acudir a la localidad de almacenamiento externo por los respaldos, disponer de vehículos para el traslado del personal, documentos y equipo e instalar el hardware y software en el centro de soporte alterno.

Actividades necesarias para operar aplicaciones criticas en el centro de soporte alterno

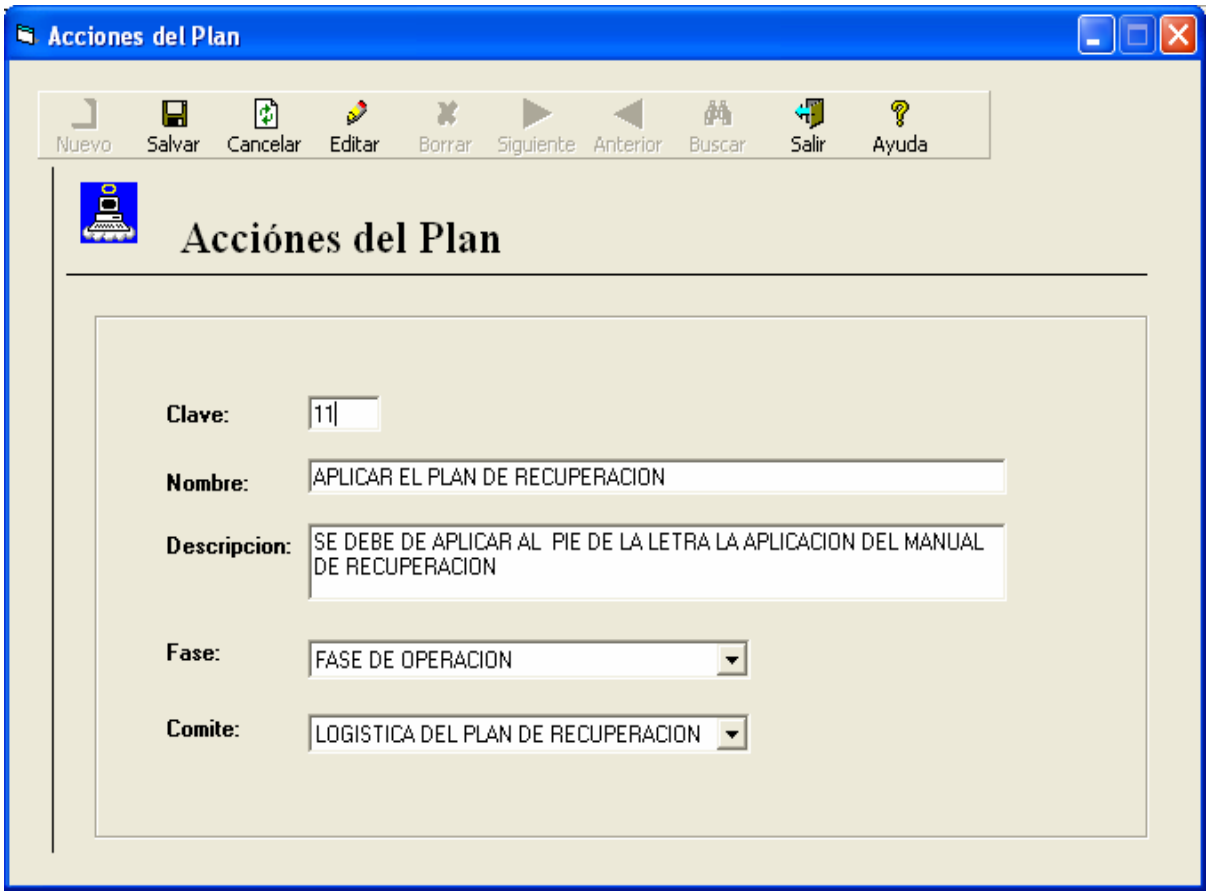
Actividades necesarias para reconstruir el Site Primario.

Actividades a realizar una vez que se declara la terminación del desastre, por ejemplo cancelar los servicios contratados, coordinar la reinstalación de operaciones en el site primario, respaldar la información procesada en centro de soporte alterno y liberar el equipo del mismo.

Los datos contemplados en esta forma son:

Clave: Se refiere a la clave de la acción a realizar
Nombre: Nombre de la acción a realizar dentro del Plan de Recuperación
Descripción: Breve Descripción de la acción a realizar
Fase: Fase a la que pertenece esta acción en particular.

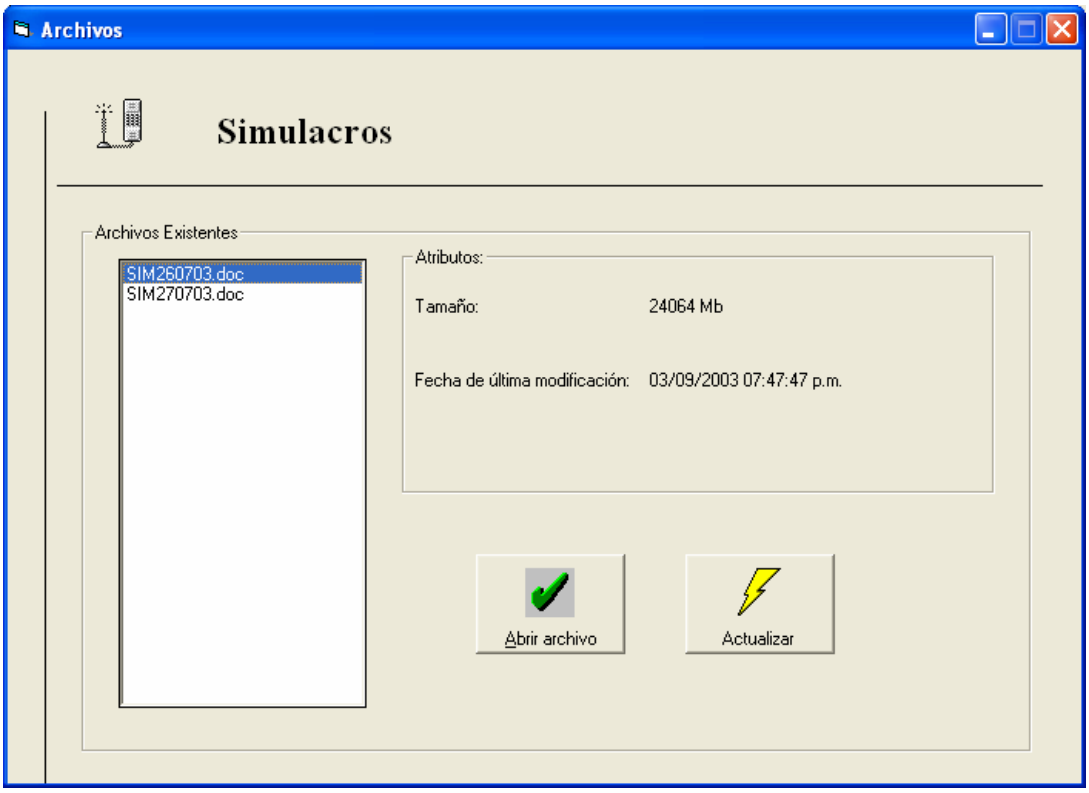
Existen tres fases dentro del plan de contingencia: La fase de preparación (FP), La fase de operación (FO) y la fase de reinstalación (FR)
Comité: El equipo que será el responsable de realizar dicha acción



Simulacros

En este módulo el administrador podrá acceder a los documentos relacionados a los simulacros realizados, con el fin de llevar un control de dichos simulacros.

La pantalla de visualización de los simulacros es la siguiente:

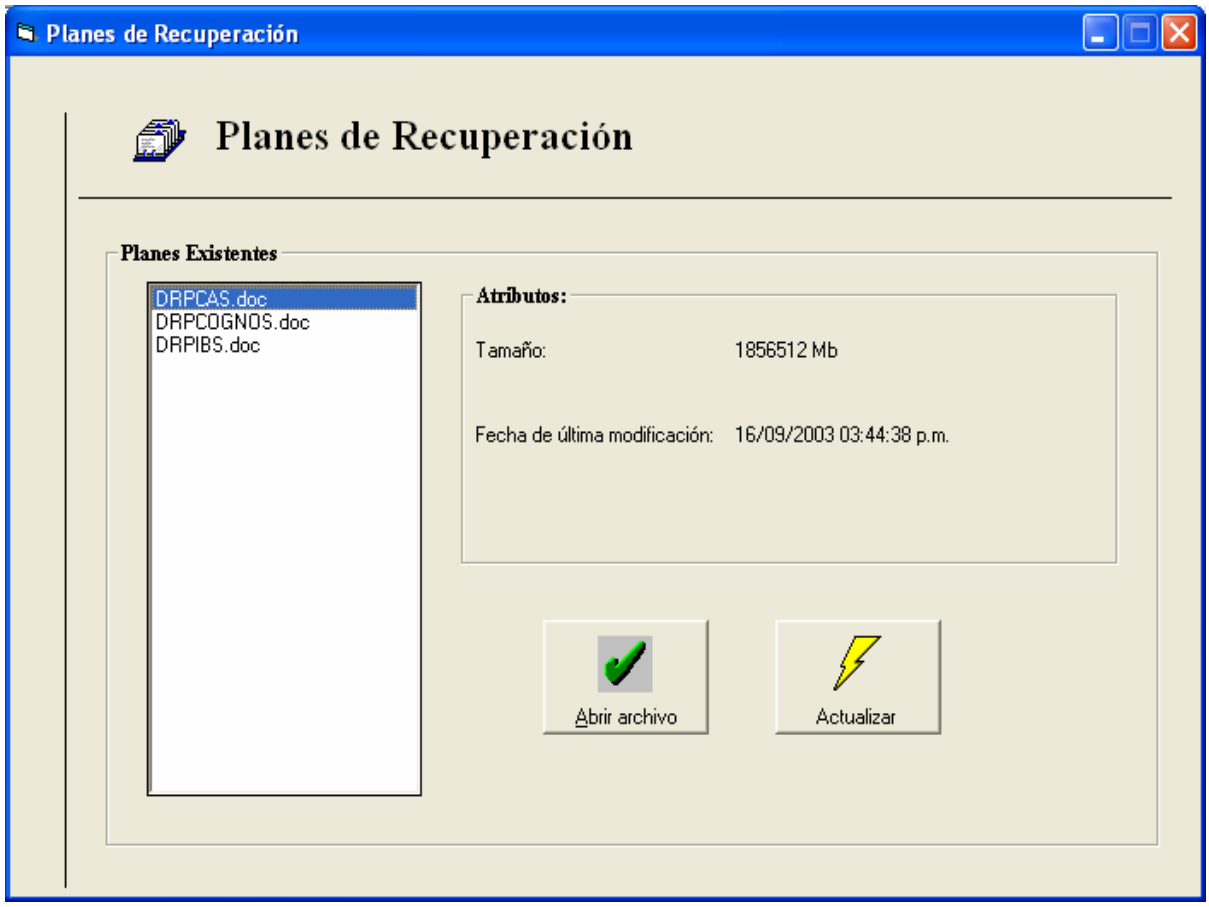


El usuario al elegir el nombre del documento relacionado al simulacro de lado derecho se presentan una serie de propiedades del simulacro, para acceder al documento relacionado con un simulacro en particular, el usuario deberá seleccionar el documento y después abrir el documento para ver los detalles del simulacro realizado. El icono correspondiente a actualizar tomara las propiedades más actuales del documento.

Planes de Contingencia

Este módulo permite la visualización de los documentos escritos que describe de manera integral los planes de recuperación desarrollados. El usuario podrá observar la versión del Plan de Recuperación. Además de que el usuario podrá elegir que documento visualizar.

La pantalla se muestra de la siguiente manera:



En este ejemplo se muestra que existen tres Planes de Contingencia escritos, los cuales el usuario puede acceder a estos de manera directa, así como administrarlos de una manera centralizada.

Pantalla Desarrollo del Plan

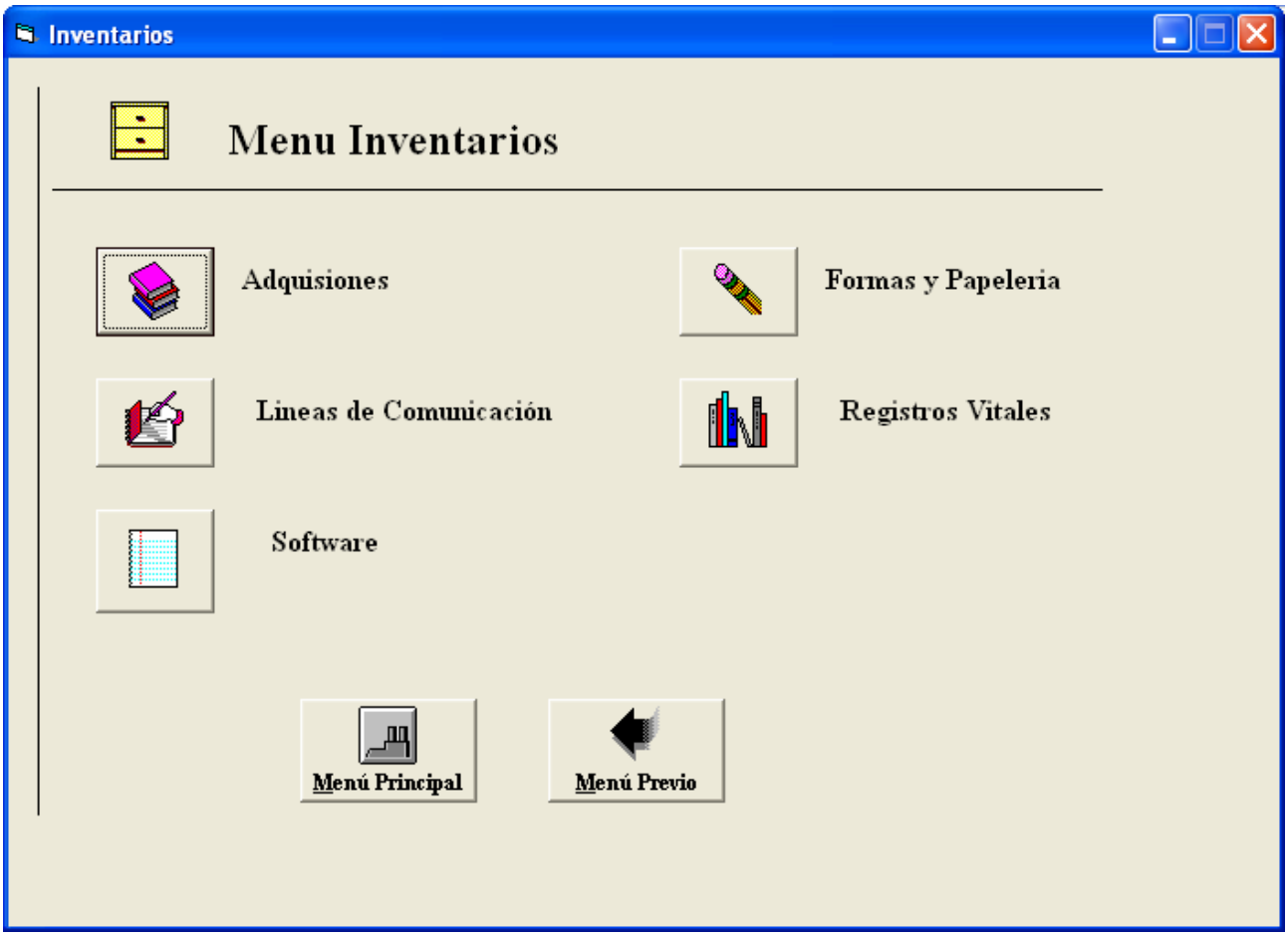
En este módulo el usuario podrá elegir dos submódulos

a) Construcción del Plan

b) Módulo Inventarios

Pantalla de Inventarios

Al seleccionar este módulo el administrador del Plan de Recuperación podrá acceder a los menús que se mencionan a continuación:



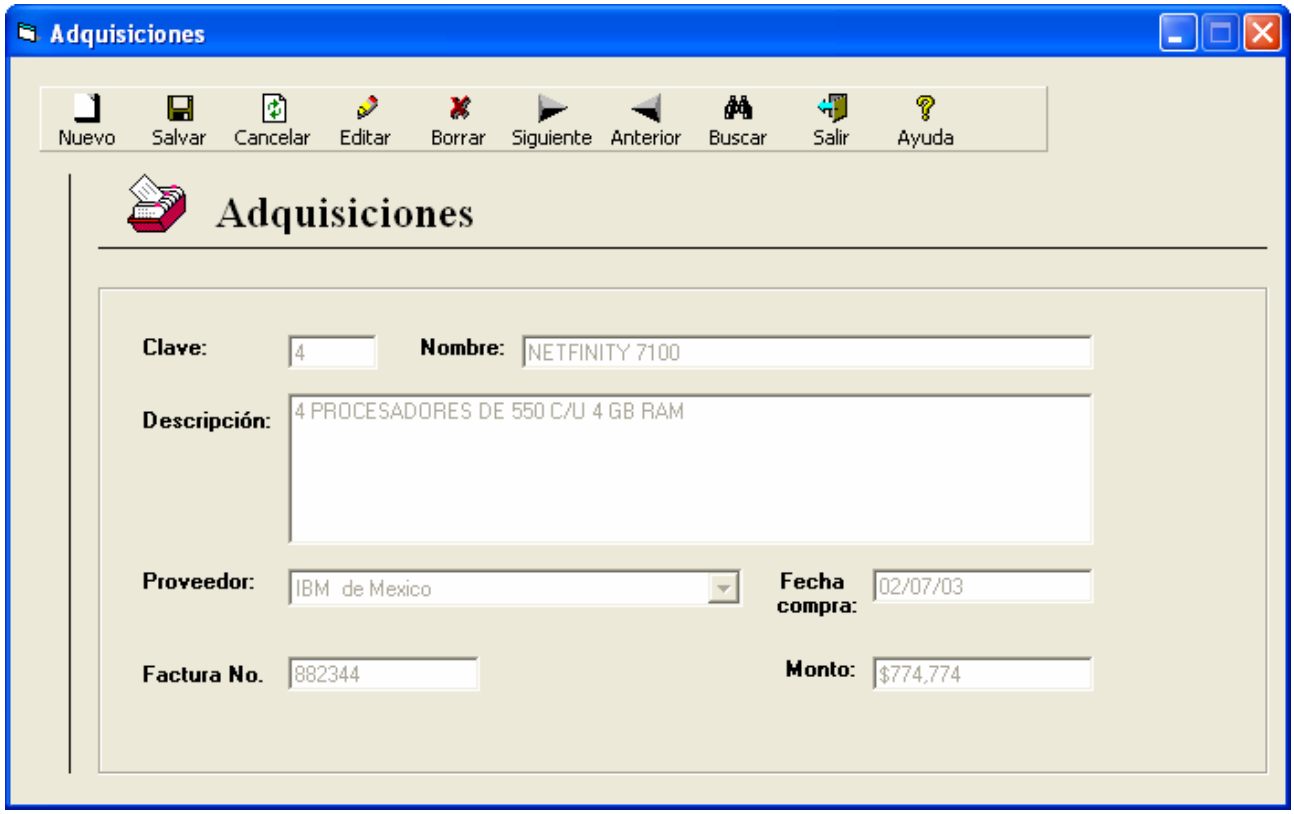
Al dar clic En la primera opción que es el botón de adquisiciones nos muestra el formulario siguiente:

Adquisiciones

En esta pantalla se lleva a cabo el registro de las compras que se realizan, en cuanto el equipo o materiales para el funcionamiento en caso de una contingencia. Una descripción de los materiales, especificando los siguientes campos:

Clave: La cave que identifica la adquisición
Nombre: Nombre de la adquisición
Descripción: Una breve información a cerca de la adquisición
Proveedor:
Fecha de Compra: La fecha en que se realizo la compra
Factura. Código de factura para cualquier aclaración posterior con el proveedor
Monto: El costo del material.

La pantalla es la siguiente:



Para obtener el reporte deseado sobre las compras diríjase al menú principal en la opción reportes adquisiciones

Líneas de Comunicación

Describe las características de cada uno de los enlaces de las líneas de comunicación, su tipo, el origen y el destino de las mismas. La información solicitada es:

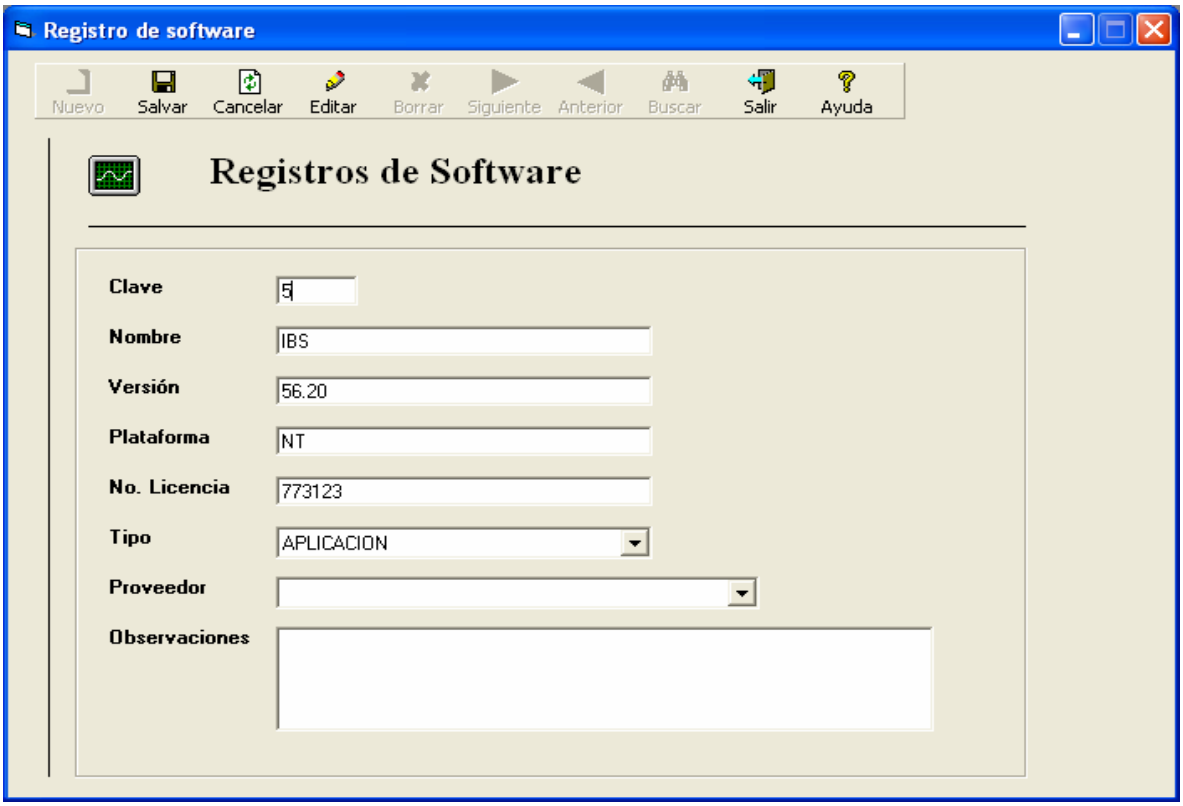
Líneas, Medio de Enlace, Velocidad, localidad origen y localidad destino: Se debe de capturar la identificación de la línea, el medio. Se puede proporcionar también otros datos como la velocidad conque la línea de comunicación opera, localidad origen y localidad destino.

La pantalla para registrar las líneas de comunicación es la que se muestra a continuación:

Para obtener un reporte impreso acerca de las líneas de comunicación existentes diríjase al menú principal en la opción reportes líneas de comunicación

Software

Es también importante tener en cuenta el tipo de software con el que opera a compañía.



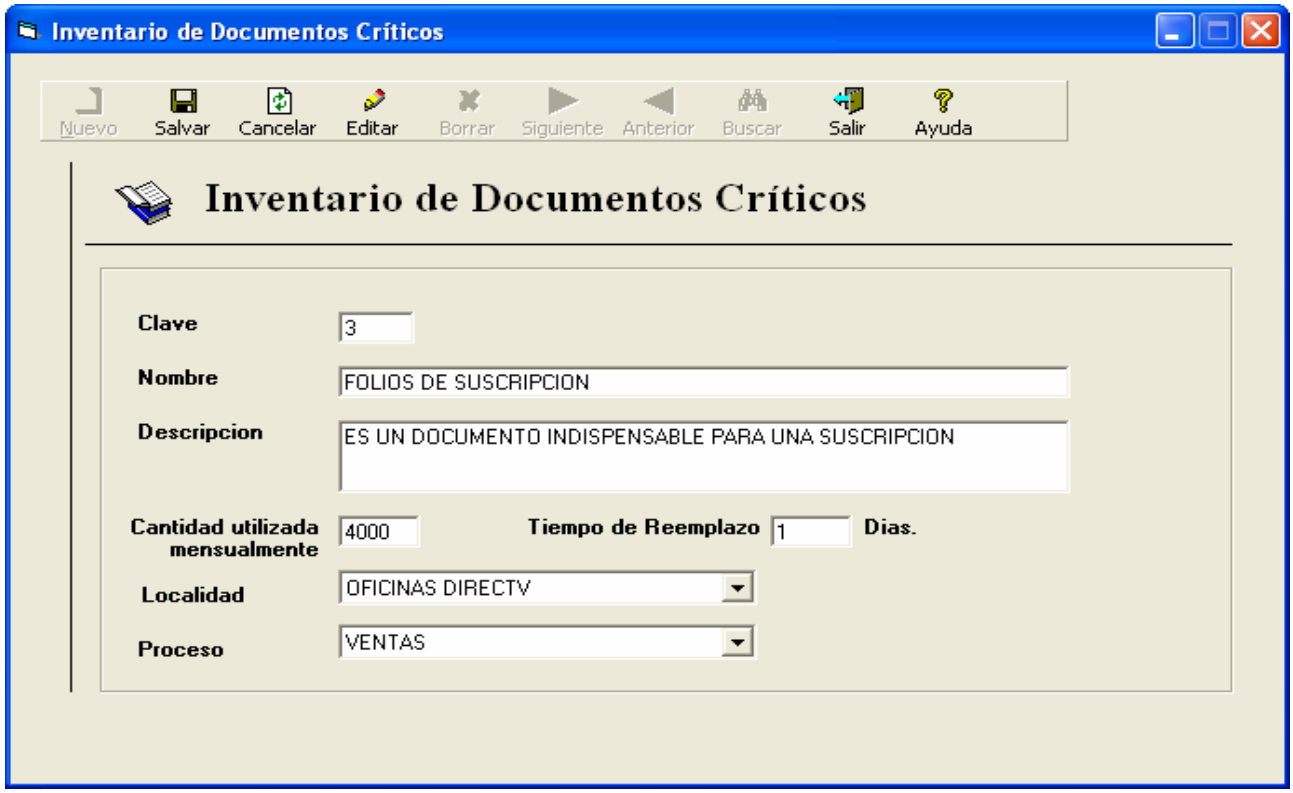
Los campos que se solicitan son los siguientes:

Clave: Clave del software
Nombre: Nombre del Software o aplicación critica
Versión: Especifica la versión
Plataforma: Especifica la plataforma del software
No. Licencia:
Observaciones: comentarios adicionales.

Inventario de Formas y documentos críticos

Esta forma sirve para tener una relación de cada una de las formas y/o documentos críticos por ejemplo (facturas, notas de crédito, cheques, folios de venta, etc.). Es importante tener presente esta información para ligar dicha información con los procesos críticos a fin de evaluar cuales procesos críticos utilizan dichos documentos, para estar preparados ante una contingencia.

Pantalla de Inventarios de Documentos Críticos



Para acceder al reporte de Documentos, se encuentra en la pantalla principal, menú reportes y documentos preimpresos

Registro Vitales.

Un registro vital consiste en información necesaria para iniciar el proceso de recuperación después de ocurrida una contingencia. Esta información puede estar contenida en cintas, disquetes, microfilm y/o documentos.

Es importante que estos registros vitales estén almacenados en un lugar externo a sistema de respaldo SOFDRP con el fin de asegurar el fácil y seguro acceso a estos y se pueda recuperar la operación de la empresa lo más pronto posible.

Los datos que se requieren son:

Clave: Identifica al registro vital
Nombre: Nombre del registro vital
Localidad: En este campo se especifica en que lugar externo se encuentra almacenado el respaldo, para su fácil localización.
Aplicación: Aplicación relacionada

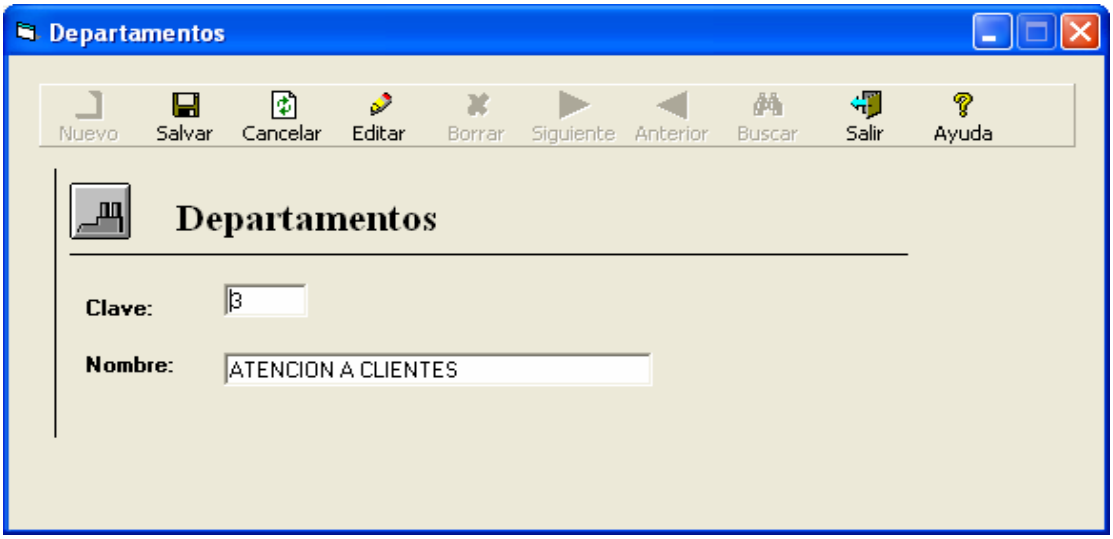
Frecuencia: Se nos da escoger entre varias opciones de la frecuencia con que se realiza el respaldo, es decir, diariamente, semanalmente, etc.
Medio: Se debe especificar en que tipo de dispositivo almacenamiento se encuentra respaldada la información, es decir si se respalda en cintas y en que tipo de cintas, disquetes, etc.
Cantidad: Muchas veces el respaldo de la información se encuentra guardado en varios dispositivos de almacenamiento, por lo cual es importante decir él Número de discos, cintas, etc. Que se utilizaron para el respaldo.
Fecha de Realización: Es la fecha en que se realizo el respaldo, para de esta forma saber la antigüedad del mismo.
Se puede imprimir un reporte de los registros vitales existentes en la aplicación dando clic en el botón llamado reporte de la pantalla principal en el módulo de reportes.

Menú Administración

Existen pantallas dentro del sistema ubicadas en la pantalla principal, en el menú de administración, en donde el administrador del Plan de Recuperación tendrá la posibilidad de crear nuevos elementos que intervienen en el Plan, como por ejemplo:

Departamentos dentro de la organización
Fases dentro del Plan
Líneas de comunicación
Medios de almacenamiento
Centros de Negocio
Medios de Transmisión
Tipos de respaldos

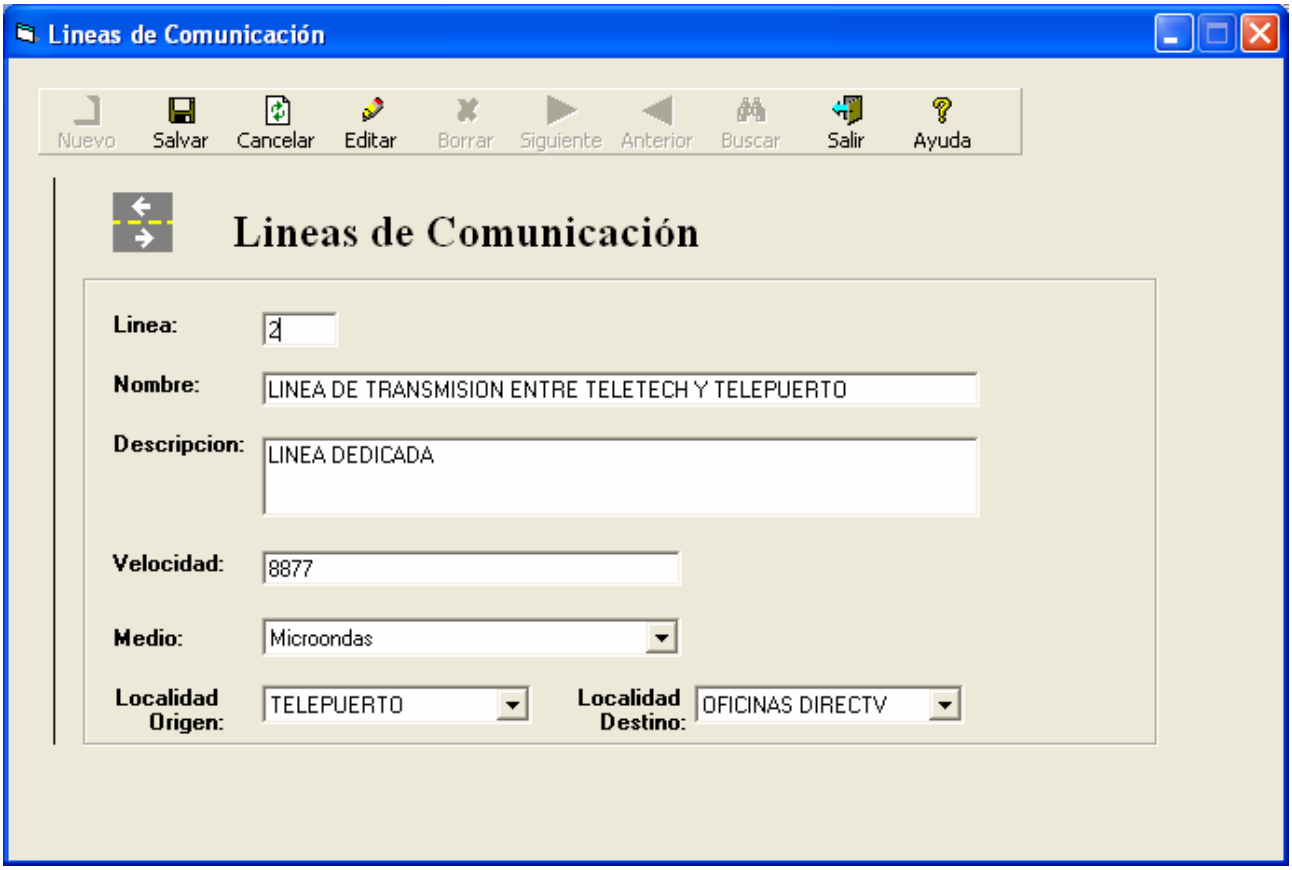
Departamentos dentro de la organización



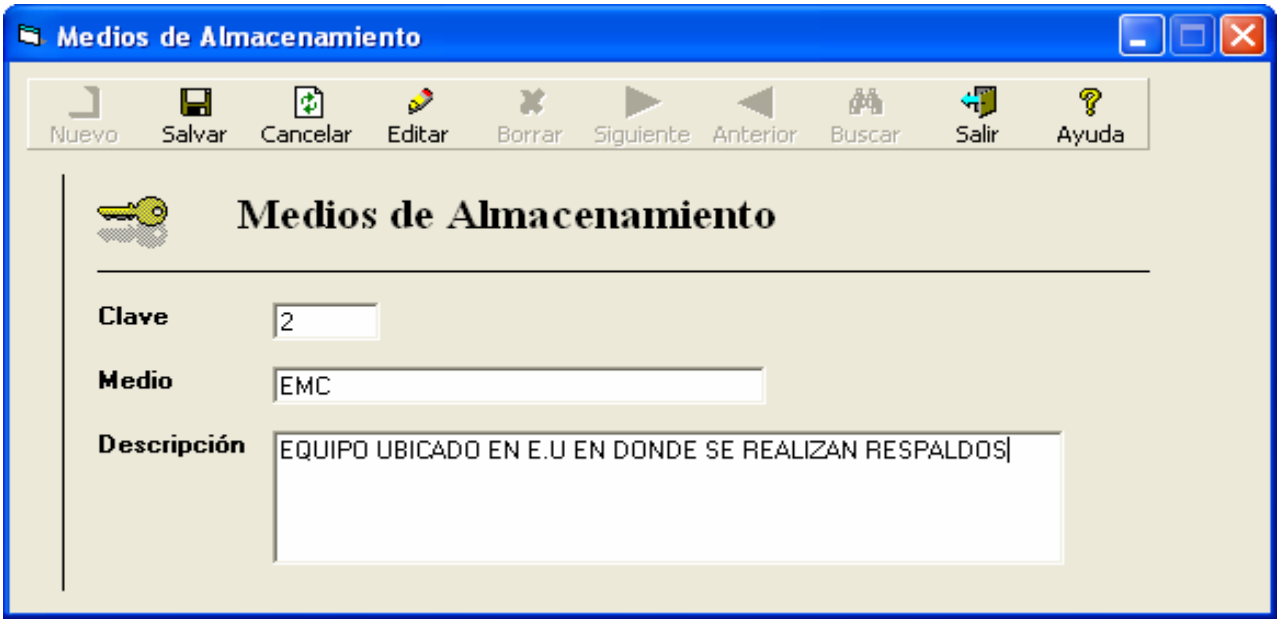
Fases dentro del Plan

Líneas de comunicación

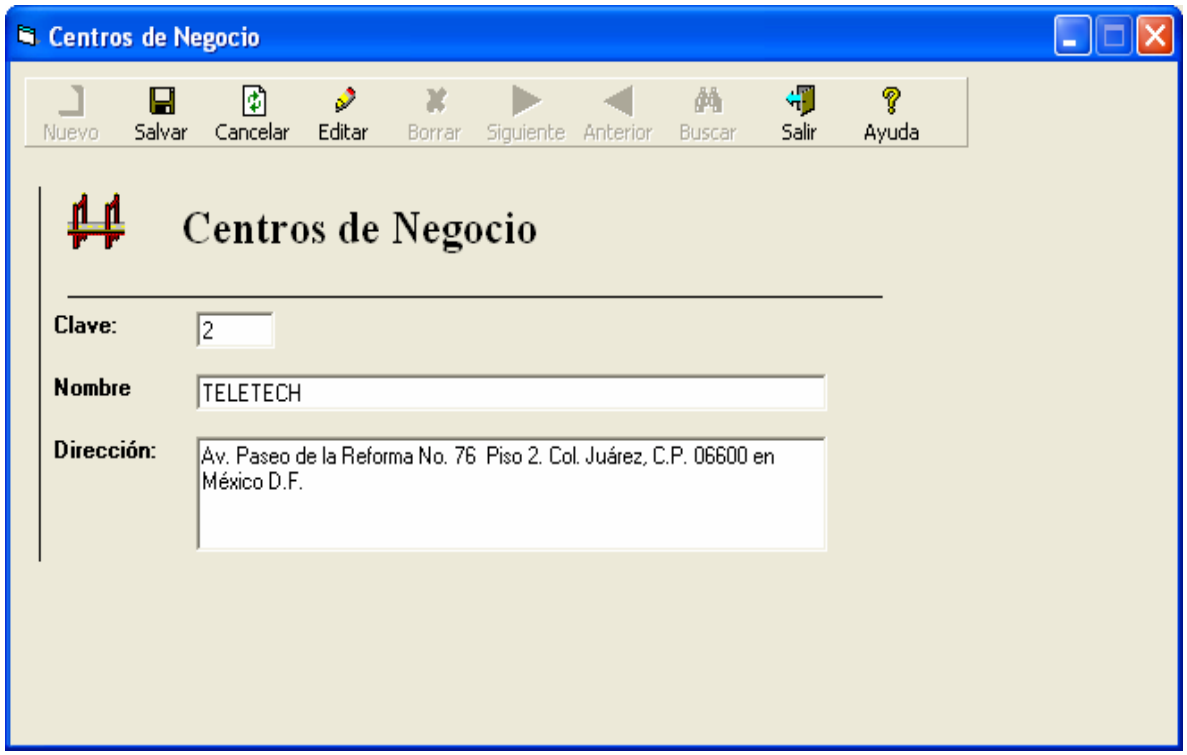
En la siguiente pantalla de captura, es necesario especifica una clave, un nombre que identifica a la línea de comunicación y una serie de características más como: velocidad, medio de transmisión, así como localidad origen y localidad destino



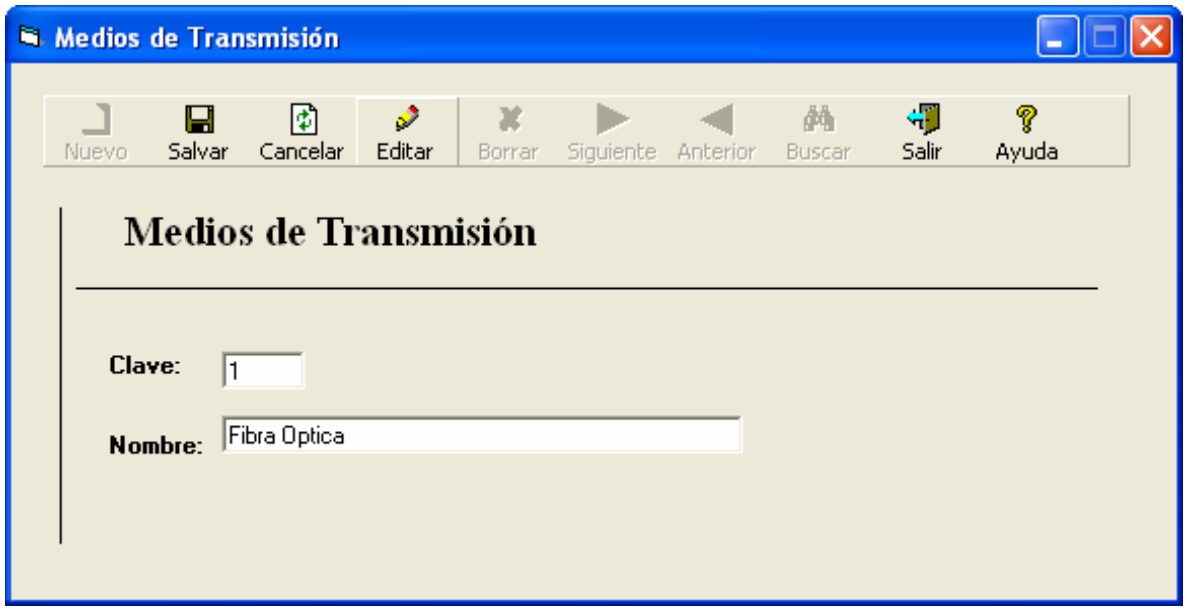
Medios de almacenamiento



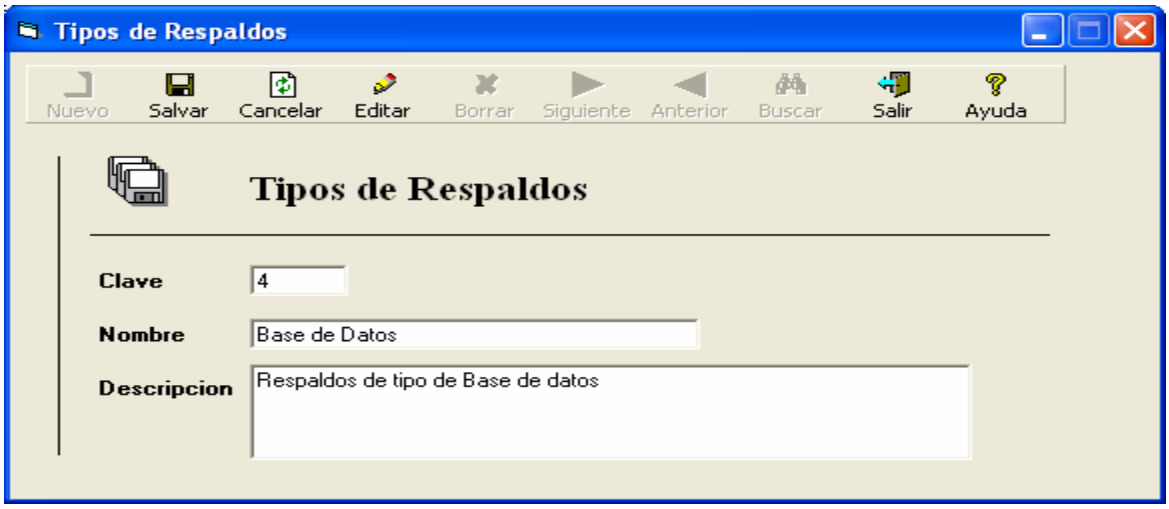
Centros de Negocio



Medios de Transmisión

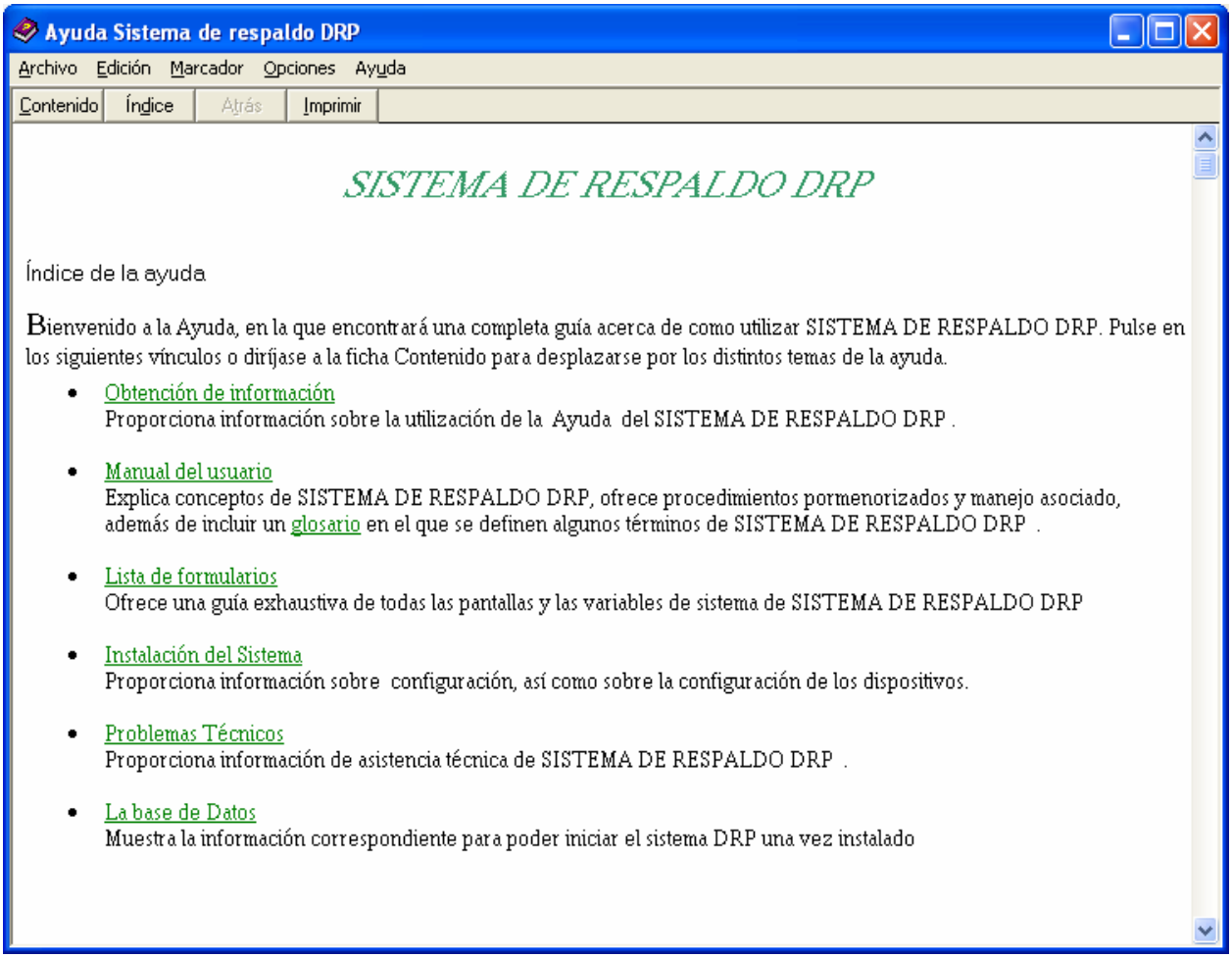


Tipos de respaldos



Ayuda

El sistema presenta la ayuda en línea, la cual mostrara información sobre edición, y navegación de los registros, así como también se completará con la ayuda escrita anteriormente.



Glosario

B

Business Continuity Planning (BCP)

Se trata de un documento que contiene una serie de procedimientos que se desarrollan, se ejecutan y se mantienen al día con el objetivo de que la empresa este preparada ante una situación no deseada.

Business Impact Analisis (BIA)

Provee la base para las prioridades de planeación de la recuperación, así como de la selección de estrategias de recuperación que reflejen un balance óptimo entre las inversiones por la planeación de la recuperación, los riesgos y exposiciones potenciales.

C

Caballos de Troya

Se le denomina caballo de Troya a un rango de amenazas de códigos malévolos que incluye virus, bombas, gusanos, etc. Este se instala por sí mismo en una máquina y hace el trabajo del programador desconocido.

Centro de Soporte Alterno

Se le denomina así a otro lugar de trabajo donde se cuente con las instalaciones y el equipo de cómputo adecuado que soporten la reactivación de los sistemas de información prioritarios para la empresa.

Cifrado

Proceso para ocultar la información contenida en un mensaje.

Códigos Bomba

La mayor parte de los virus destructivos también funcionan como códigos bomba. La idea de los Códigos bomba es que en una determinada hora y fecha, o basados en una secuencia de operaciones de la máquina, éste se disparará realizando su sucio trabajo.

D

Disaster Recovery Planning (DRP)

Se trata de un documento que contiene una serie de procedimientos que se desarrollan, se ejecutan y se mantienen al día con el objetivo de que la empresa este preparada ante una situación no deseada.

Dumpster Diving

Se le llama así a la acción de hurgar entre material informático (disquetes, cd´s, etc.). Con el fin de encontrar información importante de la organización para beneficios personales.

E

Electronic Data Procesing (EDP)

En relación con el procesamiento electrónico de datos (EDP por sus siglas en ingles), significa “datos recopilados y presentados de modo que contengan un significado”.

Equipo de Recuperación.

Está formado por un grupo de personas, las cuales realizan una serie de actividades interdependientes con el fin de lograr un objetivo común: recuperar la operatividad de la empresa en el menor tiempo posible.

Escenarios de Recuperación

Se define como escenario de recuperación a la situación que enfrenta la empresa como consecuencia de un desastre

F

Firewall

Equipo dedicado que es utilizado para comunicar la red privada con la red pública. Este equipo es un ordenador especializado que controla y administra el flujo de información entre la red privada interna y el mundo exterior. (Cortafuegos). Es un dispositivo hardware y software, que conecta entre dos o más redes y permite limitar el acceso a los sistemas en los dos sentidos.

FTP

Protocolo de Transferencia de Archivos (File Transfer Protocol)

I

IBS
Es el nombre del sistema más crítico que se menciona en el caso práctico. De origen Holandés creado por la empresa Mindport es un sistema especialmente diseñado para compañías proveedoras de servicio de TV vía satélite. Business Solutions Internet

Integridad de Datos

Se define integridad como un estado inalterado, el estado de estar completo o ser divisible. El objetivo de la integridad de datos es mantener la información de los sistemas en un estado completo e inalterado.

Intranet

Red Corporativa

O

ODBC

Conectividad Abierta de Bases de Datos, tecnología diseñada para crear un conjunto común de métodos y rutinas para acceder a almacenes de datos.

P

Piggybacking

Significa llevar a cuestas a alguien, en este contexto se hace referencia a una situación en la que un usuario termina la comunicación con otro sistema; pero el puerto permanece activo en el otro sistema; entonces, otro usuario puede empezar la comunicación con este otro sistema en el mismo puerto sin pasar ningún control de seguridad

R

Router

Dispositivo hardware para redes informáticas dotado de capacidad para conmutación y con la principal finalidad de proporcionar un encaminamiento de paquetes ip.

S

SSL

Acrónimo de Secure Socket Layer. Protocolo creado por Netscape para establecer comunicaciones seguras. Una sesión SSL esta securizada gracias al uso de técnicas de criptografía basadas en clave pública.

V

VPN

Acrónimo de Virtual Private Network. Configuración lógica de una serie de componentes hardware, que permite la utilización de redes públicas para establecer canales de comunicaciones privados a los que sólo pueden acceder usuarios autorizados.

Bibliografía

Seguridad de la Información en Sistemas de Cómputo
Luis Angel Rodriguez
Editorial Ventura

Disaster Recovery Planning Managing Risk
Toigo, John William
Prentice Hall

Computer Security
Carroll John Millar
Editorial Boston

Security of Information and Data
Daler Torgeir
Editorial Horwood

A Primer for Disaster Recovery Planning in an IT Environment
Charlotte J. Hiatt
Editorial Prentice Hall

S.O.S En su sistema de Computación
Gregor Neaga, Bruce Winter
Editorial Macmillan

Disaster Recovery Planning Managing Risk
Yordon Press

Alternatives for DRP Development
Data Security Management
Toigo, John William
Prentice Hall

Bibliografía Electrónica

http://www.sungard.com
http://www.emc.com
http://www.tivoli.com
http://www.mindport.com
http://www.aimworld.com
http://www.strohl.com
http://www.ibm.com
http://storagecentral.com
http://argus-systems.com
http://salixgroup.com