INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

Guía Práctica para el Desarrollo de Planes de Contingencia de Sistemas de Información

Lima, Febrero 2001

Elaboración	:	Sub-Jefatura de Informática
Impresión	:	En el Taller Gráfico del Instituto Nacional de Estadística e Informática
Diagramación	:	Centro de Edición del INEI
Edición	:	250 Ejemplares
Domicilio	:	Av. Gral. Garzón Nº 658 Jesús María, Lima 11
Orden Nº	:	924 - OTDETI - INEI
Depósito Legal	:	1501132001-0897

Presentación

El Instituto Nacional de Estadística e Informática (INEI), en el marco de Promoción y Difusión de las Nuevas Tecnologías de Información, pone a disposición de las entidades públicas, privadas, estudiantes y público en general, la publicación titulada: Guía Práctica para el Desarrollo de Planes de Contingencia de Sistemas de Información.

La presente publicación forma parte de la colección Seguridad Informática. Hace una breve introducción a los Sistemas de Información que incluye: La metodología práctica para el desarrollo de planes de contingencia de los sistemas de información que comprende: la identificación de riesgos, Calificación de la probabilidad de que ocurra un riesgo, Evaluación del impacto en los procesos críticos y la creación de estrategias de contingencias.

Los Planes de Contingencias le permitirán mantener la continuidad de sus sistemas de información frente a eventos críticos, de su entidad y minimizar el impacto negativo sobre la misma, sus empleados y usuarios. Deben ser parte integral de su organización y servir para evitar interrupciones, estar preparado para fallas potenciales y guiar hacia una solución.

El INEI realiza con esta publicación un aporte muy especial para todos los sectores de nuestro país, para garantizar en todo momento la continuidad de los Sistemas de Información, por ello pone a disposición la presente publicación, esperando una vez más contribuir en el desarrollo de la Sociedad de la Información.

Gilberto Moncada Vigo
Jefe
Instituto Nacional de Estadística
e Informática

Contenido

Capítulo I : Definiciones y Alcances

1. Introducción

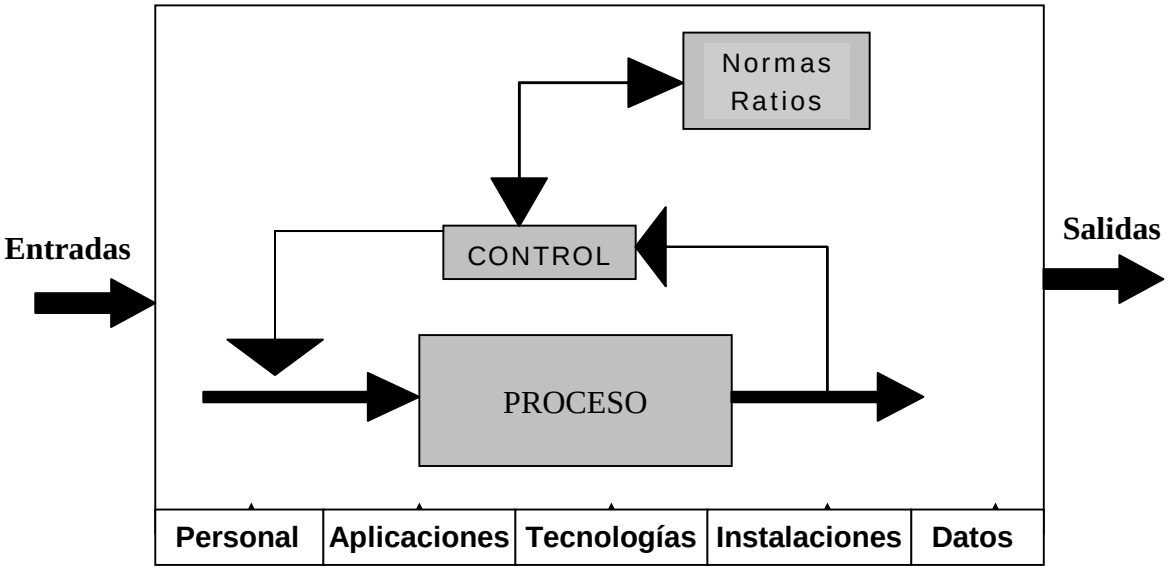
Durante varias décadas, los japoneses han desarrollado diversos programas para enfrentar los terremotos que permanentemente tienen lugar en su país. Su trabajo de preparación y contingencias no sólo ha consistido en construir infraestructura capaz de resistir los movimientos telúricos, sino que también ha contemplado un amplio proceso de educación a la población. Este es un ejemplo destacable de cómo un programa para enfrentar emergencias puede ayudar a salvar muchas vidas y a reducir los daños causados por un desastre natural.

2. ¿Qué son los Sistemas de Información ?

Un Sistema Informático utiliza ordenadores para almacenar los datos de una organización y ponerlos a disposición de su personal. Pueden ser tan simples como en el que una persona tiene una computadora y le introduce datos, los datos pueden ser registros simples como ventas diarias, se produce una entrada por cada venta.

Sin embargo la mayor parte de los sistemas son mas complejos que el enunciando anteriormente. Normalmente una organización tiene más de un sistema de computadoras para soportar las diferentes funciones de la organización, ya sean de ventas, recursos humanos, contabilidad, producción, inventario, etc.

Los sistemas de información tienen muchas cosas en común. La mayoría de ellos están formados por personas, equipos y procedimientos. Al conjugar una serie de elementos como hombres y computadoras se hace imprescindible tomar medidas que nos permitan una continuidad en la operatividad de los sistemas para no ver afectados los objetivos de las mismas y no perder la inversión de costos y tiempo.



La figura anterior nos muestra en un sentido amplio que se puede considerar un Sistema de Información (**SI**) como un conjunto de componentes que interactúan para que la empresa pueda alcanzar sus objetivos satisfactoriamente. Los componentes o recursos de un SI son los siguientes :

- **Datos:** En general se consideran datos tanto los estructurados como los no estructurados, las imágenes, los sonidos, etc.
- **Aplicaciones:** Se incluyen los manuales y las aplicaciones informáticas.
- **Tecnología:** El software y el hardware; los sistemas operativos; los sistemas de gestión de bases de datos; los sistemas de red, etc.
- **Instalaciones:** En ellas se ubican y se mantienen los sistemas de información.
- **Personal:** Los conocimientos específicos que ha de tener el personal de los sistemas de información para planificarlos, organizarlos, administrarlos y gestionarlos.

3. ¿Qué es un Plan de Contingencia?

Podríamos definir a un plan de contingencias como una estrategia planificada con una serie de procedimientos que nos faciliten o nos orienten a tener una solución alternativa que nos permita restituir rápidamente los servicios de la organización ante la eventualidad de todo lo que lo pueda paralizar, ya sea de forma parcial o total.

El plan de contingencia es una herramienta que le ayudará a que los procesos críticos de su empresa u organización continúen funcionando a pesar de una posible falla en los sistemas computarizados. Es decir, un plan que le permite a su negocio u organización, seguir operando aunque sea al mínimo.

4. Objetivos del Plan de Contingencia

- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.
- Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.

5. Aspectos Generales de la Seguridad de la Información.

5.1 La Seguridad Física

La seguridad física garantiza la integridad de los activos humanos, lógicos y materiales de un sistema de información de datos. Si se entiende la contingencia o proximidad de un daño como la definición de Riesgo de Fallo, local o general, tres serían las medidas a preparar para ser utilizadas en relación a la cronología del fallo.

5.1.1 Antes

El nivel adecuado de seguridad física, o grado de seguridad, es un conjunto de acciones utilizadas para evitar el fallo o, en su caso, aminorar las consecuencias que de el se puedan derivar.

Es un concepto aplicable a cualquier actividad, no sólo a la informática, en la que las personas hagan uso particular o profesional de entornos físicos.

- Ubicación del edificio.
- Ubicación del Centro de Procesamiento de Datos dentro del edificio.
- Compartimentación.
- Elementos de la construcción.
- Potencia eléctrica.
- Sistemas contra Incendios.
- Control de accesos.
- Selección de personal.
- Seguridad de los medios.
- Medidas de protección.
- Duplicación de medios.

5.1.2 Durante

Se debe de ejecutar un plan de contingencia adecuado. En general, cualquier desastre es cualquier evento que, cuando ocurre, tiene la capacidad de interrumpir el normal proceso de una empresa.

La probabilidad de que ocurra un desastre es muy baja, aunque se diera, el impacto podría ser tan grande que resultaría fatal para la organización. Por otra parte, no es corriente que un negocio responda por sí mismo ante un acontecimiento como el que se comenta, se deduce la necesidad de contar con los medios necesarios para afrontarlo. Estos medios quedan definidos en el Plan de Recuperación de Desastres que junto con el Centro Alternativo de Proceso de Datos, constituye el plan de contingencia que coordina las necesidades del negocio y las operaciones de recuperación del mismo.

Son puntos imprescindibles del plan de contingencia:

- Realizar un análisis de riesgos de sistemas críticos que determine la tolerancia de los sistemas
- Establecer un periodo critico de recuperación, en la cual los procesos debe de ser reanudados antes de sufrir perdidas significativas o irrecuperables.
- Realizar un Análisis de Aplicaciones Críticas por que se establecerán las prioridades del proceso.
- Determinar las prioridades del proceso, por días del año, que indiquen cuales son las aplicaciones y sistemas críticos en el momento de ocurrir el desastre y el orden de proceso correcto.

- Establecer objetivos de recuperación que determinen el período de tiempo (horas, días, semanas) entre la declaración de desastre y el momento en el que el centro alternativo puede procesar las aplicaciones críticas.
- Designar entre los distintos tipos existentes, un Centro Alternativo de Proceso de Datos.
- Asegurar la capacidad de las comunicaciones.
- Asegurar la capacidad de los servidores back-up.

5.1.3 Después

Los contratos de seguros vienen a compensar, en mayor o menor medida las pérdidas, gastos o responsabilidades que se puedan derivar para el centro de proceso de datos una vez detectado y corregido el fallo. De la gama de seguros existentes, se pueden indicar los siguientes:

- **Centros de proceso y equipamiento:** se contrata la cobertura sobre el daño físico en el CPD (Centro de Procesamiento de Datos) y el equipo contenido en el.
- **Reconstrucción de medios de software:** cubre el daño producido sobre medios software tanto los que son de propiedad del tomador de seguro como aquellos que constituyen su responsabilidad.
- **Gastos extra:** cubre los gastos extra que derivan de la continuidad de las operaciones tras un desastre o daño en el centro de proceso de datos. Es suficiente para compensar los costos de ejecución del plan de contingencia.
- **Interrupción del negocio:** cubre las pérdidas de beneficios netos causadas por las caídas de los medios informáticos o por la suspensión de las operaciones.
- **Documentos y registros valiosos:** Se contrata para obtener una compensación en el valor metálico real por la perdida o daño físico sobre documentos y registros valiosos no amparados por el seguro de reconstrucción de medios software.
- **Errores y omisiones:** proporciona protección legal ante la responsabilidad en que pudiera incurrir un profesional que cometiera un acto, error u omisión que ocasione una perdida financiera a un cliente.
- **Cobertura de fidelidad:** cubre las pérdidas derivadas de actos deshonestos o fraudulentos cometidos por empleados.
- **Transporte de medios:** proporciona cobertura ante pérdidas o daños a los medios transportados.
- **Contratos con proveedores y de mantenimiento:** proveedores o fabricantes que aseguren la existencia de repuestos y consumibles, así como garantías de fabricación.

5.2 Conceptos Generales

5.2.1 Privacidad

Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidas o transmitidas a otros.

5.2.2 Seguridad

Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos.

El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.

5.2.3 Integridad

Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.

El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

5.2.4 Datos

Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), vídeo (secuencia de tramas), etc.

5.2.5 Base de Datos

Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que los utilizan.

También puede definirse, como un conjunto de archivos interrelacionados que es creado y manejado por un Sistema de Gestión o de Administración de Base de Datos (Data Base Management System - DBMS).

Las características que presenta un DBMS son las siguientes:

- Brinda seguridad e integridad a los datos.
- Provee lenguajes de consulta (interactivo).
- Provee una manera de introducir y editar datos en forma interactiva.
- Existe independencia de los datos, es decir, que los detalles de la organización de los datos no necesitan incorporarse a cada programa de aplicación.

5.2.6 Acceso

Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.

5.2.7 Ataque

Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

5.2.8 Ataque Activo

Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: El borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

5.2.9 Ataque Pasivo

Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje

electrónico, telefónico o la intercepción de una red. Todo ésto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene.

5.2.10 Amenaza

Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

5.2.11 Incidente

Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido

5.2.12 Golpe (Breach)

Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

6. Seguridad Integral de la Información

La función del procesamiento de datos es un servicio de toda la institución, que apoya no sólo a los sistemas de información administrativa sino también a las operaciones funcionales. La Seguridad un aspecto de mucha importancia en la correcta Administración Informática, lo es también de toda la Institución.

Las medidas de seguridad están basadas en la definición de controles físicos, funciones, procedimientos y programas que conlleven no sólo a la protección de la integridad de los datos, sino también a la seguridad física de los equipos y de los ambientes en que éstos se encuentren.

En relación a la seguridad misma de la información, estas medidas han de tenerse en cuenta para evitar la pérdida o modificación de los datos, información o software inclusive, por personas no autorizadas, para lo cual se deben tomar en cuenta una serie de medidas, entre las cuales figurarán el asignar números de identificación y contraseñas a los usuarios.

Capítulo II : Fases de la Metodología para el Desarrollo de un Plan de Contingencia de los Sistemas de Información

Debemos de tener presente que mucho dependerá de la infraestructura de la empresa y de los servicios que ésta ofrezca para determinar un modelo de desarrollo de plan, no existe un modelo único para todos, lo que se intenta es dar los puntos más importantes a tener en cuenta.

La metodología empleada para el desarrollo y aplicación del plan de contingencias de los sistemas de información, ha sido desarrollada por el INEI, en base a la experiencia lograda en el desarrollo de planes de contingencia para el problema del año 2000.

La presente metodología se podría resumir en ocho fases de la siguiente manera:

- **Planificación:** preparación y aprobación de esfuerzos y costos.
- **Identificación de riesgos:** funciones y flujos del proceso de la empresa.
- **Identificación de soluciones:** Evaluación de Riesgos de fallas o interrupciones.
- **Estrategias:** Otras opciones, soluciones alternativas, procedimientos manuales.
- **Documentación del proceso:** Creación de un manual del proceso.
- **Realización de pruebas:** selección de casos soluciones que probablemente funcionen.
- **Implementación:** creación de las soluciones requeridas, documentación de los casos.
- **Monitoreo:** Probar nuevas soluciones o validar los casos.

FASE 1 : PLANIFICACION

1.1 Diagnóstico

Cada vez que nos encontremos en una actividad que requiere el diseño de una propuesta de solución para un determinado problema, es necesario siempre la revisión exhaustiva de cada uno de los componentes que conforman nuestro sistema, es por esta razón siempre debemos de realizar una etapa de diagnostico para poder asegurar que las acciones de solución propuestas tengan un fundamento realista y no tener que volver a rehacer toda propuesta.

1.1.1 Organización Estructural y Funcional.

En este aspecto se deben describir y analizar las Direcciones, Gerencias o dependencias en las que se divide la empresa o institución haciendo referencia de las funciones más importantes que desempeñan cada una de ellas, priorizando tales funciones en relación al sistema productivo de bienes o servicios que desarrollan.

Estas Entidades tienen Organigramas que se rigen por Manuales de Organización y Funciones.

1.1.2 Servicios y/o Bienes Producidos.

En este punto se hará referencia sobre los bienes y/o servicios que produce la empresa o institución según el orden de importancia por la generación de beneficios. Si la empresa produce más de un bien la prioridad será determinada según el criterio de los Directivos.

Además se debe elaborar un directorio de clientes priorizando de acuerdo a la magnitud de los bienes o servicios que consumen.

También se harán un breve análisis del mercado de consumo de los bienes y servicios producidos, identificando las zonas o sectores de mayor consumo.

1.1.3 Servicios y Materiales Utilizados.

Con relación a los servicios utilizados se debe elaborar un directorio de empresas o instituciones que abastecen de energía, comunicación, transporte, agua, salud y otros servicios resaltando la importancia de ellos en el sistema de producción de la entidad y verificando la seguridad de los servicios sin problemas de afectación por algún tipo de problema.

También debe hacerse un directorio de todas la entidades abastecedoras de materias primas o insumos para la producción de información.

1.1.4 Inventario de Recursos Informáticos.

El inventario de recursos informáticos se realizará por dependencias y en forma clasificada:

- **Computadoras:** 386, 486 y las Pentium, impresoras, scanners, etc.
- **Programas:** De sistemas operativos, procesadores de textos, hojas de cálculo, lenguajes de programación, software de base.
- **Aplicativos Informáticos:** Del sistema de Contabilidad, de Trámite Documentario, Planillas, Almacén, Ventas, Presupuesto, Personal.
- **Equipos Empotrados:** De Industrias: Hornos y envasadoras. De Banca y Seguros, Cajeros automáticos y bóvedas. De Oficinas, Centrales telefónicas.

Estos inventarios deberán hacerse a través de formularios sistemáticamente elaborados.

El procesamiento de este inventario puede ser de dos tipos:

Proceso Automatizado.- Utilizando herramientas informáticas de diferente nivel, grado de detalle y costo, que pueden acelerar el tiempo de la toma del inventario, procesamiento de datos y emisión de resultados.

Proceso Manual.- Utilizando formatos de recopilación de información.
El conocimiento del Inventario de estos recursos nos permitirá hacer una evaluación de los riesgos de la operatividad de los sistemas de información.

Cada formato consta de dos partes:

a.- Datos componentes: Donde se registran los datos básicos de ubicación, identificación y características primarias, así como también su importancia, compatibilidad y adaptabilidad.
b.- Análisis del proceso de adaptación del componente:
Incluye datos de costos, fecha de culminación, medios utilizados y medidas de contingencia.

1. 2 Planificación

La fase de planificación es la etapa donde se define y prepara el esfuerzo de planificación de contingencia/continuidad. Las actividades durante esta fase incluyen:

- Definición explícita del alcance, indicando qué es lo que se queda y lo que se elimina, y efectuando un seguimiento de las ambigüedades. Una declaración típica podría ser, “La continuidad de los negocios no cubre los planes de recuperación de desastres que ya fueron emitidos.”

- Definición de las fases del plan de eventos (por ejemplo, los períodos pre-evento, evento, y post-evento) y los aspectos sobresalientes de cada fase.
- Definición de una estrategia de planificación de la continuidad del negocio de alto nivel.
- Identificación y asignación de los grupos de trabajo iniciales; definición de los roles y responsabilidades.
- Definición de las partes más importantes de un cronograma maestro y su patrón principal.
- Identificación de las fuentes de financiamiento y beneficios del negocio; revisión del impacto sobre los negocios.
- Duración del enfoque y comunicación de las metas y objetivos, incluyendo los objetivos de la empresa.
- Definición de estrategias para la integración, consolidación, rendición de informes y arranque.
- Definición de los términos clave (contingencia, continuidad de los negocios, etc.)
- Desarrollo de un plan de alto nivel, incluyendo los recursos asignados.
- Obtención de la aprobación y respaldo de la empresa y del personal gerencial de mayor jerarquía. Provisión de las primeras estimaciones del esfuerzo.
- El plan debe ser ejecutado independientemente de las operaciones y procedimientos operativos normales .
- Las pruebas para el plan serán parte de (o mantenidas en conjunción con) los ejercicios normalmente programados para la recuperación de desastres, las pruebas específicas del plan de contingencia de los sistemas de información y la realización de pruebas a nivel de todos los clientes.
- No habrá un plan de respaldo, y tampoco se dará una reversión ni se podrá frenar el avance del plan de contingencia.
- Si ocurre un desastre, una interrupción, o un desfase de gran magnitud en los negocios de la empresa durante el período del calendario de eventos, se pondrán en práctica los planes de continuidad de los negocios o de contingencia.
- Si la organización ha puesto en moratoria los cambios al sistema, se deben permitir las excepciones a dicha moratoria solamente para los cambios de tipo regulador o para los problemas más importantes que afecten la producción o las operaciones de la empresa, y solamente después de haber obtenido la aprobación del nivel ejecutivo.

FASE 2 : IDENTIFICACION DE RIESGOS

La Fase de Identificación de Riesgos, busca minimizar las fallas generadas por cualquier caso en contra del normal desempeño de los sistemas de información a partir del análisis de los proyectos en desarrollo, los cuales no van a ser implementados a tiempo.

El objetivo principal de la Fase de Reducción de Riesgo, es el de realizar un análisis de impacto económico y legal, determinar el efecto de fallas de los principales sistemas de información y producción de la institución o empresa.

2.1 Análisis y Evaluación de Riesgos

Es necesario reconocer y reducir de riesgos potenciales que afecten a los productos y servicios; es por ello que se considera dentro de un Plan de Contingencia, como primer paso la Reducción de Riesgos, para favorecer el cumplimiento de los objetivos institucionales.

El análisis y evaluación de riesgos se desarrolla en 2 situaciones

1. Para entidades que desarrollan Planes de Contingencias su plan de adaptación y no tienen soluciones adecuadas.

   Para aquellas entidades que están realizando Planes de Contingencia, el análisis y evaluación de riesgos consta de:

   1. Evaluar el impacto de los procesos críticos.
   2. Valorar la certificación de los proveedores
   3. Privilegiar proyectos, eliminando aquellos que resultan extemporáneos.
   4. Detectar deficiencias ante cambios en los sistemas afectados.
   5. Guardar copias de información empresarial mediante convenios de soporte.

2. Entidades que a la fecha no han tomado previsión.

   Para aquellas entidades que no están realizando Planes de Contingencia, el análisis y evaluación de riesgos consta de:

   1. Realización un diagnóstico integral del Sistema de Información.
   2. Elaborar una lista de Servicios afectados evaluando su importancia, magnitud del impacto, cuantificar con niveles A, B, C u otro.
   3. Identificar todos los procesos de los servicios afectados.
   4. Analizar sólo los procesos críticos de los servicios.

2.2 Identificar los Procesos Críticos

Al igual que las situaciones de falla, las alternativas pueden ser infinitas. Por ende, se deben identificar muchas para ser capaces de seleccionar las mejores opciones de contingencia. Comience por los riesgos ya identificados como prioridades máximas porque causarían el mayor impacto negativo en los servicios y en las funciones críticas de su organización.

2.3 Análisis de las Operaciones Actuales

El análisis de operación del método actual de trabajo (es decir, cómo y en qué orden su organización obtiene funciones comerciales) puede revelar las oportunidades para reducir, eliminar o simplificar ciertas operaciones o procesos.

Algunas funciones probablemente pueden ser realizadas por terceros sin pérdida de control. Probablemente pueden reducirse algunas operaciones en términos de

pasos e interfaces que ellos requieren. Un almacén parcialmente automatizado puede requerir 24 acciones manuales separadas para llenar una orden grande. Si la organización puede cortar esto en 33 por ciento, a 16 acciones manuales, la eficiencia incrementada puede liberar algunos recursos que pueden usarse en otra parte. Por supuesto, tales acciones van de la mano con la capacitación. Desde el punto de vista de los sistemas de información, tales consideraciones pueden ser cruciales porque puede haber una necesidad de revertir a las operaciones manuales y en ciertos casos sostener las operaciones existentes.

Si consideramos que "No existe producto y/o servicio sin un proceso. De la misma manera, que no existe proceso sin un producto o servicio". Aunque no todos los procesos generan un producto o servicio útil (creando valor agregado) para la institución. Por lo que es necesario realizar un análisis de las operaciones y los procesos que involucran.

- Organización. Cualquier grupo, empresa, corporación, planta, oficina de ventas, etc.

- Función. Un grupo dentro de la organización funcional. Funciones características serían ventas y mercadeo, contabilidad, ingeniería de desarrollo, compras y garantía de calidad.

- Proceso. Cualquier actividad o grupo de actividades que emplee un insumo, le agregue valor a éste y suministre un producto a un cliente externo o interno. Los procesos utilizan los recursos de una organización para suministrar resultados definitivos.

- Proceso de producción. Cualquier proceso que entre en contacto físico con el hardware o software que se entrega a un cliente externo, hasta aquel punto en el cual el producto se empaca (por ejemplo, fabricación de computadoras, preparación de alimentos para el consumo masivo de los clientes, refinación de petróleo, transformación de hierro en acero). Esto no incluye los procesos de embarque y distribución.

- Proceso de la empresa. Todos los procesos de servicios y los que respaldan a los de producción (por ejemplo, de pedidos, proceso de cambio en ingeniería, de planilla, diseño del proceso de manufactura). Un proceso de la empresa consiste en un grupo de tareas lógicamente relacionadas que emplean los recursos de la organización para dar resultados definidos en apoyo de los objetivos de la organización.

Al emplear estas definiciones, se puede observar que casi todo lo que hacemos es un proceso y que los procesos de la empresa desempeñan un papel importante en la supervivencia económica de nuestras organizaciones.

En todas las organizaciones existen, literalmente, centenares de procesos que se realizan diariamente. Más del 80% de éstos son repetitivos, cosas que hacemos una y otra vez. Estos procesos repetitivos (áreas administrativas, manufactureras e intermedias) pueden y deben controlarse, en gran parte, tal como se vigilan los de manufactura. Se manejan muchos procesos de las instituciones y empresas que son tan complejos como el proceso de manufactura.

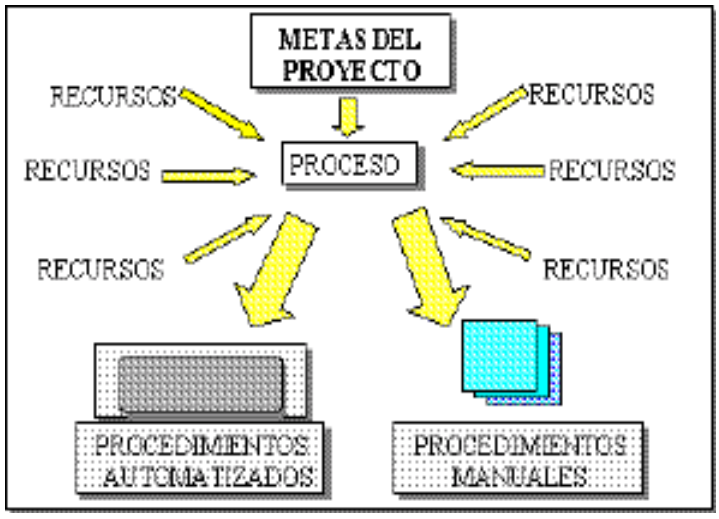
2.4 Uso de la Técnica de Análisis de Procesos

Consideremos para el uso de la técnica de análisis de procesos:

- El ciclo de vida empieza con la descripción de un proceso basado en las metas del proyecto, mientras se utilizan los recursos descritos del proceso.
- El proceso se fija al asignar los recursos.
- El proceso puede instalarse en una máquina o pueden ser procedimientos a seguir por un grupo de personas.
- El proceso es supervisado y medido durante su uso.
- Los datos obtenidos de esta medida se evalúan durante todo el tiempo que se desenvuelva el proceso. Una descripción del proceso existente puede empezar con un informe actual, obtenido de la supervisión y documentación del proceso.

El Proceso de Dirección del Ciclo de Vida en la Figura muestra la descripción de los componentes del proceso y la producción de los principales insumos de trabajo. La descripción del proceso funcionalmente se descompone en el:

1. Análisis del Proceso
2. Plan del Proceso
3. Aplicación del Proceso.



El Análisis del proceso involucra identificación, mientras se analiza el proceso, y los requisitos del proceso. El Plan del proceso involucra el modelamiento de la arquitectura y la descomposición funcional del proceso. La Aplicación del proceso involucra llevar a cabo el plan del proceso para crear tareas a realizarse y proporcionar la capacitación necesaria para las personas que realicen dichas tareas. También la aplicación del proceso involucra la preparación del proceso para su actuación en la empresa o institución, el proceso consiste en los detalles específicos del proyecto y fijar los recursos necesarios.

Diagrama del Proceso Descompuesto

A continuación presentamos una lista de procesos típicos de las empresas definidos por IBM. Esto ayudará a definir los procesos de la empresa.

- Manejo de índices.
- Diseño de sistemas de control.
- Desarrollo de comunicaciones avanzadas
- Diseño de componentes de cable
- Prueba de diseño
- Revisión de diseño y materiales
- Revisión de documentos
- Especificación de diseño a alto nivel
- Coordinación entre divisiones
- Diseño lógico y verificación
- Calificación de componentes
- Diseño del sistema de energía
- Divulgación del producto
- Confiabilidad y utilidad del sistema
- Requerimiento del sistema
- Diseño interactivo de sistemas para el usuario
- Análisis de la competencia
- Apoyo de los sistemas de diseño
- Desarrollo de la información
- Instrumentos de diseño físico
- Diseño de sistemas
- Gerencia de cambio en ingeniería

Es el procedimiento por el cual se estudian los procesos dentro de una secuencia (Línea de producción) de producción o provisión de servicios, que a continuación son presentados, teniendo en consideración:

- Las Funciones Institucionales.
- Los procesos derivados.
- Los subprocesos.

FASE 3 : IDENTIFICACIÓN DE SOLUCIONES

Un proyecto de plan de contingencia no sirve si se queda en plan o papel.
Un plan de contingencias debe contemplar todos los procesos institucionales sean estos manuales y/o automatizados, evaluando el volumen de información o materiales afectados, a fin de definir la complejidad de los sistemas.

La magnitud, de un plan de contingencia será proporcional a la complejidad, importancia, costo del servicio al cual está destinado a proteger y el riesgo asociado a la misma.

El esquema general del plan de contingencias de los sistemas de información, esta constituido por 3 grandes fases:

1. Fase de Reducción de Riesgos
2. Fase de Recuperación de Contingencia
3. Fase de Organización de un Sistema de Alerta contra Fallas

Se debe tener en cuenta al determinar los objetivos, en qué parámetros generales se va a basar, para poner en operación el plan de contingencias.

En cualquier caso, sus planes deben identificar dependencias e impactos y, al mismo tiempo, los recursos necesarios para implementar cada alternativa de contingencia. Se deben buscar alternativas "creativas", que logren el efecto de mitigar el impacto en caso de una falla. En la siguiente tabla se muestra la matriz del plan de contingencia y algunos ejemplos.

Matriz de planificación de contingencia y ejemplos

OPCIONES	OPERACIÓN MANUAL	REEMPLAZO	EXTERNALIZACION DEL SERVICIO
Reparación rápida y de defecto	Recurra al proceso manual sólo en caso de clientes prioritarios. Asegure que contará con personal el 1 y 2 de enero.	Tenga disponible software de repuesto que cumpla con los requisitos	Use personal temporalmente para llenar brecha
Reparación parcial	Use hojas de cálculo o base de datos para ofrecer alguna de la funcionalidad original del sistema (fecha de captura).	Use base de datos o paquetes COTS para reemplazar la funcionalidad del sistema	Haga que el contratista procese los pagos en sus propias instalaciones
Reparación total	Ofrezca operaciones totalmente funcionales a través del proceso manual, utilizando personal adicional si es necesario	Elimine esfuerzos de reparación e implemente un sistema comercial funcional, rápidamente	Entregue el manejo de la plantilla de pago a una firma comercial especialista

3.1 Identificación de Alternativas

Como indicamos anteriormente, un buen método para identificar alternativas consiste en revisar los planes de administración de emergencia o recuperación de fallas. Estos son algunos ejemplos de alternativas que pudieran ayudarle al inicio del proceso de preparación.

- Planifique la necesidad de personal adicional para atender los problemas que ocurran.
- Recurra al procesamiento manual (de facturas, órdenes, cheques, etc.) si fallan los sistemas automatizados.
- Planifique el cierre y reinicio progresivo de los dispositivos y sistemas que se consideran en riesgo.
- Instale generadores si no tiene acceso a la red de energía pública.

- Disponga del suministro adicional de combustible para los generadores, en caso de fallas eléctricas prolongadas.

- Disponga de bombas manuales de combustible y úselas si fallan las electrónicas.

- Elaborar un programa de vacaciones que garantice la presencia permanente del personal.

- No haga nada y vea qué pasa – esta estrategia es algunas veces llamada arreglar sobre falla.

3.2 Identificación de Eventos Activadores

Cuando el equipo de planificación seleccione la mejor alternativa de contingencia, debe definir los activadores que provocarán la implementación del plan. Los activadores son aquellos eventos que permitirán decir "OK", es el momento de pasar al plan B". Incluyen las fallas de los sistemas, u otros eventos que hacen evidente la necesidad de implementar el plan de contingencia. Sin embargo, muchos eventos activadores serán predefinidos como puntos de decisión "pasar/no pasar", el evento que active la decisión de poner en funcionamiento el proceso alternativo puede ser una alerta establecida a una falla anticipada.

La información necesaria para definir los activadores para cada sistema o proceso, provendrá tanto del programa de implementación para los sistemas de información, como de los requerimientos de tiempo desplegados para cada plan de contingencia.

A continuación se muestran algunos ejemplos de los tipos de eventos que pueden servir como activadores en sus planes de contingencia:

- Información de un vendedor respecto a la tardía entrega o no disponibilidad de un componente de software.

- Tardío descubrimiento de serios problemas con una interfaz.

- Tempranas (no anticipadas) fallas del sistema – corrección/reemplazo no está lista para sustituir.

- Fallas del Sistema (datos corruptos en informes o pantallas, transacciones pérdidas, entre otros).

- Fallas de interfaces –intercambios de datos no cumplen los requisitos.

- Fallo de la infraestructura regional (energía, telecomunicaciones, sistemas financieros)

- Problemas de implementación (por ejemplo, falta de tiempo o de fondos).

- Aseveraciones falsas o erróneas sobre el cumplimiento, descubiertas demasiado tarde para iniciar las acciones de cumplimiento.

Cabe mencionar que, para desarrollar este proyecto es necesario conocer los lineamientos generales del sistema afectado, es decir el tipo de producción al cual pertenece pudiendo pertenecer al sector de bienes o al sector servicios. Una vez establecido a que rubro de la producción pertenece, identificamos el departamento u área ligada y las funciones que en ella realiza, las áreas principales pueden ser:

- Contabilidad
- Administración
- Finanzas
- Comercialización
- Producción
- Seguridad

Se deberán identificar las fallas potenciales que puedan ocurrir para cada sistema, considerando la provisión de datos incorrectos, y fiabilidad del sistema para la institución, y así desarrollar una lista de alternativas priorizadas de fallas.

3.3 Identificación de Soluciones

El objetivo es reducir el costo de encontrar una solución en la medida de lo posible, a tiempo de documentar todos los riesgos identificados.

Actividades importantes a realizar:

- La asignación de equipos de solución para cada función, área funcional o área de riesgo de la organización.
- La asociación de soluciones con cada riesgo identificado- se recomienda tener un abanico de alternativas de soluciones, por que las soluciones se analizaran y se compararan posteriormente.
- Comparar los riesgos y determinarles pesos respecto a su importancia crítica en término del impacto de los mismos.
- Clasificar los riesgos.
- La elaboración de soluciones de acuerdo con el calendario de eventos.
- La revisión de la factibilidad de las soluciones y las reglas de implementación.
- La identificación de los modos de implementación y restricciones que afectan a las soluciones.
- La definición e identificación de equipos de acción rápida o equipos de intensificación por área funcional o de negocios de mayor importancia.
- Sopesar las soluciones y los riesgos y su importancia crítica en lo que respecta a su eficacia y su costo, siendo la meta la solución más inteligente.

La revisión de soluciones comparándolas con el nivel mínimo aceptable de resultados o servicios.

3.4 Fallas Genéricas Funcionales de los Sistemas a tener en Consideración.

Se han encontrado varias fallas comunes a muchos sistemas de computación.

Estos incluyen:

- **Autentificación.** En muchos sistemas, los usuarios no pueden determinar si el hardware y el software con que funcionan son los que se supone que deben ser. Esto hace fácil al intruso reemplazar un programa sin conocimiento del usuario. Un usuario puede inadvertidamente teclear una contraseña en un programa de entrada falso.

- **Cifrado.** La lista maestra de contraseñas debe ser almacenada, cifrada, lo que a menudo no se hace.

- **Implementación.** Un diseño bien pensado de un mecanismo de seguridad puede ser implementado de forma improcedente.

- **Confianza implícita.** Un problema corriente, una rutina supone que otra está funcionando bien cuando, de hecho, debería estar examinando detenidamente los parámetros suministrados por la otra.

- **Compartimiento implícito.** El sistema puede depositar inadvertidamente información importante del sistema, en un espacio de direcciones del usuario.

- **Comunicación entre procesos.** El intruso puede usar un mecanismo de SEND/RECEIVE para probar varias posibilidades. Por ejemplo el intruso puede pedir un recurso del sistema y suministrar una contraseña. La información devuelta puede indicar "contraseña correcta", confirmando la contraseña adivinada por el intruso.

- **Verificación de la legalidad.** El sistema puede no estar realizando una validación suficiente de los parámetros del usuario.

- **Desconexión de línea.** En tiempos compartidos y en redes, cuando la línea se pierde (por cualquier razón), el sistema operativo debe inmediatamente dar de baja del sistema al usuario o colocar al usuario en un estado tal, que sea necesaria la reautorización para que el usuario obtenga de nuevo el control. Algunos sistemas permiten que un proceso "flote" después de una desconexión de línea. Un intruso puede llegar a obtener el control del proceso y usar cualesquier recurso a los que tenga acceso el proceso.

- **Descuido del operador.** Un intruso puede engañar a un operador y hacer que cargue un paquete de disco con un sistema operativo falso.

- **Paso de parámetros por referencia en función de su valor.** Es más seguro pasar los parámetros directamente en registros, que tener los registros apuntando a las localidades que contienen los parámetros. El paso por referencia puede llevar a una situación en la cual los parámetros, pueden aún encontrarse en el espacio de direcciones del usuario después de una verificación de la legalidad.

El usuario podría así suministrar parámetros legítimos, verificarlos, y modificarlos justo, antes de ser utilizados por el sistema.

- **Contraseñas.** Las contraseñas son, a menudo, fáciles de adivinar u obtener mediante ensayos repetidos. Debiendo implementarse con número máximo (3) de intentos infructuosos.

- **Entrampamiento al intruso.** Los sistemas deben contener mecanismos de entrampamiento para atraer al intruso inexperto. Es una buena primera línea de detección, pero muchos sistemas tienen trampas inadecuadas.

- **Privilegio.** En algunos sistemas hay demasiados programas con muchos privilegios. Esto es contrario al principio del menor privilegio.

- **Confinamiento del programa.** Un programa prestado de otro usuario puede actuar como caballo de Troya: puede robar o alterar los archivos del usuario que los prestó.

- **Residuos.** A menudo el intruso puede encontrar una lista de contraseñas con sólo buscar en una papelera. Los residuos se dejan a veces en el almacenamiento después de las operaciones rutinarias del sistema. La información delicada debe ser siempre destruida antes de liberar o descargar el medio que ocupa (almacenamiento, papel, etc.). Las trituradoras de papel son algo corriente en ese aspecto.

- **Blindaje.** Una corriente en un cable genera un campo magnético alrededor de él; los intrusos pueden de hecho conectarse a una línea de transmisión o a un sistema de computación sin hacer contacto físico. Puede usarse el blindaje eléctrico para prevenir tales "intrusiones invisibles".

- **Valores de umbral.** Están diseñados para desanimar los intentos de entrada, por ejemplo. Después de cierto número de intentos inválidos de entrar al sistema, ese usuario (o el terminal desde donde se intentan las entradas) debe ser bloqueado y el administrador del sistema, advertido. Muchos sistemas carecen de esta característica.

3.5 Ataques Genéricos a Sistemas Operativos

Ciertos métodos de penetración se han utilizado efectivamente en muchos sistemas.

- **Asincronismo**. Con procesos múltiples que progresan de forma asincrónica, es posible que un proceso modifique los parámetros cuya validez ha sido probada por otro, pero que aún no ha utilizado. Con ésto, un proceso puede pasar valores malos a otro, aún cuando el segundo realice una verificación extensa.

- **Rastreo.** Un usuario revisa el sistema de computación, intentando localizar información privilegiada.

- **Entre líneas.** Se usa un terminal especial para conectarse a la línea de comunicación mantenida por un usuario dado de alta en el sistema, que está inactivo en ese momento.

- **Código clandestino.** Se hace un parche en el sistema operativo bajo la pretensión de una depuración. El código contiene trampas que permiten realizar a continuación reentradas no autorizadas al sistema.

- **Prohibición de acceso.** Un usuario escribe un programa para hacer caer al sistema, poner al sistema en un ciclo infinito, o monopolizar recursos del sistema. Lo que se intenta aquí es el negar el acceso o servicio a los usuarios legítimos.

- **Procesos sincronizados interactivos.** Los procesos usan las primitivas de sincronización del sistema para compartir y pasarse información entre sí.

- **Desconexión de línea.** El intruso intenta obtener acceso al trabajo de un usuario después de una desconexión de línea, pero antes de que el sistema reconozca la desconexión.

- **Disfraz.** El intruso asume la identidad de un usuario legítimo, después de haber obtenido la identificación apropiada por medios clandestinos.

- **Engaño al operador.** Un intruso inteligente puede, a menudo, engañar al operador del computador y hacer que realice una acción que comprometa la seguridad del sistema.

- **Parásito.** El intruso utiliza un terminal especial para conectarse a una línea de comunicación. El intruso intercepta los mensajes entre el usuario y el procesador, modifica el mensaje o lo reemplaza por completo.

- **Caballo de Troya.** El intruso coloca un código dentro del sistema que le permita accesos posteriores no autorizados. El caballo de Troya puede dejarse permanentemente en el sistema o puede borrar todo rastro de sí mismo, después de la penetración.

- **Parámetros inesperados.** El intruso suministra valores inesperados a una llamada al supervisor, para aprovechar una debilidad de los mecanismos de verificación de la legalidad del sistema.

A medida que la computación se hace más asequible, los problemas de seguridad aumentan. Las comunicaciones de datos y las redes suponen un gran aumento de la vulnerabilidad de los sistemas basados en computadores. El hecho de ser favorables al usuario, implica también un incremento de la vulnerabilidad.

Los requisitos de seguridad de un sistema dado, definen lo que para ese sistema significa la seguridad. La seguridad externa se ocupa de la protección del sistema de computación contra intrusos y desastres. La seguridad de la interfase del usuario se encarga de establecer la identidad del usuario antes de permitir el acceso al sistema. La seguridad interna se encarga de asegurar una operación confiable y sin

problemas del sistema de computación, y de garantizar la integridad de los programas y datos.

La autorización determina qué acceso se permite a qué entidades. La división de responsabilidades da a la gente distintos conjuntos de responsabilidades. Ningún empleado trata con una gran parte de la operación del sistema, de modo que para comprometer la seguridad tienen que estar implicados varios empleados.

La vigilancia trata de la supervisión y auditoría del sistema, y de la autentificación de los usuarios. En la verificación de las amenazas, el sistema operativo controla las operaciones delicadas, en vez de darle el control directo a los usuarios. Los programas de vigilancia realizan operaciones sensibles.

Cuando los programas de vigilancia han de tener un acceso mayor que los programas del usuario, para servir las peticiones del usuario, ésto se denomina amplificación.

3.6 Seguridad en Redes

3.6.1 Las Funciones de Seguridad de Red

En el intento de proteger una red de computadoras, existen varias funciones comunes a las cuales deben dirigirse. La siguiente es una lista de cuatro problemas básicos:

- El anfitrión promiscuo, la red debuggers.
- La autenticación de cliente y servidor.
- La autorización de cliente y servidor
- Contabilidad de cliente y servidor.

a. El anfitrión promiscuo

El anfitrión promiscuo es uno de los principales problemas de seguridad y uno de los problemas más urgentes de cualquier red. Si un intruso es paciente, él puede simplemente mirar (con una red debugger o anfitrión promiscuo) que los paquetes fluyen de aquí para allá a través de la red. No toma mucha programación el análisis de la información que fluye sobre la red.

Un ejemplo simple es un procedimiento de login remoto. En el procedimiento login, el sistema pedirá y recibirá el nombre y contraseña del usuario a través de la red.

Durante la transmisión, esta información no es codificada o encriptada de cualquier forma. Una persona paciente simplemente puede esperar, y así recolectar toda la información que necesita para romper cualquier cuenta.

b. Autenticación

El procedimiento de login remoto ilustra el problema de autenticación. ¿Cómo presenta usted credenciales al anfitrión remoto para probar que usted es usted?.

¿Cómo hace usted ésto, de forma que no se repita por el mecanismo simple de una jornada registrada?.

c. Autorización

Aún cuando usted puede probar que usted es quien dice que es, simplemente, ¿Qué información debería permitir el sistema local accesar desde a través de una red?. Este problema de autorización parecería ser simple en concepto, pero considerar los problemas de control de acceso, cuando todo el sistema tiene su identidad remota de usuario, el problema de autorización sería un problema de seguridad bastante serio, en donde intervienen los conceptos de funciones autorizadas, niveles de autorización, etc.

d. Contabilidad

Finalmente, considerar el problema de contabilidad. Hay que recordar que nosotros debemos asumir que hay otros con un conocimiento mayor de sistemas. ¿Cuánta contabilidad tiene que hacer el sistema para crear una pista de revisión y luego examinar?

3.6.2 Componentes de Seguridad

Para un intruso que busque acceder a los datos de la red, la línea de ataque más prometedora será una estación de trabajo de la red. Estas se deben proteger con cuidado. Debe habilitarse un sistema que impida que usuarios no autorizados puedan conectarse a la red y copiar información fuera de ella, e incluso imprimirla.

Por supuesto, una red deja de ser eficiente si se convierte en una fortaleza inaccesible. El administrador de la red tal vez tenga que clasificar a los usuarios de la red con el objeto de adjudicarles el nivel de seguridad adecuado. A continuación se sugiere un sistema en tres niveles:

- **Nivel de administración.** Aquellos que diseñan, mantienen o ponen en marcha la red. Este debe estar constituido sólo por el administrador o por un pequeño grupo de personal de soporte y administración.

- **Usuarios fiables.** Aquellos usuarios que cumplen las normas y cuyo trabajo se pueda beneficiar de una mayor libertad de acceso a la red.

- **Usuarios vulnerables.** Aquellos que muestran falta de competencia, son excesivamente curiosos o beligerantes, o los que por alguna razón no se puede confiar.

Estos niveles pueden tener un reflejo en el número de barreras que se establecen para el acceso al sistema y el tipo de derechos de acceso que se conceden, para cuando se ha obtenido la conexión, así como el nivel de supervisión y la frecuencia de las comprobaciones.

3.6.3 Control de Acceso a la Red

- Restringir el acceso a las áreas en que están las estaciones de trabajo mediante llaves, tarjetas de identificación, tarjetas inteligentes y sistemas biométricos.
- Restringir las posibilidad de conectar estaciones mediante llaves, tarjetas de identificación, tarjetas inteligentes y sistemas biométricos.
- Identificación para la red con clave de acceso.
- Protección con clave de todas la áreas sensitivas de datos y restricción de acceso a los programas, según su uso.
- Registro de toda la actividad de la estación de trabajo.
- Protección con clave de acceso o bloqueo de todas las operaciones de copia a disquete en las estaciones de trabajo.
- Monitorización de todas las operaciones de copia en disquete en las estaciones de trabajo.

3.6.4 Protección del Servidor

La parte más importante de la red es el servidor. La concentración de los datos en el servidor, en términos de cantidad e importancia, hace que sea necesario protegerlo de todas las eventualidades.

La dependencia en que esté el servidor no debe ser accesible para nadie, excepto para el administrador de la red. No se debe permitir que personas que no han de utilizar el servidor estén cerca de él. Las impresoras y otros periféricos deben mantenerse alejados de ojos fisgones.

Dada la importancia del servidor y la cantidad de datos que pasan por él, es necesario efectuar copias de seguridad, del servidor. Cabe recordar que las copias de seguridad del servidor de archivos son un elemento especialmente valioso, debiéndose quedar guardados en un lugar cerrado, seguro y con las condiciones ambientales necesarias. Un conjunto de copias de seguridad se debe trasladar regularmente a otro lugar seguro (de preferencia otro local).

Redes y tolerancia a fallas

La tolerancia a fallas es la capacidad de la red de continuar funcionando, en el caso que se produzca un problema importante o una caída catastrófica, sin daño para los datos y sin que el funcionamiento cambie perceptiblemente.

La tolerancia a fallas, se refiere no sólo a la redundancia, sino a la detección de errores. Por lo general, la tolerancia a fallas conduce a un elemento hardware redundante, que entra en funcionamiento de forma automática en el caso que el componente primario falle. Sin embargo la tolerancia a fallas puede ser algo como duplicar la FAT (tabla de localización de archivos) y las entradas de directorio en áreas distintas de un mismo disco, o una simple verificación de lectura tras escritura, con lo que se asegura que los datos nunca se escriben en un sector dañado del disco.

No todas las redes requieren el mismo grado de tolerancia a fallas.

3.6.5 Protegiendo la Red

Estaciones de trabajo sin floppy disk. Una posible solución para poder impedir la copia de programas y datos fuera de la red en disquetes, y que a través de los disquetes ingresen virus y otros programas dañinos a la red, es dotar a los usuarios vulnerables con estaciones de trabajo sin floppy disk.

3.6.6 Tecnología RAID, (Ofrece tolerancia a fallas y corrige errores)

RAID (Arreglo Redundante de Discos Asequibles) reemplaza los sistemas de almacenamiento, grandes y costosos, con múltiples unidades de disco duro, pequeñas e idénticas. Potencialmente la tecnología RAID puede reducir el costo del almacenamiento, aumentar la velocidad y mejorar la confiabilidad del sistema.

El arreglo RAID sólo responde como un disco duro grande, en lugar de varios discos identificados por letras (en el caso de múltiples discos duros conectados a una computadora estándar). Más importante aún, el contenido de un archivo no está concentrado en un sólo disco duro, sino que está esparcido a lo largo del arreglo, aumentando la seguridad de la información.

Sin embargo, esta seguridad tiene su precio. El precio por megabyte disminuye a medida que aumenta la capacidad del disco, por lo tanto un arreglo de discos menores inherentemente cuesta más que una unidad mayor de la misma capacidad total.

RAID también requiere un controlador de disco duro especial como el UltraStor Ultra 124F basado en EISA. Un sistema RAID ofrece menos capacidad total que la suma de los discos que lo componen.

La redundancia en el diseño de RAID significa que una parte de los datos almacenados se duplica para ayudar a detectar errores y corregirlos. Este método de almacenamiento pone fin a los errores de lectura y escritura y ofrece una verdadera tolerancia a fallas.

Además, los sistemas RAID pueden ofrecer a los usuarios de las redes, acceso a todos los datos, aunque un disco duro en el arreglo, falle catastróficamente.

Esta tecnología va más allá de los asuntos de confiabilidad para mejorar el rendimiento. Los múltiples discos en el arreglo pueden leer y escribir los datos en paralelo, dividiendo la información entre los discos a nivel de bit, byte o bloque, usando un proceso llamado la división de datos (data striping), y potencialmente pueden multiplicar la transferencia de información máxima por el número de discos en el arreglo.

Los controladores de discos avanzados pueden manejar múltiples peticiones simultáneamente, un método de búsqueda que reduce el tiempo de acceso a casi cero. Con este proceso, uno de los discos realiza la búsqueda mientras el sistema lee de otros discos.

NIVELES DE RAID

RAID viene en cinco niveles diferentes, los niveles del uno al cinco, cada uno diseñado para un uso específico. Estos números son simples designaciones de los diferentes métodos de proteger los datos en los discos duros y no describen los niveles de velocidad o calidad: RAID 1 no es mejor ni peor que RAID 5. El tipo de RAID apropiado para su servidor depende de cómo usa su red y el tipo de protección que desea proporcionarle.

- **RAID 1.** Significa una redundancia total, dos discos de igual capacidad que duplican el contenido (o reflejan), uno del otro. Uno resguarda al otro automática y continuamente. El arreglo regresa a una operación de un solo disco si cualquiera de las unidades falla.

- **El Sistema RAID 1** está diseñado para los tipos de informaciones esenciales, cuyo reemplazo sería difícil y costoso. Aunque esta duplicación reduce la capacidad potencial de almacenamiento a la mitad, típicamente no tiene ningún efecto en el rendimiento. Sin embargo, los controladores RAID 1 sofisticados potencialmente, pueden duplicar el rendimiento leyendo sectores alternos de ambos discos.

- **RAID 2.** Divide cada bit de los bytes o bloques de información entre discos separados y luego añade varios discos más para la corrección de errores. Por ejemplo, un sistema RAID 2 almacena una información digital de 16 bits en 16 discos, con 5 o 6 discos adicionales para la corrección de errores, o información de paridad. El número exacto de discos de corrección de errores que usa su sistema depende del algoritmo de división que se emplee. La penalidad en el tamaño del disco puede ser de hasta 37,5 por ciento, tres bits de corrección por cada ocho bits de información. Además, el diseño RAID 2 aumenta el

tamaño de la unidad de almacenamiento mínima (el tamaño de los sectores se multiplica por el número de discos, un arreglo de 16 discos tiene sectores de 8.192 bits), haciéndolo ineficiente para almacenar archivos pequeños en tantos discos. Por otra parte RAID 2 logra razones de transferencia más elevadas porque los discos manejan los bits en paralelo.

Los errores se corrigen sobre la marcha, sin efectuar el rendimiento, porque el controlador puede reconstituir la mayoría de los errores de la información redundante, sin tener que repetir la lectura de los discos duros.

- **RAID 3.** Elimina parte de la minuciosidad que ofrece RAID 2, ya que utiliza la detección de errores en lugar de la corrección de errores. La detección de errores mediante el proceso de verificación de paridad requiere menos discos en el arreglo, típicamente uno por arreglo. Cuando el controlador detecta un error, hace que el arreglo vuelva a leer la información para resolver el problema. Esto requiere una revolución adicional en todos los discos del arreglo, lo que añade una pequeña demora en la operación del disco.

- **RAID 4.** Los sistemas RAID 4, trabajan a nivel de sector en lugar de a nivel de bits. Los archivos se dividen entre los discos a nivel de sector, los sectores se leen serialmente, el primero de un disco, el segundo del próximo disco, y así sucesivamente. Para detectar errores, RAID 4 añade un disco dedicado a la paridad, mientras que el controlador de RAID 4 puede aumentar la velocidad con la división de datos. Se pueden leer simultáneamente dos o más sectores de discos diferentes, almacenarlos en RAM, que es mucho más rápida, normalmente varias órdenes de magnitud, y leerlos secuencialmente a la velocidad de la memoria.

  Los mejores controladores de RAID 4 también procesan múltiples peticiones de datos simultáneamente, reorganizándolas, y luego leyendo los discos de la manera más eficiente, una tecnología conocida como búsqueda elevadora (elevator seeking). Sin embargo, la escritura es más lenta que la lectura porque RAID 4 usa una tecnología de leer - después de escribir. Después de escribir la información en el disco, se lee para determinar la paridad y escribir esa información en el disco de paridad.

- **RAID 5.** Elimina el disco de paridad dedicado de un sistema RAID 4. La información de paridad se añade como otro sector que rota por los discos del arreglo, exactamente igual a los datos ordinarios. Para un rendimiento mejor, los controladores de RAID 5 pueden añadir la división de datos y la búsqueda elevadora. Además, el sistema puede tener suficiente redundancia para ser tolerante a las fallas.

VENTAJAS Y DESVENTAJAS DE LA TECNOLOGIA RAID

- Dos tipos de RAID dominan los arreglos usados por las computadoras. RAID 1 es popular en los servidores de archivos NetWare, aunque Novell usualmente se refiere a esta tecnología como reflexión (mirroring). Sin embargo, la mayoría de los dispositivos de computadoras llamados arreglos de discos, se adaptan al diseño RAID 5, ya que RAID 4 no ofrece ventajas reales, y RAID 2 y RAID 3 requieren demasiados discos y tienen demasiadas desventajas para ser útiles en la mayoría de las aplicaciones del entorno de la PC.

- Además de las capacidades extremas que se pueden obtener de los múltiples discos, la única ventaja que RAID ofrece a las computadoras de un solo usuario es potencialmente una mayor velocidad de transferencia. DOS usa entradas y salidas seriales (una petición de almacenamiento se debe satisfacer antes de emitir la otra), lo que no se beneficia de las búsquedas elevadoras.

- La confiabilidad adicional de un sistema RAID es una virtud dudosa cuando los discos duros ordinarios tienen clasificaciones MTBF (mean time between failures o tiempo promedio entre roturas) de 150.000 a 350.000 horas.

- Los servidores de archivos basados en PCs y la tecnología RAID, tienen sentido cuando se comparan a los sistemas de almacenamiento en los mainframes y minicomputadoras tradicionales: con discos duros del tamaño de refrigeradores de alta capacidad.

- La protección de la información que ofrecen los arreglos RAID, sustituye la solidez mecánica de las unidades de discos grandes, mientras logran una confiabilidad idéntica y en algunos casos superior.

FASE 4 : ESTRATEGIAS

Las estrategias de contingencia / continuidad de los negocios están diseñadas para identificar prioridades y determinar en forma razonable las soluciones a ser seleccionadas en primera instancia o los riesgos a ser encarados en primer lugar. Hay que decidir si se adoptarán las soluciones a gran escala, como las opciones de recuperación de desastres para un centro de datos.

4.1 Actividades Importantes

- La revisión de procesos, flujos, funciones y opciones de importancia crítica.
- La definición de las opciones de contingencia seleccionadas para cada riesgo identificado (nivel de componente, nivel de proceso de la empresa).
- La revisión / depuración del cronograma maestro, incluyendo prioridades, fechas importantes en el calendario de eventos y dependencias cruzadas en diversos proyectos o áreas.

- La consolidación de soluciones de acuerdo a las funciones o áreas de negocios más importantes e identificar las estrategias globales.
- La identificación de los impactos de las soluciones y estrategias para ahorrar costos, como puede ser la selección de una solución para cubrir varios riesgos, Se deben de considerar varios elementos de costo: como el costo de crear la solución, el costo de implementar la solución, y el costo de mantener vigente dicha solución. Debido a que la continuidad de las operaciones de la organización constituye el enfoque primordial, la estrategia de la empresa rige el análisis de costos.
- La obtención de aprobaciones finales para el financiamiento, antes de que se apruebe la solución.
- La identificación de los beneficios es un elemento clave para asegurar que el costo del proyecto este equilibrado con los retornos reales de la organización.

4.2 Preparativos para la Identificación de Soluciones Preventivas

Los puntos que deben ser cubiertos por todos las áreas informáticas y usuarios en general son:

- Respaldar toda la información importante en medio magnético, ya sea en disquetes, cintas o CD-ROM, dependiendo de los recursos con que cuente cada área. Acordamos que lo que debe respaldarse es INFORMACION y no las aplicaciones.
- Generar discos de arranque para las máquinas dependiendo de su sistema operativo, ya sea DOS, Win95/98 o WinNT, libres de virus y protegidos contra escritura.
- Mantener una copia de antivirus más reciente en disco para emergencias (dependiendo del fabricante, variarán las instrucciones para generarlo).
- Guardar una copia impresa de la documentación de los sistemas e interfaces, al igual de los planes de contingencia definidos por el resto de las áreas.
- Instalar todos los Service Packs que el equipo necesite y llevar un registro de los mismos, en caso de formatear el equipo o desinstalar aplicaciones.

4.3 Medida de Precaución y Recomendación

4.3.1 En Relación al Centro de Cómputo

- Es recomendable que el Centro de Cómputo no esté ubicado en las áreas de alto tráfico de personas o con un alto número de invitados.
- Hasta hace algunos años la exposición de los Equipos de Cómputo a través de grandes ventanales, constituían el orgullo de la organización, considerándose necesario que estuviesen a la vista del público, siendo constantemente visitados. Esto ha cambiado de modo radical, principalmente por el riesgo de terrorismo y sabotaje.
- Se deben evitar, en lo posible, los grandes ventanales, los cuales además de que permiten la entrada del sol y calor (inconvenientes para el equipo de cómputo), puede ser un riesgo para la seguridad del Centro de Cómputo.
- Otra precaución que se debe tener en la construcción del Centro de Cómputo, es que no existan materiales que sean altamente inflamables, que despiden humos sumamente tóxicos o bien paredes que no quedan perfectamente selladas y despidan polvo.
- El acceso al Centro de Cómputo debe estar restringido al personal autorizado. El personal de la Institución deberá tener su carné de identificación siempre en un lugar visible.
- Se debe establecer un medio de control de entrada y salida de visitas al centro de cómputo. Si fuera posible, acondicionar un ambiente o área de visitas.
- Se recomienda que al momento de reclutar al personal se les debe hacer además exámenes psicológicos y médico y tener muy en cuenta sus antecedentes de trabajo, ya que un Centro de Cómputo depende en gran medida, de la integridad, estabilidad y lealtad del personal.
- El acceso a los sistemas compartidos por múltiples usuarios y a los archivos de información contenidos en dichos sistemas, debe estar controlado mediante la verificación de la identidad de los usuarios autorizados.
- Deben establecerse controles para una efectiva disuasión y detección, a tiempo, de los intentos no autorizados de acceder a los sistemas y a los archivos de información que contienen.
- Se recomienda establecer políticas para la creación de los password y establecer periodicidad de cambios de los mismos.
- Establecer políticas de autorizaciones de acceso físico al ambiente y de revisiones periódicas de dichas autorizaciones.
- Establecer políticas de control de entrada y salida del personal, así como de los paquetes u objetos que portan.
- La seguridad de las terminales de un sistema en red podrán ser controlados por medios de anulación del disk drive, cubriéndose de esa manera la seguridad contra robos de la información y el acceso de virus informáticos.

- Los controles de acceso, el acceso en sí y los vigilantes deben estar ubicados de tal manera que no sea fácil el ingreso de una persona extraña. En caso que ingresara algún extraño al centro de Cómputo, que no pase desapercibido y que no le sea fácil a dicha persona llevarse un archivo.
- Las cámaras fotográficas no se permitirán en ninguna sala de cómputo, sin permiso por escrito de la Dirección.
- Asignar a una sola persona la responsabilidad de la protección de los equipos en cada área.
- El modelo de seguridad a implementar, estará basado en el entorno y en la política y estrategias de la instalación.

4.3.1.1 Respecto a la Administración de la Cintoteca:

- Debe ser administrada bajo la lógica de un almacén. Esto implica ingreso y salida de medios magnéticos (sean cintas, disquetes cassettes, cartuchos, Discos remobibles, CD's, etc.), obviamente teniendo más cuidado con las salidas.
- La cintoteca, que es el almacén de los medios magnéticos (sean cintas, disquetes cassettes, cartuchos, Discos remobibles, CD's, etc.) y de la información que contienen, se debe controlar para que siempre haya determinado grado de temperatura y de la humedad.
- Todos los medios magnéticos deberán tener etiquetas que definan su contenido y nivel de seguridad.
- El control de los medios magnéticos debe ser llevado mediante inventarios periódicos.

4.3.1.2 Respecto a la Administración de Impresoras:

- Todo listado que especialmente contenga información confidencial, debe ser destruido, así como el papel carbón de los formatos de impresión especiales.
- Establecer controles de impresión, respetando prioridades de acuerdo a la cola de impresión.
- Establecer controles respecto a los procesos remotos de impresión.

Niveles de Control:

Existen dos tipos de activos en un Centro de Cómputo. Los equipos físicos y la información contenida en dichos equipos. Estos activos son susceptibles de robo o daño del equipo, revelación o destrucción no autorizada de la información clasificada, o interrupción del soporte a los procesos del negocio, etc.

El valor de los activos a proteger, está determinado por el nivel de clasificación de la información y por el impacto en el negocio, causado por pérdida o destrucción del Equipo o información. Hay que distinguir los activos en nivel clasificado y no clasificado. Para los de nivel no clasificado, no será necesario control. Cualquier control debe basarse únicamente en el valor del equipo y servicios que ellos prestan.

En cambio tratándose de nivel clasificado, deben observarse además todas la medidas de seguridad de la información que estos equipos contengan.

4.3.2 Medios de Almacenamientos

4.3.2.1 Recomendaciones para el Mantenimiento de Cintas Magnéticas y Cartuchos.

Las cintas magnéticas y cartuchos deben guardarse bajo ciertas condiciones, con la finalidad de garantizar una adecuada conservación de la información almacenada.

a. Cintas Magnéticas:

- La temperatura y humedad relativa del ambiente en que se encuentran almacenados deben estar en el siguiente rango:

  Temperatura : 4ºC a 32ºC

  Humedad Relativa : 20 % a 80 %

- El ambiente debe contar con aire acondicionado.
- Las cintas deben colocarse en estantes o armarios adecuados.
- Deberá mantenerse alejados de los campos magnéticos.
- Se les debe dar un mantenimiento preventivo en forma periódica a fin de desmagnetizar impurezas que se hayan registrado sobre ellas.

b. Cartuchos:

- La temperatura y humedad relativa del ambiente en que se encuentran almacenados deben estar en el siguiente rango:

  Temperatura : 16ºC a más

  Humedad Relativa : 20 % a 80 %

- La temperatura interna del Drive puede oscilar entre: 5ºC a 45ºC.

- Deben ser guardados dentro de su caja de plástico.
- Deben mantenerse alejados de campos magnéticos.

4.3.2.2 Recomendaciones para el Mantenimiento de Discos Magnéticos

Las recomendaciones para el buen mantenimiento de los discos magnéticos son:

a. En general los discos magnéticos son medios de almacenamiento "delicados", pues si sufren un pequeño golpe puede ocasionar que la información se dañe o producir un CRASH al sistema.

b. El cabezal de lectura-escritura debe estar lubricado para evitar daños al entrar en contacto con la superficie del disco.

c. Se debe evitar que el equipo sea colocado en una zona donde se acumule calor, ya que el calor interfiere en los discos cuando algunas piezas se dilatan más que otras, o se secan los lubricantes. Con ello se modifican la alineación entre el disco y los cabezales de lectura-escritura, pudiéndose destruir la información.

d. Las ranuras de los ventiladores de refrigeración deben estar libres.

e. Se debe evitar, en lo posible, la introducción de partículas de polvo que pueden originar serios problemas.

4.3.2.3 Recomendaciones para el Mantenimiento de los Discos Duros

Aunque el conjunto de cabezales y discos viene de fábrica sellado herméticamente, debe evitarse que los circuitos electrónicos que se encuentran alrededor se llenen de partículas de polvo y suciedad que pudieran ser causa de errores.

El ordenador debe colocarse en un lugar donde no pueda ser golpeado, de preferencia sobre un escritorio resistente y amplio.

Se debe evitar que la microcomputadora se coloque en zonas donde haya acumulación de calor. Esta es una de las causas más frecuentes de las fallas de los discos duros, sobre todo cuando algunas piezas se dilatan más que otras.

No se debe mover la CPU conteniendo al disco duro cuando esté encendido, porque los cabezales de lectura-escritura pueden dañar al disco.

Una de las medidas más importantes en este aspecto, es hacer que la gente tome conciencia de lo importante que es cuidar un Microcomputador.

4.3.2.4 Recomendaciones para el Mantenimiento de Disquetes

Las recomendaciones que a continuación se sugieren se aplican en general para los diferentes tipos de disquetes: de 5 ¼" y 3 ½" de alta y baja densidad en ambos casos.

a. Debe mantenerse a una temperatura normal, en un rango comprendido entre los 10ºC y 52ºC, con la finalidad de evitar que se deteriore el material del cual está hecho.

b. Para coger el disquete debe hacerse por la parte plástica y nunca por la parte física interna, debido a que por su tecnología, el proceso de almacenamiento es magnético y el cuerpo humano ejerce cierta fuerza magnética y puede desmagnetizarse.

c. De manera similar, no debe acercarse a los disquetes ningún cuerpo con propiedades magnéticas (como los imanes), ya que podrían provocar la pérdida irrecuperable de los datos ya almacenados.

d. Cuando se esté grabando o borrando información no se debe levantar la compuerta del disk drive (disquete de 5 ¼") o presionar el botón (disquete de 3 ½"), porque puede ocurrir que no sólo se dañe la información restante, sino también el formato lógico, tomándolos como bloques de sectores dañados.

e. Los disquetes deben mantenerse en sus respectivas fundas y en su manipuleo se debe evitar:

   - Doblar los disquetes
   - Colocar un peso sobre ellos, debiendo mantenerse en zonas libres.
   - Tratarlos como una placa simple de plástico, es decir, no se debe usar clips o grapas para unirlos con otros materiales (hojas u otros disquetes).

4.3.3 Respecto a los Monitores

La forma más fácil y común de reducir la fatiga en la visión que resulta de mirar a una pantalla todo el día, es el uso de medidas contra la refección.

Generalmente éstos vienen en forma de una pantalla con un terminado áspero o algún tipo de capa contra brillo con una base de sílice, sobre la superficie de la pantalla del monitor.

Se recomienda sentarse por lo menos a 60 cm. (2 pies) de la pantalla. No sólo ésto reducirá su exposición a las emisiones (que se disipan a una razón

proporcional al cuadrado de la distancia), sino que puede ayudar a reducir el esfuerzo visual.

También manténgase por lo menos a 1 m. o 1.20 m. (3 o 4 pies) del monitor de su vecino, ya que la mayoría de los monitores producen más emisiones por detrás, que por delante.

Finalmente apague su monitor cuando no lo esté usando

4.3.4 Recomendación para el Cuidado del Equipo de Cómputo

Teclado. Mantener fuera del teclado grapas y clips pues, de insertarse entre las teclas, puede causar un cruce de función.

Cpu. Mantener la parte posterior del cpu liberado en por lo menos 10 cm. Para asegurar así una ventilación mínima adecuada.

Mouse. Poner debajo del mouse una superficie plana y limpia, de tal manera que no se ensucien los rodillos y mantener el buen funcionamiento de éste.

Protectores de pantalla. Estos sirven para evitar la radiación de las pantallas a color que causan irritación a los ojos.

Impresora. El manejo de las impresoras, en su mayoría, es a través de los botones, tanto para avanzar como para retroceder el papel.

Por Ejemplo:
Caso Epson FX-1170/LQ-1070 no usar rodillo cuando esté prendido.

Caso Epson DFX-5000/8000 tratar con cuidado los sujetadores de papel y no apagar de súbito, asegurarse que el ON LINE esté apagado, así evitaremos problemas de cabezal y sujetador.

Caso de mala impresión, luego de imprimir documentos o cuadros generados, apagar por unos segundos la impresora para que se pierda el set dejado.

4.3.4.1 Mantener las Areas Operativas Limpias y Pulcras

Todas las razones para mantener las áreas operativas limpias y pulcras son numerosas, para enunciarlas aquí. Sin embargo, algunos de los problemas que usted puede evitar son: el peligro de fuego generado por la acumulación de papeles bajo el falso piso, el daño potencial al equipo por derramar el café, leche o chocolate en los componentes del sistema, el peligro de fuego que se presentan por el excesivo almacenamiento de hojas continuas, el peligro por fumar y las falsas alarmas creadas por detectores de humo. Estos son solamente algunos de los problemas encontrados en las áreas operativas con reglas poco estrictas de limpieza.

FASE 5 : DOCUMENTACION DEL PROCESO

Todo el proceso de lograr identificar soluciones ante determinados problemas no tendrá su efecto verdadero si es que no se realiza una difusión adecuada de todos los puntos importantes que este implica, y un plan de Contingencia con mucho mayor razón necesita de la elaboración de una documentación que sea eficientemente orientada.

Como puntos importantes que debe de incluir esta documentación podremos citar las siguientes:

- Cuadro de descripción de los equipos y las tareas para ubicar las soluciones a las contingencias.
- La documentación de los riesgos, opciones y soluciones por escrito y en detalle.
- La identificación y documentación de listas de contacto de emergencia, la identificación de responsables de las funciones con el fin de garantizar que siempre haya alguien a cargo, y que pueda ser contactada si falla un proceso de importancia.

FASE 6 : REALIZACION DE PRUEBAS Y VALIDACION

6.1 Plan de Recuperación de Desastres

Es importante definir los procedimientos y planes de acción para el caso de una posible falla, siniestro o desastre en el área Informática, considerando como tal todas las áreas de los usuarios que procesan información por medio de la computadora.

Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño producido, lo que permitirá recuperar en el menor tiempo posible el proceso perdido.

La elaboración de los procedimientos que se determinen como adecuados para un caso de emergencia, deben ser planeados y probados fehacientemente.

Los procedimientos deberán ser de ejecución obligatoria y bajo la responsabilidad de los encargados de la realización de los mismos, debiendo haber procesos de verificación de su cumplimiento. En estos procedimientos estará involucrado todo el personal de la Institución.

Los procedimientos de planes de recuperación de desastres deben de emanar de la máxima autoridad Institucional, para garantizar su difusión y estricto cumplimiento.

Las actividades a realizar en un Plan de Recuperación de Desastres se pueden clasificar en tres etapas:

6.1.1 Actividades Previas al Desastre.

6.1.2 Actividades Durante el Desastre.

6.1.3 Actividades Después del Desastre.

6.1.1 Actividades Previas al Desastre

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de la información, que nos aseguren un proceso de Recuperación con el menor costo posible a nuestra Institución.
Podemos detallar las siguientes Actividades Generales :

- Establecimiento del Plan de Acción.
- Formación de Equipos Operativos.
- Formación de Equipos de Evaluación (auditoría de cumplimiento de los procedimientos sobre Seguridad).

➢ **Establecimiento de Plan de Acción**

En esta fase de Planeamiento se debe de establecer los procedimientos relativos a:

a) Sistemas e Información.

b) Equipos de Cómputo.

c) Obtención y almacenamiento de los Respaldos de Información (BACKUPS).

d) Políticas (Normas y Procedimientos de Backups).

a) Sistemas e Información. La Institución deberá tener una relación de los Sistemas de Información con los que cuenta, tanto los realizados por el centro de cómputo como los hechos por las áreas usuarias. Debiendo identificar toda información sistematizada o no, que sea necesaria para la buena marcha Institucional.

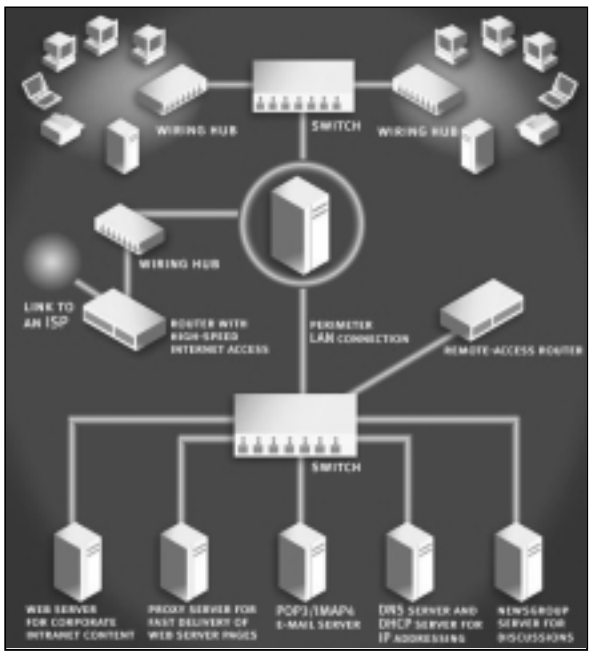
La relación de Sistemas de Información deberá detallar los siguientes datos:

- Nombre del Sistema.
- Lenguaje o Paquete con el que fue creado el Sistema. Programas que lo conforman (tanto programas fuentes como programas objetos, rutinas, macros, etc.).
- La Dirección (Gerencia, Departamento, etc.) que genera la información base (el «dueño» del Sistema).
- Las unidades o departamentos (internos/externos) que usan la información del Sistema.
- El volumen de los archivos que trabaja el Sistema.
- El volumen de transacciones diarias, semanales y mensuales que maneja el sistema.

- El equipamiento necesario para un manejo óptimo del Sistema.
- La(s) fecha(s) en las que la información es necesitada con carácter de urgencia.
- El nivel de importancia estratégica que tiene la información de este Sistema para la Institución (medido en horas o días que la Institución puede funcionar adecuadamente, sin disponer de la información del Sistema). Equipamiento mínimo necesario para que el Sistema pueda seguir funcionando (considerar su utilización en tres turnos de trabajo, para que el equipamiento sea el mínimo posible).
- Actividades a realizar para volver a contar con el Sistema de Información (actividades de Restore).

Con toda esta información se deberá de realizar una lista priorizada (un ranking) de los Sistemas de Información necesarios para que la Institución pueda recuperar su operatividad perdida en el desastre (contingencia).

b) Equipos de Cómputo. Aparte de las Normas de Seguridad que se verán en los capítulos siguientes, hay que tener en cuenta:



- Inventario actualizado de los equipos de manejo de información (computadoras, lectoras de microfichas, impresoras, etc.), especificando su contenido (software que usa, principales archivos que contiene), su ubicación y nivel de uso Institucional.

- Pólizas de Seguros Comerciales. Como parte de la protección de los Activos Institucionales, pero haciendo la salvedad en el contrato, que en casos de siniestros, la restitución del Computador siniestrado se podrá hacer por otro de mayor potencia (por actualización tecnológica), siempre y cuando esté dentro de los montos asegurados.
- Señalización o etiquetado de los Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo etiquetar (colocar un sticker) de color rojo a los Servidores, color amarillo a las PC's con Información importante o estratégica y color verde a las PC's de contenidos normales.

- Tener siempre actualizada una relación de PC's requeridas como mínimo para cada Sistema permanente de la Institución (que por sus funciones constituyen el eje central de los Servicios Informáticos de la Institución), las funciones que realizaría y su posible uso en dos o tres turnos de trabajo, para cubrir las funciones básicas y prioritarias de cada uno de estos Sistemas.

c) Obtención y Almacenamiento de los Respaldos de Información (BACKUPS).

Se deberá establecer los procedimientos para la obtención de copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los Sistemas o aplicativos de la Institución. Para lo cual se debe contar con:

- Backups del Sistema Operativo (en caso de tener varios Sistemas Operativos o versiones, se contará con una copia de cada uno de ellos).

- Backups del Software Base (Paquetes y/o Lenguajes de Programación con los cuales han sido desarrollados o interactúan nuestros Aplicativos Institucionales).

- Backups del Software Aplicativo (Considerando tanto los programas fuentes, como los programas objetos correspondientes, y cualquier otro software o procedimiento que también trabaje con la data, para producir los resultados con los cuales trabaja el usuario final). Se debe considerar también las copias de los listados fuentes de los programas definitivos, para casos de problemas.

- Backups de los Datos (Bases de Datos, Indices, tablas de validación, passwords, y todo archivo necesario para la correcta ejecución del Software Aplicativo de nuestra Institución).

- Backups del Hardware. Se puede implementar bajo dos modalidades:

  Modalidad Externa. Mediante convenio con otra Institución que tenga equipos similares o mayores y que brinden la seguridad de poder procesar nuestra Información, y ser puestos a nuestra disposición, al ocurrir una contingencia y mientras se busca una solución definitiva al siniestro producido. Este tipo de convenios debe tener tanto las consideraciones de equipamiento como de ambientes y facilidades de trabajo que cada institución se compromete a brindar, y debe de ser actualizado cada vez que se efectúen cambios importantes de sistemas que afecten a cualquiera de las instituciones.

  Modalidad Interna. Si tenemos más de un local, en ambos debemos tener señalados los equipos, que por sus características técnicas y capacidades, son susceptibles de ser usados como equipos de emergencia del otro local, debiéndose poner por

escrito (igual que en el caso externo), todas las actividades a realizar y los compromisos asumidos.

En ambos casos se deberá probar y asegurar que los procesos de restauración de Información posibiliten el funcionamiento adecuado de los Sistemas. En algunos casos puede ser necesario volver a recompilar nuestro software aplicativo bajo plataformas diferentes a la original, por lo que es imprescindible contar con los programas fuentes, al mismo grado de actualización que los programas objeto.

d) Políticas (Normas y Procedimientos de Backups)

Se debe establecer los procedimientos, normas, y determinación de responsabilidades en la obtención de los Backups mencionados anteriormente en el punto «c», debiéndose incluir:

- Periodicidad de cada Tipo de Backup.
- Respaldo de Información de movimiento entre los períodos que no se sacan Backups (backups incrementales).
- Uso obligatorio de un formulario estándar para el registro y control de los Backups.
- Correspondencia entre la relación de Sistemas e Informaciones necesarias para la buena marcha de la empresa, y los backups efectuados.
- Almacenamiento de los Backups en condiciones ambientales óptimas, dependiendo del medio magnético empleado.
- Reemplazo de los Backups, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar (reciclaje o refresco).
- Almacenamiento de los Backups en locales diferentes donde reside la información primaria (evitando la pérdida si el desastre alcanzo todo el edificio o local estudiado).
- Pruebas periódicas de los Backups (Restore), verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.

➢ **Formación de Equipos Operativos**

En cada unidad operativa de la Institución, que almacene información y sirva para la operatividad Institucional, se deberá designar un responsable de la seguridad de la Información de su unidad. Pudiendo ser el jefe de dicha Area Operativa.

Sus labores serán:

- Ponerse en contacto con los propietarios de las aplicaciones y trabajar con ellos.

- Proporcionar soporte técnico para las copias de respaldo de las aplicaciones.
- Planificar y establecer los requerimientos de los sistemas operativos en cuanto a archivos, bibliotecas, utilitarios, etc., para los principales sistemas y subsistemas.
- Supervisar procedimientos de respaldo y restauración.
- Supervisar la carga de archivos de datos de las aplicaciones, y la creación de los respaldos incrementales.
- Coordinar líneas, terminales, módem, otros aditamentos para comunicaciones.
- Establecer procedimientos de seguridad en los sitios de recuperación.
- Organizar la prueba de hardware y software.
- Ejecutar trabajos de recuperación.
- Cargar y probar archivos del sistema operativo y otros sistemas almacenados en el local alternante.
- Realizar procedimientos de control de inventario y seguridad del almacenamiento en el local alternante.
- Establecer y llevar a cabo procedimientos para restaurar el lugar de recuperación.
- Participar en las pruebas y simulacros de desastres.

➢ **Formación de Equipos de Evaluación (Auditoría de cumplimiento de los procedimientos sobre Seguridad)**

Esta función debe ser realizada de preferencia por personal de Inspectoría, de no ser posible, la realizará el personal del área de Informática, debiendo establecerse claramente sus funciones, responsabilidades y objetivos :

- Revisar que las Normas y procedimientos con respecto a Backups y seguridad de equipos y data se cumpla.
- Supervisar la realización periódica de los backups, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.
- Revisar la correlación entre la relación de Sistemas e Informaciones necesarios para la buena marcha de la Institución, y los backups realizados.
- Informar de los cumplimientos e incumplimientos de las Normas, para las acciones de corrección respectivas.

6.1.2 Actividades Durante el Desastre

Una vez presentada la Contingencia o Siniestro, se deberá ejecutar las siguientes actividades, planificadas previamente:

a) Plan de Emergencias.

b) Formación de Equipos.

c) Entrenamiento.

a) Plan de Emergencias

En este plan se establecen las acciones se deben realizar cuando se presente un Siniestro, así como la difusión de las mismas.

Es conveniente prever los posibles escenarios de ocurrencia del Siniestro:

Durante el día.
Durante la Noche o madrugada.

Este plan deberá incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, debiendo detallar :

- Vías de salida o escape.
- Plan de Evacuación del Personal.
- Plan de puesta a buen recaudo de los activos (incluyendo los activos de Información) de la Institución (si las circunstancias del siniestro lo posibilitan)
- Ubicación y señalización de los elementos contra el siniestro (extinguidores, cobertores contra agua, etc.)
- Secuencia de llamadas en caso de siniestro, tener a la mano: elementos de iluminación (linternas), lista de teléfonos de Bomberos / Ambulancia, Jefatura de Seguridad y de su personal (equipos de seguridad) nombrados para estos casos.

b) Formación de Equipos

Establecer claramente cada equipo (nombres, puestos, ubicación, etc.) con funciones claramente definidas a ejecutar durante el siniestro.

Si bien la premisa básica es la protección de la Integridad del personal, en caso de que el siniestro lo permita (por estar en un inicio o estar en una área cercana, etc.), deberá de existir dos equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y otro para el salvamento de los recursos Informáticos, de acuerdo a los lineamientos o clasificación de prioridades.

c) Entrenamiento

Establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestros, de acuerdo a los roles que se le hayan asignado en los planes de evacuación del personal o equipos, para minimizar costos se puede aprovechar fechas de recarga de extinguidores, charlas de los proveedores, etc.

Un aspecto importante es que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los elementos directivos, dando el ejemplo de la importancia que la alta dirección otorga a la Seguridad Institucional.

6.1.3 Actividad Después del Desastre

Después de ocurrido el Siniestro o Desastre es necesario realizar las actividades que se detallan, las cuales deben estar especificadas en el Plan de Acción.

a) Evaluación de Daños.

b) Priorización de Actividades del Plan de Acción.

c) Ejecución de Actividades.

d) Evaluación de Resultados.

e) Retroalimentación del Plan de Acción.

a) Evaluación de Daños.

Inmediatamente después que el siniestro ha concluido, se deberá evaluar la magnitud del daño que se ha producido, que sistemas se están afectando, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.

Adicionalmente se deberá lanzar un pre-aviso a la Institución con la cual tenemos el convenio de respaldo, para ir avanzando en las labores de preparación de entrega de los equipos por dicha Institución.

b) Priorización de Actividades del Plan de Acción.

Toda vez que el Plan de Acción es general y contempla una pérdida total, la evaluación de daños reales y su comparación contra el Plan, nos dará la lista de las actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de nuestra Institución.

Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, para ver su asignamiento temporal a las

actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

c) Ejecución de Actividades.

La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas en el Plan de acción. Cada uno de estos equipos deberá contar con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato a la jefatura a cargo del Plan de Contingencias.

Los trabajos de recuperación tendrán dos etapas, la primera la restauración del servicio usando los recursos de la Institución o local de respaldo, y la segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio de nuestro Sistema e imagen Institucional, como para no perjudicar la operatividad de la Institución o local de respaldo.

d) Evaluación de Resultados

Una vez concluidas las labores de Recuperación del (los) Sistema(s) que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción, como se comportaron los equipos de trabajo, etc.

De la Evaluación de resultados y del siniestro en si, deberían de salir dos tipos de recomendaciones, una la retroalimentación del plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

e) Retroalimentación del Plan de Acción.

Con la evaluación de resultados, debemos de optimizar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

El otro elemento es evaluar cual hubiera sido el costo de no haber tenido nuestra Institución el plan de contingencias llevado a cabo.

FASE 7 : IMPLEMENTACION

La fase de implementación se da cuando han ocurrido o están por ocurrir los problemas para este caso se tiene que tener preparado los planes de contingencia para poder aplicarlos. Puede también tratarse esta etapa como una prueba controlada.

7.1 De las Emergencia Físicas

CASO A: Error Físico de Disco de un Servidor (Sin RAID).

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

1. Ubicar el disco malogrado.
2. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
3. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
4. Bajar el sistema y apagar el equipo.
5. Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle partición.
6. Restaurar el último backup en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
7. Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.
8. Habilitar las entradas al sistema para los usuarios.

CASO B: Error de Memoria RAM

En este caso se dan los siguiente síntomas:

- El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.
- Ante procesos mayores se congela el proceso.
- Arroja errores con mapas de direcciones hexadecimales.
- Es recomendable que el servidor cuente con ECC (error correct checking), por lo tanto si hubiese un error de paridad, el servidor se autocorregirá.

Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la compañía, a menos que la dificultad apremie, cambiarlo inmediatamente.

Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
2. El servidor debe estar apagado, dando un correcto apagado del sistema.
3. Ubicar las memorias malogradas.
4. Retirar las memorias malogradas y reemplazarlas por otras iguales o similares.
5. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.

6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
7. Probar los sistemas que están en red en diferentes estaciones.
8. Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios.

CASO C: Error de Tarjeta(s) Controladora(s) de Disco

Se debe tomar en cuenta que ningún proceso debe quedar cortado, debiéndose ejecutar las siguientes acciones:

1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
2. El servidor debe estar apagado, dando un correcto apagado del sistema.
3. Ubicar la posición de la tarjeta controladora.
4. Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar.
5. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
7. Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.

CASO D: Caso de Incendio Total

En el momento que se dé aviso por los altavoces de alguna situación de emergencia general, se deberá seguir al pie de la letra los siguientes pasos, los mismos que están encausados a salvaguardar la seguridad personal, el equipo y los archivos de información que tenemos en cintas magnéticas.

- Ante todo, se recomienda conservar la serenidad. Es obvio que en una situación de este tipo, impera el desorden, sin embargo, es muy recomendable tratar de conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.
- En ese momento cualquiera que sea(n) el (los) proceso(s) que se esté(n) ejecutando en el Computador Principal, se deberá enviar un mensaje (si el tiempo lo permite) de "Salir de Red y Apagar Computador", seguidamente digitar Down en el (los) servidor(es).
- Se apagará (poner en OFF) la caja principal de corriente del departamento de sistemas.
- Tomando en cuenta que se trata de un incendio de mediana o mayor magnitud, se debe tratar en lo posible de trasladar el servidor fuera del local, se abandonará el edificio en forma ordenada, lo más rápido posible, por las salidas destinadas para ello.

CASO E: Caso de Inundación

- Para evitar problemas con inundaciones se ha de instalar tarimas de un promedio de 20 cm de altura para la ubicación de los servidores. De esta manera evitaremos inconvenientes como el referido.
- En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.
- Dado el caso de que se obvió una conexión que está al ras del piso, ésta debe ser modificada su ubicación o en su defecto anular su conexión.
- Para prevenir los corto circuitos, asegurarse de que no existan fuentes de líquidos cerca a las conexiones eléctricas.
- Proveer cubiertas protectoras para cuando el equipo esté apagado.

CASO F: Caso de Fallas de Fluido Eléctrico

Se puede presentar lo siguiente:

1. Si fuera corto circuito, el UPS mantendrá activo los servidores y algunas estaciones, mientras se repare la avería eléctrica o se enciende el generador.
2. Para el caso de apagón se mantendrá la autonomía de corriente que el UPS nos brinda (corriente de emergencia(*)), hasta que los usuarios completen sus operaciones (para que no corten bruscamente el proceso que tienen en el momento del apagón), hasta que finalmente se realice el By-pass de corriente con el grupo electrógeno, previo aviso y coordinación.
3. Cuando el fluido eléctrico de la calle se ha restablecido se tomarán los mismos cuidados para el paso de grupo electrógeno a corriente normal (o UPS).

***** Llámese corriente de emergencia a la brindada por grupo electrógeno y/o UPS.
****** Llámese corriente normal a la brindada por la compañía eléctrica.
******* Se contará con transformadores de aislamiento (nivelan la corriente) asegurando que la corriente que entre y salga sea 220v, evitando que los equipos sufran corto circuito por elevación de voltaje (protegiendo de esta manera las tarjetas, pantallas y CPU del computador).

7.2 De las Emergencias Lógicas de Datos

CASO A: Error Lógico de Datos

La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:

- Caída del servidor de archivos por falla de software de red.
- Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.
- Bajar incorrectamente el servidor de archivos.
- Fallas causadas usualmente por un error de chequeo de inconsistencia física.

En caso de producirse alguna de las situaciones descritas anteriormente; se deben realizar las siguientes acciones:

PASO 1: Verificar el suministro de energía eléctrica. En caso de estar conforme, proceder con el encendido del servidor de archivos, una vez mostrado el prompt de Dos, cargar el sistema operativo de red.

PASO 2: Deshabilitar el ingreso de usuarios al sistema.

PASO 3: Descargar todos los volúmenes del servidor, a excepción del volumen raíz. De encontrarse este volumen con problemas, se deberá descargarlo también.

PASO 4: Cargar un utilitario que nos permita verificar en forma global el contenido del(os) disco(s) duro(s) del servidor.

PASO 5: Al término de la operación de reparación se procederá a habilitar entradas a estaciones para manejo de soporte técnico, se procederá a revisar que las bases de datos índices estén correctas, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente.

Si se presenta el caso de una o varias bases de datos no reconocidas como tal, se debe recuperar con utilitarios.

CASO B: Caso de Virus

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:

Para servidor:

- Se contará con antivirus para el sistema que aíslan el virus que ingresa al sistema llevándolo a un directorio para su futura investigación
- El antivirus muestra el nombre del archivo infectado y quién lo usó.
- Estos archivos (exe, com, ovl, nlm, etc.) serán reemplazados del diskett original de instalación o del backup.
- Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

Para computadoras fuera de red:

Se revisará las computadoras que no estén en red con antivirus de disquete.
De suceder que una computadora se haya infectado con uno o varios virus ya sea en la memoria o a nivel disco duro, se debe proceder a realizar los siguientes pasos:

1. Utilizar un disquete que contenga sistema operativo igual o mayor en versión al instalado en el computador infectado. Reiniciar el computador con dicho disquete.
2. Retirar el disquete con el que arrancó el computador e insertar el disquete antivirus, luego activar el programa de tal forma que revise todos los archivos y no sólo los ejecutables. De encontrar virus, dar la opción de eliminar el virus. Si

es que no puede hacerlo el antivirus, recomendará borrar el archivo, tomar nota de los archivos que se borren. Si éstos son varios pertenecientes al mismo programa, reinstalar al término del Scaneado. Finalizado el scaneado, reconstruir el Master Boot del disco duro

FASE 8 : MONITOREO

La fase de Monitoreo nos dará la seguridad de que podamos reaccionar en el tiempo preciso y con la acción correcta. Esta fase es primordialmente de mantenimiento. Cada vez que se da un cambio en la infraestructura, debemos de realizar un mantenimiento correctivo o de adaptación.

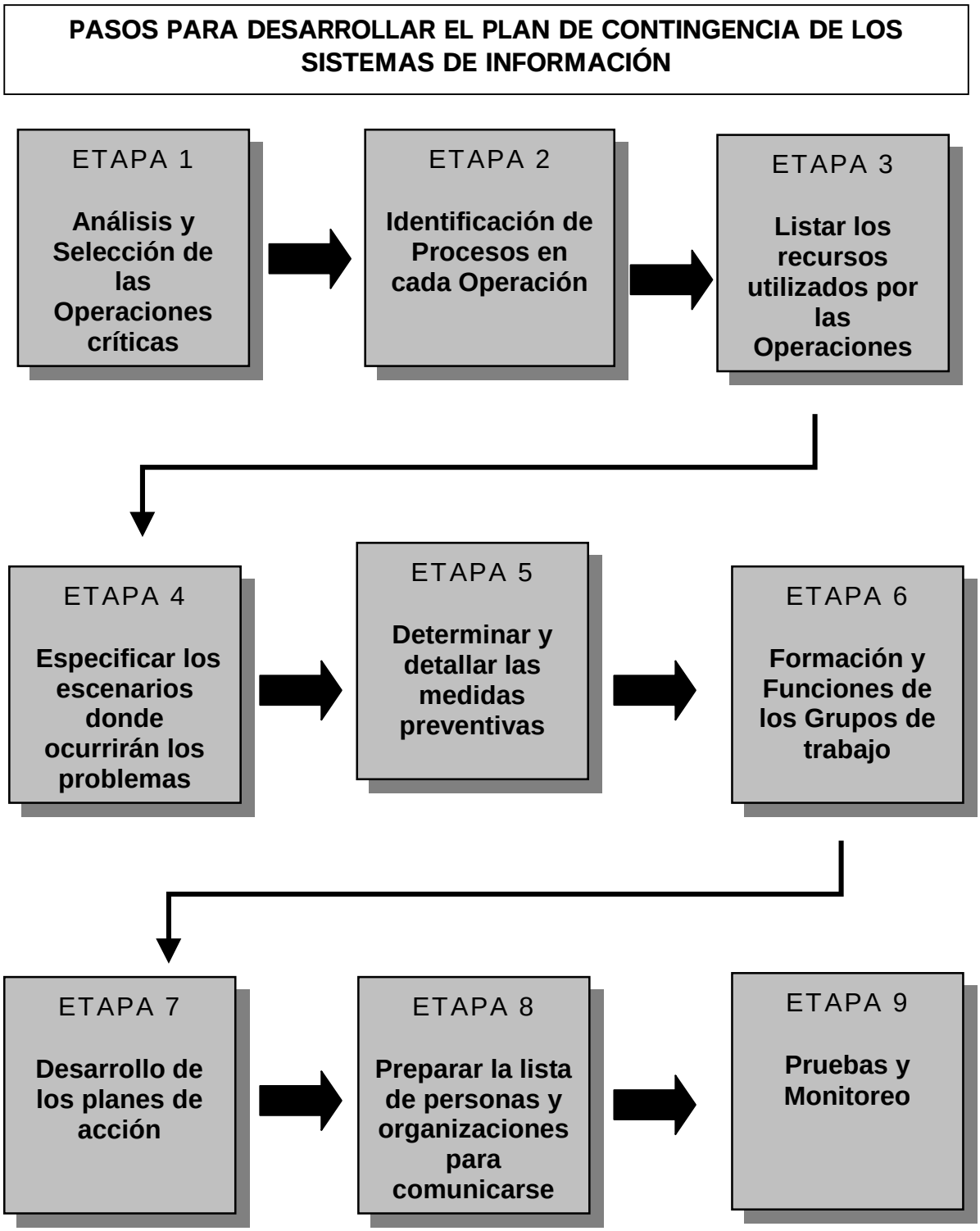
Un punto donde se tiene que actuar es por ejemplo cuando se ha identificado un nuevo riesgo o una nueva solución. En este caso, toda la evaluación del riesgo se cambia, y comienza un nuevo ciclo completo, a pesar de que este esfuerzo podría ser menos exigente que el primero.

Esto es importante ya que nos alimentamos de las nuevas posibilidades de soluciones ante nuevos casos que se puedan presentar.

Podríamos enumerar las actividades principales a realizar:

- Desarrollo de un mapa de funciones y factores de riesgo.
- Establecer los procedimientos de mantenimiento para la documentación y la rendición de informes referentes a los riesgos.
- Revisión continua de las aplicaciones.
- Revisión continua del sistema de backup
- Revisión de los Sistemas de soporte eléctrico del Centro de Procesamiento de Datos.

Capítulo III: Visión Práctica para realizar un Plan de Contingencia de los Sistemas de Información



ETAPA I : Análisis y Selección de las Operaciones Críticas

En esta etapa hay que definir cuales serán nuestras operaciones críticas y tienen que ser definidas en función a los componentes de los sistemas de información los cuales son: Datos, Aplicaciones, Tecnología Hardware y Software, instalaciones y personal.

Dentro de las cuales podemos identificar las siguientes, las cuales pueden variar de sistema a sistema :

- Reportes Impresos de Informes del Sistema.
- Consultas a las Bases de Datos vía Internet.
- Consultas a las Bases de Datos vía LAN.
- Sistema de Backup y Recuperación de Data.
- Sistema de ingreso y modificación en la Base de Datos de documentos que llegan y salen al exterior.
- Los Servidores de Bases de Datos y Aplicaciones.
- Los Servicios de Red.
- Los Medios de Transmisión.
- Las Topologías de Red.
- Los Métodos de control de acceso.

Se ha listado los procesos críticos de manera genérica y evaluado su grado de importancia en función a la magnitud del impacto si los procesos pueden detenerse, y luego clasificados en niveles **H** (Alta), **R** (Regular) y **L** (Bajo)

Se tiene que elaborar una tabla denominada Operaciones Críticas de los SI, que consta de tres campos:

- Operaciones críticas
- Objetivo de la Operación
- Prioridad de la Operación

CUADRO 1. OPERACIONES CRITICAS DEL SISTEMA DE INFORMACION

Operaciones Críticas	Objetivos de la Operación	Prioridad de la Operación
Reportes Impresos de Informes del Sistema	■ Informes de los estados financieros de la organización. ■ Informes de plantillas del personal. ■ Informes de producción mensual, anual.	R
Consultas a las Bases de Datos vía Internet	■ Informes a los clientes. ■ Información a los proveedores. ■ Sistema de ventas vía Internet.	L
Consultas a las Bases de Datos vía LAN	■ Inventarios ■ Revistas, electrónicas.	R

Operaciones Críticas	Objetivos de la Operación	Prioridad de la Operación
Sistema de Backup y Recuperación de Data	■ Procesos de Backups de la información. ■ Establecimiento de las frecuencias de almacenamiento de datos.	H
Sistema de Ingreso y modificación en la Base de Datos de documentos que llegan y salen al exterior.	■ Proceso de los programas que realizan la entrada y salida de la información. ■ Mantenimiento adecuado de las aplicaciones. ■ Equipamiento necesario para un funcionamiento optimo del sistema.	H

H = Alta **R = Regular** **L = Baja**

Se ha tomado solo estas operaciones como modelo para detallar el desarrollo del Plan, pero cabe recordar que debemos de tener muy en cuenta que hay mas operaciones que son críticas y que debemos tener cuidado al identificarlas ya que esto contribuirá para el buen desarrollo del Sistema de Información de su organización, es por eso que debemos de analizar con cuidado para no tener problemas posteriores.

CUADRO 2: PROCESOS ESTRATEGICOS DEL NEGOCIO

OPERACION PRINCIPAL	CONTENIDO DE LA OPERACION	PRIORIDAD DE LA OPERACION
VENTAS (A)	■ Ventas a los clientes	R
ORDENES ACEPTADAS (B)	■ Aceptar órdenes de los clientes ■ Administración de las ventas a crédito	H
ENVIO Y REPARTO (C)	■ Administración del inventario ■ Envío de productos ■ Reparto de las ventas a crédito	H
COMPRA (D)	■ Dando órdenes a los fabricantes ■ Administración de la compra a crédito	H
PRODUCCIÓN (E)	■ Fabricación	H
ESTADÍSTICAS (F)	■ Estadísticas mensuales ■ Estadísticas anuales	R
ELABORACION DE INFORMES DE LA ADMINISTRACIÓN (G)	■ Elaboración de reportes totales de Administración	L

H = Alta **R = Regular** **L = Baja**

- Para cada una de las operaciones principales, enumerar sus procesos.
- Investigar qué recursos de la empresa (equipamiento, herramientas, sistemas, etc.) son usados, descríbalos y enumérelos.

CUADRO 3 : ANALISIS SOBRE UN PROCESO DEL NEGOCIO

Nombre de la operación : ***Aceptación de órdenes***

NÚMERO DE PROCEDIMIENTOS	PROCESOS DE NEGOCIOS	RECURSOS USADOS	NUMERO DE SERIE DEL RECURSO	ORDENES ó NOTAS
B – 1	**Recepción de órdenes de pedido**	Teléfonos fijos	S1	Clientes E y F
		PC´s	S2	Clientes G
		Líneas dedicadas	S3	Clientes H
B – 2	**Confirmar la cantidad total límite de órdenes recibidas**	Sistema de aceptación de la orden (Software)	S4	
B – 3	**Confirmar si se cuenta con el Stock para atender los pedidos**	Sistema de aceptación de la orden	S4	
B – 4	**Registrar las órdenes**	Sistema de aceptación de la orden	S4	
B – 5	**Enviar las confirmaciones de órdenes (faxearlas automáticamente)**	Sistema de aceptación de la orden	S4	
		Faxes	S2	De nosotros para los clientes
B – 6	**Indicar el envío o remitirlas a sus respectivos centros**	Sistema de aceptación de la orden	S4	
		Líneas dedicadas	S3	De los Grupos de Trabajo a los centros de reparto

- Se utiliza las nomenclaturas para identificar los procedimientos y a que proceso pertenece.
- Enumerar Recursos Utilizados para los Procesos
- Describir ubicaciones de proveedores de servicios por los procesos de cada operación.
- Investigue y describa a los proveedores de servicios.

CUADRO 4: LISTA DE RECURSOS UTILIZADOS

N° Serie del Recurso	Recurso	Ubicación	Proveedor del Servicio	Recursos de operaciones utilizados por
S1-1	Pc's	Externo	Proveedor A	B-1
S1-2		Interno	Soporte técnico	B-1
S2-1	Software de Administración de compras	Externo	Proveedor A	B-1, B-5, K-1
S2-2		Interno	Soporte técnico	B-1, K-1
S3	Líneas dedicadas	Externo	Teléfono A (Red)	B-1, B-6, K-1
S4-1	Sistema de aceptación de orden (Software Base)	Interno	Desarrollo interno (aplicación)	B-2, B-3, B-4, B-5, B-6, S-10, N-1, N-6, N-7, N-11
S4-2		Interno	Electrónica B (Hardware y otros)	B-2, B-3, B-4, B-5, B-6, S-1, S-6, S-10, N-1, N-2, N-3, N-7, N-11
S5	Almacén automatizado	Interno	Maquinaria Q	N-2, N-3
S6	Maquinaria de embolsado	Interno	Maquinaria de precisión R	N-4
S7	Elevadores del almacén	Interno	Industria pesada S	S-9, K-5
S8	Camiones internos	Interno	Motores T	S-7, N-9
S9	Servicio de reparto a domicilio	Externo	Transporte L	N-9
S10	Servidores	Interno	Electrónica B	B-1, B-2, B-3 B-4,N-1
S11	Software Clientes	Interno	Desarrollo Interno	B1- , N-9 , B-2 , B-3

- Estudio Puntual de Fallas
- Considerando el contenido de cada operación, determinar cuanto tiempo una interrupción puede ser tolerada.
- Describir con que frecuencia se utiliza un recurso y que tiempo una parada o interrupción bloquea la operación.

CUADRO 5: LISTA DEL PERIODOS ACEPTABLES DE INTERRUPCION

N° Serie del Recurso	Recurso	Recursos de operaciones utilizados por	Frecuencia de uso	Período aceptable de Interrupción
S1-1	PC´s (Red)	B-1	Cada día	Medio día
S1-2	PC´s (Red)	B-1	Cada día	Medio día
S2-1	Software (Red)	B-1	Cada día	Medio día
		K-1	Cada día	Medio día
S2-2	Software de administración de Compras	B-1	Cada día	Medio día
		B-5	Cada día	Medio día
		K-1	Cada día	Medio día

N° Serie del Recurso	Recurso	Recursos de operaciones utilizados por	Frecuencia de uso	Período aceptable de Interrupción
S3	Líneas dedicadas	B-1	Cada día	Medio día
		B-6	Cada noche	Un día
		K-1	Cada 3 días	3 días
S4-1	Sistema de aceptación de orden	B-2	Cada día	Medio día
		B-3	Cada día	Medio día
		B-4	Cada día	Medio día
S10	Servidores	B-1	Cada día	3 horas
S11	Software Cliente	B1,B3, B5	Cada día	3 horas

- Estudie y describe el estado de fabricación de los productos que constituyen recursos
- Las soluciones varían según el período asumido de la parada.
- Calcular y describir el período que se pasará hasta la recuperación del elemento afectado, basado en la información confirmada

CUADRO 6 : LISTA DE PROBLEMAS PROBABLES A OCURRIR

N° Serie del Recurso	Recurso	Proveedor del Servicio	Resultados confirmados	Juicio de compañías	
			Condiciones de preparación de las medidas preventivas	Posibilidad del problema	Periodo necesario para la recuperación
S10	Servidores	Electrónica (Red)	Preparación de las medidas preventivas	Pequeña	3 Horas
S11-1	Software Clientes	Desarrollo (Red)	Preparación de las medidas preventivas	Pequeña	3 horas
S11-2		Electrónica O (Fax)	Equipos listos para los problemas de los sistema de información	Pequeña	3 horas
S3	Líneas dedicadas	Teléfono A (Red)	Preparación de las medidas preventivas	Pequeña	Medio día
S4-1	Sistema de aceptación de orden (Software Base)	Desarrollo interno (aplicación)	Preparación de las medidas preventivas	Media	2 días
S4-2		Electrónica B (Hardware)	Preparación de las medidas preventivas	Pequeña	5 días
S5	Almacén automatizado	Industrial Q	Preparación de las medidas preventivas	Pequeña	2 días
S7	Elevadores del almacén	Industria pesada S	Las partes que pueden tener problemas son reemplazadas y las máquinas examinadas	Pequeña	3 días
S9	Servicio de reparto a domicilio	Transporte L	Preparación de las medidas preventivas	Grande	2 días
S2	Sistema de Administración de la Compra	Desarrollo interno (aplicación)	Preparación de las medidas preventivas	Media	7 días

ETAPA 2. Identificación de Procesos en Cada Operación

Para cada una de las operaciones críticas en la Etapa 1, se debe enumerar los procesos que tienen.

Los responsables de desarrollar los planes de contingencia deben de coordinar en cooperación con el personal a cargo de las operaciones de los Sistemas Analizados, los cuales son conocedores de dichos procesos críticos.

Se debe de investigar que recursos administrativos (equipamiento, herramientas, sistemas, etc.) son usados en cada proceso, se ha descrito y codificado cada recurso, como: sistema eléctrico, tarjetas, transporte, red de datos, PC's. A su vez también se ha determinado su novel de riesgo, como críticos y no críticos.

La tabla elaborada contiene cinco campos:

- Código de procedimientos
- Procesos
- Recursos Utilizados
- Código del Recurso
- Nivel de Riesgo

CUADRO 7. PROCESOS DEL AREA ANALIZADA (E)

Código del Proceso	Procesos	Plan de Contingencia	Código del recurso	Nivel del Riesgo
E- 1	Proceso de los programas que realizan la entrada y salida de la información	Sistema Eléctrico	R1	Crítico
		Red de Datos	R2	Crítico
		Servidores	R3	Crítico
		Sistemas de Gestión	R4	Crítico
		Impresoras	R5	No Crítico
		Humanos	R6	No Crítico
		PC's	R7	Crítico
E - 2	Mantenimiento adecuado de las aplicaciones	Sistema Eléctrico	R1	Crítico
		Red de Datos	R2	Crítico
		Servidores	R3	Crítico
		PC's	R7	Crítico
		Impresoras	R5	No Crítico
		Humanos	R6	No Crítico
		Teléfono	R8	Crítico
		Humanos	R6	No Crítico
		PC's	R7	Crítico
		Servidores	R3	Crítico
		Red de Datos	R2	Crítico
		Teléfono	R8	Crítico

Mediante la siguiente tabla de costos, podremos identificar cuales son los procesos que representan mayor costo y posteriormente utilizar esta información para evaluar la prioridad de acciones frente a los procedimientos en nuestra tabla de prioridades.

CUADRO 8. FORMATO DE COSTOS DE CADA PROCESO

CODIGO DE PROCESO	PROCESOS	COSTOS REPRESENTATIVOS (US $)
A	Ventas	10,000
B	Aceptación de Ordenes	500
C	Envió y Reparto	2,500
D	Compras	50,000
E	Producción	80,000
F	Estadísticas	5,000
G	Elaboración de Informes de la Administracion	1,000

Podemos personalizar nuestra tabla de costos según nuestro caso y detallarla según lo mas realistamente posible, ya que de esto dependerá el darle la prioridad necesaria a cierto tipo de procesos los cuales quizás no puedan ser identificadas a simple inspección.

ETAPA 3. Listar los Recursos Utilizados por las Operaciones

En esta etapa se identifica a los proveedores de los servicios y recursos usados, considerados críticos, para los procesos de cada operación en la Etapa 2.

- Se tiene que identificar los recursos asociados al Sistema de Información, basados en los códigos del recurso descritos en la etapa 2.
- Se investiga y describe, si los recursos están dentro del Sistema de Información o fuera de este, (como compra a otros proveedores de servicios externos o productos).
- Se investiga y describe a los proveedores de servicios y recursos.
- La importancia de un mismo recurso difiere de operación en operación. Para esto se señala a que operaciones esta relacionado el mismo recurso, esto es necesario para determinar las medidas preventivas para posibles problemas del Sistema de Información.

El cuadro 9 contiene los siguientes campos:

- Código del Recurso
- Recurso
- Ubicación
- Proveedor del Servicio
- Recurso de Operaciones utilizados por

CUADRO 9. LISTA DE RECURSOS CRITICOS UTILIZADOS E

Código del Recurso	Recursos	Ubicación	Proveedor del Servicio	Recursos Utilizados Por
S1	PC´s (Red)	Interno	Area de Soporte	E1,E2.E3
S2	Software de Administración de compras	Interno	Area de Soporte	E1,E2,E3
S10	Servidores	Interno	Area de Soporte	E1,E2,E3
S4	Software de Gestión de órdenes (Software de los diferentes módulos que tiene la organización)	Interno	Area de Desarrollo de Software	E1
S1-2	PC's	Interno	Area de Soporte	E1,E2,E3
S11	Software Cliente	Externo	Proveedor	E2,E3
		Interno	Soporte Técnico	E2,E3

ETAPA 4. Especificación de Escenarios en los Cuales Pueden Ocurrir los Problemas

- En consideración de la condición de preparar medidas preventivas para cada recurso, se ha evaluado su posibilidad de ocurrencia del problema como (alta, mediana, pequeña).
- Se calculará y describirá el período que se pasará hasta la recuperación en caso de problemas, basados en información confirmada relacionada con los Sistemas de Información.

Mediante el siguiente cuadro podemos elaborar la Probabilidad de fallas de cada uno de los recursos identificados

CUADRO 10. TABLA DE PROBABILIDAD DE FALLAS DE RECURSOS

Recursos	Probabiliad de Falla			
	Alta	**Media**	**Baja**	**Ninguna**
S 1	Alta	Media	Baja	
			X	
S 2	Alta	Media	Baja	
		X	**X**	
S 3	Alta	Media	Baja	
		X	**X**	
S 4	Alta	Media	Baja	
		X	**X**	
S 10	Alta	Media	Baja	
		X		
S 11	Alta	Media	Baja	
			X	

El cuadro 11 presenta los siguientes campos:

- Código del Recurso
- Recurso
- Proveedor del Servicio

- Resultados Confirmados
- Análisis de Riesgo (probabilidad del problema, período necesario para la recuperación, frecuencia de uso)

CUADRO 11. LISTA DE PROBLEMAS PROBABLES A OCURRIR

Código del Recurso	Recurso	Proveedor del Servicio (Oficina de Acción)	Resultados Confirmados	Análisis de Riesgo		
			Consideraciones de preparación de las medidas preventivas	Probabilidad del Problema	Período Necesario para la Recuperación	Frecuencia de Uso
S 1	PC´s	Soporte Técnico	Preparado	Baja	10 minutos	24 horas
S 2	Software de administración de compras	Area de Soporte	Programada a ser finalizada en 3 meses	Media/Alta	2 horas	15 horas
S 10	Servidores	Area de Soporte	Programada a ser finalizada en 3 meses	Media/Alta	2 horas	15 horas
S 4	Software de Sistemas de Aceptación de órdenes	Area de Desarrollo	Programada a ser finalizada en 2 meses	Media/Alta	2 horas	15 horas
S 11	Software Cliente	Proveedor	Programada a ser finalizada en 2 meses	Baja	2 horas	8 horas
		Soporte Técnico	Programada a ser finalizada en 2 meses	Baja	2 horas	2 horas

Mediante la siguiente tabla debemos de priorizar los riesgos identificados tomando en cuenta tanto el impacto del riesgo como la probabilidad de una falla en el área como sigue:

CUADRO 12. TABLA MATRIZ DE PRIORIDADES DE ATENCION DE RIESGOS

Impacto				
	ALTO	**Prioridad 2**	**Prioridad 1**	**Prioridad 1**
	MEDIO	**Prioridad 3**	**Prioridad 2**	**Prioridad 1**
	BAJO	**Prioridad 3**	**Prioridad 3**	**Prioridad 2**
		BAJA	**MEDIA**	**ALTA**
		Probabilidad		

En la siguiente tabla se ha descrito los procedimientos de las medidas preventivas tomadas en detalle, cuando los problemas ocurren.

Las medidas preventivas se dan si se ha probado, investigado y listado los recursos necesarios para llevarlos a cabo, tales como el equipo, manual de fallas y funcionamiento.

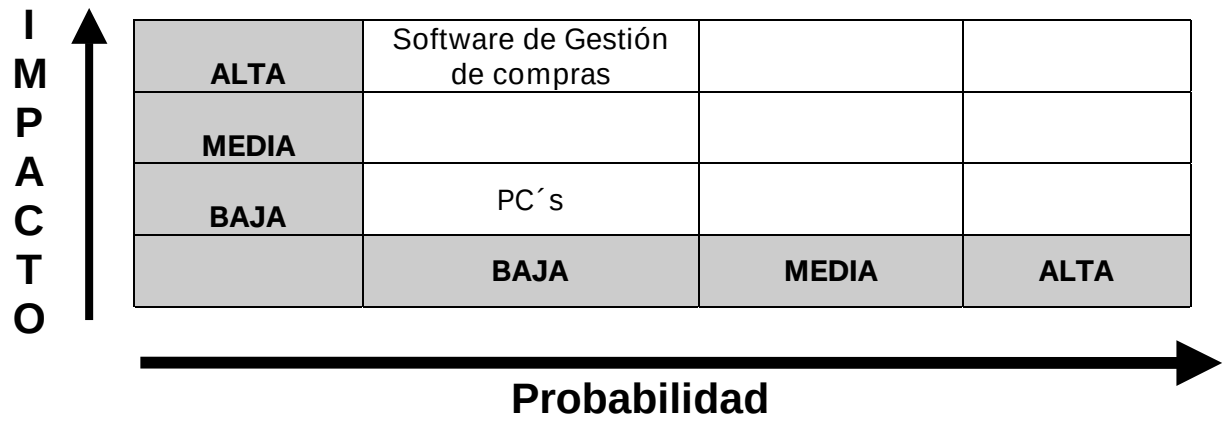
La tabla 6 presenta los siguientes campos

- Orden
- Procesos
- Procedimiento
- Recursos necesarios (medidas alternativas)

CUADRO 13. DETALLES DE MEDIDAS PREVENTIVAS DEL AREA ANALIZADA

ORDEN	PROCESOS	PROCEDIMIENTO	RECURSOS NECESARIOS (MEDIDAS ALTERNATIVAS)
1	Proceso de los programas que realizan la entrada y salida de la información	■ Ingreso y recepción de expedientes ■ (cartas, oficios, informes, etc.) ■ Envío de los documentos a todas las áreas de la institución ■ Salida de documentos(cartas, oficios, informes, etc.)	■ Puesta en funcionamiento del grupo electrógeno ■ Operaciones Manuales ■ Puesta en marcha de una red LAN interna.
2	Mantenimiento adecuado de las aplicaciones	■ Programación de cronograma de mantenimiento ■ Elaboración de órdenes de compra y órdenes de servicios	■ Puesta en funcionamiento del grupo electrógeno. ■ Comunicación con teléfonos móviles.
3	Equipamiento necesario para un funcionamiento optimo del sistema	■ Actividades de soporte técnico para casos de fallas ■ Almacén de control de bienes ■ Programación de requerimientos.	■ Puesta en funcionamiento del grupo electrógeno ■ Comunicación con teléfonos móviles. ■ Puesta en Marcha de una red LAN interna.

Como paso OPCIONAL, se pueden mostrar los riesgos en la Matriz de Análisis de Riesgo. Cada riesgo se coloca en el rectángulo. Esto corresponde a la evaluación del impacto y probabilidad de falla del área del riesgo



ETAPA 5 Determinar y Detallar las Medidas Preventivas

Se ha determinado y descrito las medidas preventivas para cada recurso utilizado en el uso y mantenimiento de los Sistemas de Información, cuando los problemas ocurran, considerando el entorno de problemas que suceden y el período de interrupción aceptable que se estima en la etapa 4.

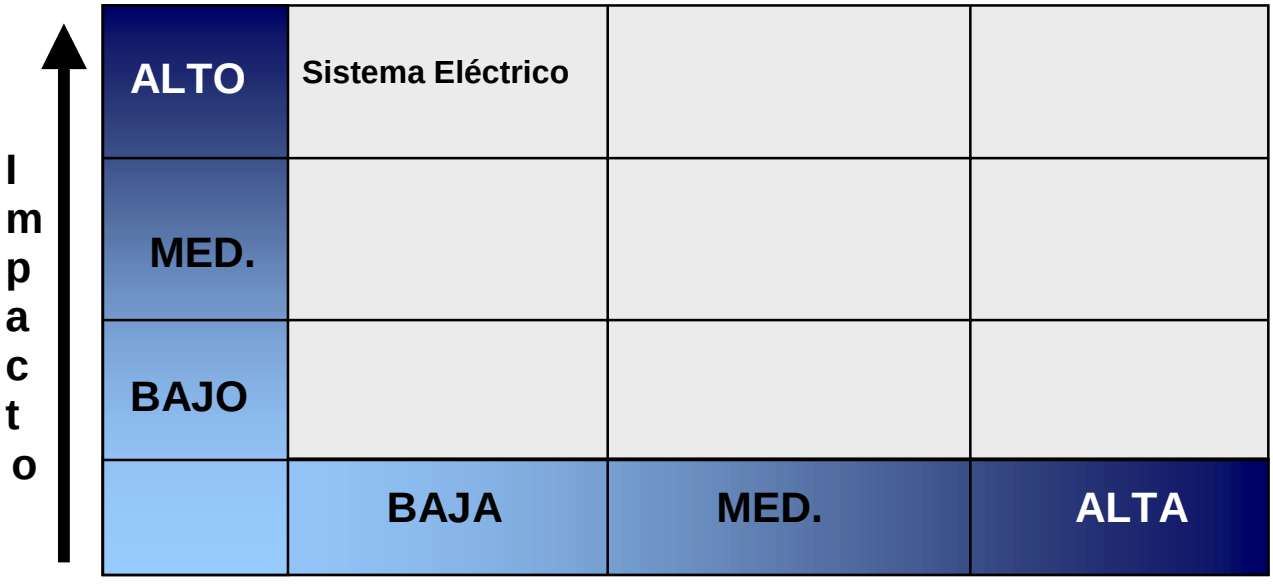
Si hay mas de un conjunto de medidas preventivas para un recurso, se ha determinado cual se empleara, para tomar en consideración sus costos y efectos.

Los campos principales considerados en la tabla 5 son los siguientes:

- Código del Recurso
- Recurso
- Problema Asumido (Análisis de Riesgo)
- Medidas preventivas / alternativas

CUADRO 14. LISTA DE MEDIDAS PREVENTIVAS

Código del Recurso	Recurso	Problema Asumido (análisis de Riesgo)		Medidas preventivas/alternativas	
		Posibilidad de ocurrencia del problema	Período de parada aceptable	Ejecutada Si o No	Contenido
S1	PC´s	Baja	Medio día	NO	Transacciones Manuales
S2	Software de administración de compras	Media/Alta	Medio día	SI	Transacciones Manuales
S3	Servidores	Media/Alta	Medio día	SI	Red Local
S4	Sistemas de Gestión	Media/Alta	2 horas	SI	Transacciones Manuales
S11	Software cliente	Baja	4 horas	NO	Transacciones Manuales



ETAPA 6. Formación y Funciones de los Grupos de Trabajo

Se debe determinar claramente los pasos para establecer los Grupos de Trabajo, desde las acciones en la fase inicial, las cuales son importantes para el manejo de la crisis de administración.

Los Grupos de Trabajo permanecerán en operación cuando los problemas ocurran, para tratar de solucionarlos.

Se elaborará un Organigrama de la estructura funcional de los Grupos de Trabajo.

CUADRO 15. FUNCIONES DE LOS GRUPOS DE TRABAJO DEL SISTEMA ADMINISTRATIVO DE LOS SISTEMAS DE INFORMACION

Dirección	Nombre	Cargo	Funciones
Área de Administración		Director Técnico	Dirección de Administración
		Especialista	Encargado de la oficina de abastecimientos y servicios auxiliares
		Especialista	Encargado de la oficina ejecutiva de personal
Área de Desarrollo de Software		Director Técnico	Dirección técnica de desarrollo de software
		Especialista	Responsable del respaldo de la información Bases de Datos y Aplicaciones
		Especialista	Responsable de configuración e instalación de los programas o aplicaciones
Dirección Técnica de Soporte		Director Técnico	Dirección técnica de soporte técnico
		Técnico	Responsable de las Pcs y Servidores
		Técnico	Responsable del Software Base
		Especialista	Responsable de Correo Electrónico
		Técnico	Soporte Técnico a usuarios

ETAPA 7. Desarrollo de los Planes de Acción

Se estableció los días en los cuales los problemas son mas probables a ocurrir, incluyendo los sistemas de la institución, clientes, proveedores e infraestructura de la organización. Se señala los días anunciados, cuando los problemas pueden ocurrir y otros temas.

El siguiente es un cuadro modelo donde debemos señalar exactamente las ocurrencias de fallas y las acciones respectivas aplicadas para cada uno de nuestras realidades.

CUADRO 16. LISTA DE ACCIONES ANTE FALLAS DE RECURSOS

Código del Recurso	Recurso	Acción	Como Confirmar	Operador	Programa para la acción	Localización para la acción	Ocurrencia del Problema
S 1	Pc´s	Confirmar la ocurrencia de los problemas	El área de administración comunicara al responsable sobre la ocurrencia del problema	Área de Administración	En la mañana del día	Todas las oficinas de la institución	Falla de los PC´s
S 2	Software de administración de compras	Confirmar la ocurrencia de los problemas	El administrador de la Red supervisará la red e informara cualquier problema	Dirección Técnica de Soporte Técnico	En todo el día	Oficinas administrativas	Caída de la red en ciertas áreas
S 3	Servidores de Gestión	Confirmar la ocurrencia de los problemas	El administrador de la red supervisará e informará cualquier problema	Dirección Técnica de Soporte técnico	En todo el día	Oficinas administrativas	Caída de la red en el área de gestión
S 10	Sistemas de Gestión	Confirmar la ocurrencia de los problemas	El administrador de los servidores supervisará e informará cualquier problema	Dirección Técnica de Soporte	En todo el día	Oficinas administrativas	Paralización o fallas en los programas o aplicaciones
S 11	Software cliente	Confirmar la ocurrencia de los problemas	Cobertura de los medios	Área de Soporte Técnico	En el día	Lugar de la persona a cargo	Caída del sistema en el área de interés.

ETAPA 8. Preparación de la Lista de Personas y Organizaciones para Comunicarse en Caso de Emergencia

Se creará un directorio telefónico del personal considerado esencial para la organización en esas fechas críticas, incluyendo el personal encargado de realizar medidas preventivas y los responsables para las acciones de la recuperación y preparación de medios alternativos.

A su vez también se creará un listado telefónico de todos los proveedores de servicio del recurso.

Este directorio se usa para realizar comunicaciones rápidas con los proveedores de servicio del recurso, incluso con los fabricantes, vendedores o abastecedores de servicio contraídos, si ocurren los problemas, para hacer que investiguen y que identifiquen las causas de los problemas y que comiencen la recuperación de los sistemas

CUADRO 17. FORMATO DE LISTA TELEFONICA DEL PERSONAL ESENCIAL EN CASO DE PROBLEMAS RELACIONADOS CON EL SISTEMA ADMINISTRATIVO

Función		Empleado	Primer Número de contacto	Segundo Número de contacto	Tiempo
Dirección	Cargo				

CUADRO 18. FORMATO DE LISTA TELEFONICA DE LOS PROVEEDORES DE SERVICIOS

Código del Recurso	Recurso	Proveedor del Servicio	Dpto. a Cargo	Sección o Persona a Cargo	Número Telefónico

TABLA DE ANALISIS DE RIESGOS

Como Resultado final deberemos elaborar un cuadro donde se muestre los principales componentes de el plan de contingencias . En la cual podremos anotar los riesgos en el siguiente Formato tabla de Análisis de Riesgo, la prioridad que tendrá la accione de determinada área afectada en función al impacto tanto funcional como de costos, así como también anotaremos su correspondiente estrategia de contingencia.

CUADRO 19. FORMATO TABLA DE ANALISIS DE RIESGOS

Area Afectada	Riesgos identificados	Impacto	Area Relacionada	Probabilidad de falla	Area de Acción	Prioridad	Estrategia de Contingencia
Todas las Oficinas	Perdida del software cliente						
Todas las Oficinas	Falla del software de administración de compras						
Todas las Oficinas	Falla de los servicios de red (servidores)						
Todas las oficinas	Falla de las PC´s						

Etapa 9 . Pruebas y Monitoreo

En esta etapa hay que desarrollar la estrategia seleccionada, implantándose con todas las acciones previstas, sus procedimientos y generando una documentación del plan.

Hay que tener en claro como pasamos de una situación normal a una alternativa, y de que forma retornamos a la situación normal. Hay situaciones en que debemos de contemplar la reconstrucción de un proceso determinado, ejemplo: por alguna circunstancia dada se determino que la facturación se realice en forma manual, restablecido el servicio que nos llevo a esta contingencia debemos tener el plan como recuperar estos datos para completar la información que día a día utilizan las demás áreas.

Antes de realizar las pruebas, los planes deberían ser revisados y juzgados independientemente en lo que respecta a su eficacia y razonabilidad.

Las pruebas recomendadas para los planes de recuperación de desastres incluyen una prueba periódica preliminar y un ensayo general, en el que se crea un simulacro de una crisis con el fin de observar la eficacia del plan. Las actividades importantes a realizar son:

- La validación de las estrategias de continuidad de los negocios de una unidad de negocios.
- La validación en implementación de un plan (con las operaciones de la empresa y los representantes de dichas operaciones)
- Realización de pruebas en cada unidad para ver la eficacia de la solución.
- La preparación y ejecución de pruebas integradas para verificar la eficacia de la solución.

La preparación y ejecución de pruebas casos/eventos, probar las respuestas en caso de situaciones de crisis, en base a un caso en el que los eventos ocurren al azar y se intensifican en forma gradual.

Capitulo IV: Prueba de Plan de Contingencia

4.1 Introducción

Todos los planes de contingencia deben ser probados para demostrar su habilidad de mantener la continuidad de los procesos críticos de la empresa. Las pruebas se efectúan simultáneamente a través de múltiples departamentos, incluyendo entidades comerciales externas.

Realizando pruebas se descubrirán elementos operacionales que requieren ajustes para asegurar el éxito en la ejecución del plan, de tal forma que dichos ajustes perfeccionen los planes preestablecidos.

4.2 Objetivos

- El objetivo principal, es determinar si los planes de contingencia individuales son capaces de proporcionar el nivel deseado de apoyo a la sección o a los procesos críticos de la empresa, probando la efectividad de los procedimientos expuestos en el plan de contingencias.

- Las pruebas permiten efectuar una valoración detallada de los costos de operación en el momento de ocurrencia de una contingencia.

4.3 Procedimientos Recomendados para las Pruebas del Plan de Contingencias, Niveles de Prueba

Se recomiendan tres niveles de prueba:

- Pruebas en pequeñas unidades funcionales o divisiones.
- Pruebas en unidades departamentales
- Pruebas interdepartamentales o con otras instituciones externas.

La premisa es comenzar la prueba en las unidades funcionales más pequeñas, extendiendo el alcance a las unidades departamentales más grandes, para finalmente realizar las pruebas entre unidades interdepartamentales o con otras instituciones externas.

4.4 Métodos para Realizar Pruebas de Planes de Contingencia

a) Prueba Específica

Consiste en probar una sola actividad, entrenando al personal en una función especifica, basándose en los procedimientos estándar definidos en el Plan de Contingencias. De esta manera el personal tendrá una tarea bien definida y desarrollará la habilidad para cumplirla.

b) Prueba de Escritorio

Implica el desarrollo de un plan de pruebas a través de un conjunto de preguntas típicas (ejercicios).

Características:

- La discusión se basa en un formato preestablecido.
- Esta dirigido al equipo de recuperación de contingencias.
- Permite probar las habilidades gerenciales del personal que tiene una mayor responsabilidad

Los ejercicios de escritorio, son ejecutados por el encargado de la prueba y el personal responsable de poner el plan de contingencias en ejecución, en una situación hipotética de contingencia. Un conjunto de preguntas se pedirán que resuelva el personal. El encargado y el personal utilizarán el plan de contingencias para resolver las respuestas a cada situación. El encargado contestará a las preguntas que se relacionan con la disponibilidad del personal entrenado, suficiencia de los recursos, suficiencia de máquinas, y si los requerimientos necesarios están a la mano. Los ajustes serán hechos al plan o al ambiente determinado durante esta fase si cualquier parte del plan no cumple con los objetivos propuestos.

c) Simulación en Tiempo Real

Las pruebas de simulación real, en un departamento, una división, o una unidad funcional de la empresa esta dirigido una situación de contingencia por un período de tiempo definido.

- Las pruebas se hacen en tiempo real
- Es usado para probar partes específicas del plan
- Permite probar las habilidades coordinativas y de trabajo en equipo de los grupos asignados para afrontar contingencias.

4.5 Preparaciones Pre Prueba

- Repasar los planes de contingencia seleccionados para probar.
- Verificar si se han asignado las respectivas responsabilidades.
- Verificar que el plan este aprobado por la alta dirección de la institución.
- Entrenar a todo el personal involucrado, incluyendo orientación completa de los objetivos del plan, roles, responsabilidades y la apreciación global del proceso.
- Establecer la fecha y la hora para la ejecución de la prueba.
- Desarrollar un documento que indique los objetivos, alcances y metas de la prueba y distribuirlo antes de su ejecución.
- Asegurar la disponibilidad del ambiente donde se hará la prueba y del personal esencial en los días de ejecución de dichas pruebas.

- No hacer «over test»—la meta es aprender y descubrir las vulnerabilidades, no generar fracaso y frustración.
- La prueba inicial se enfoca principalmente en entrenar al equipo que ejecutará con éxito el plan de contingencias, solucionando el problema y reestableciendo a la normalidad las actividades realizadas.
- Enfocar los procesos comerciales críticos que dependen de sistemas específicos o compañías externas donde se asume que hay problemas.
- Definir el ambiente donde se realizaran las reuniones del equipo de recuperación de contingencias.
- Distribuir una copia de la parte del Plan de Contingencias a ser ejecutado.

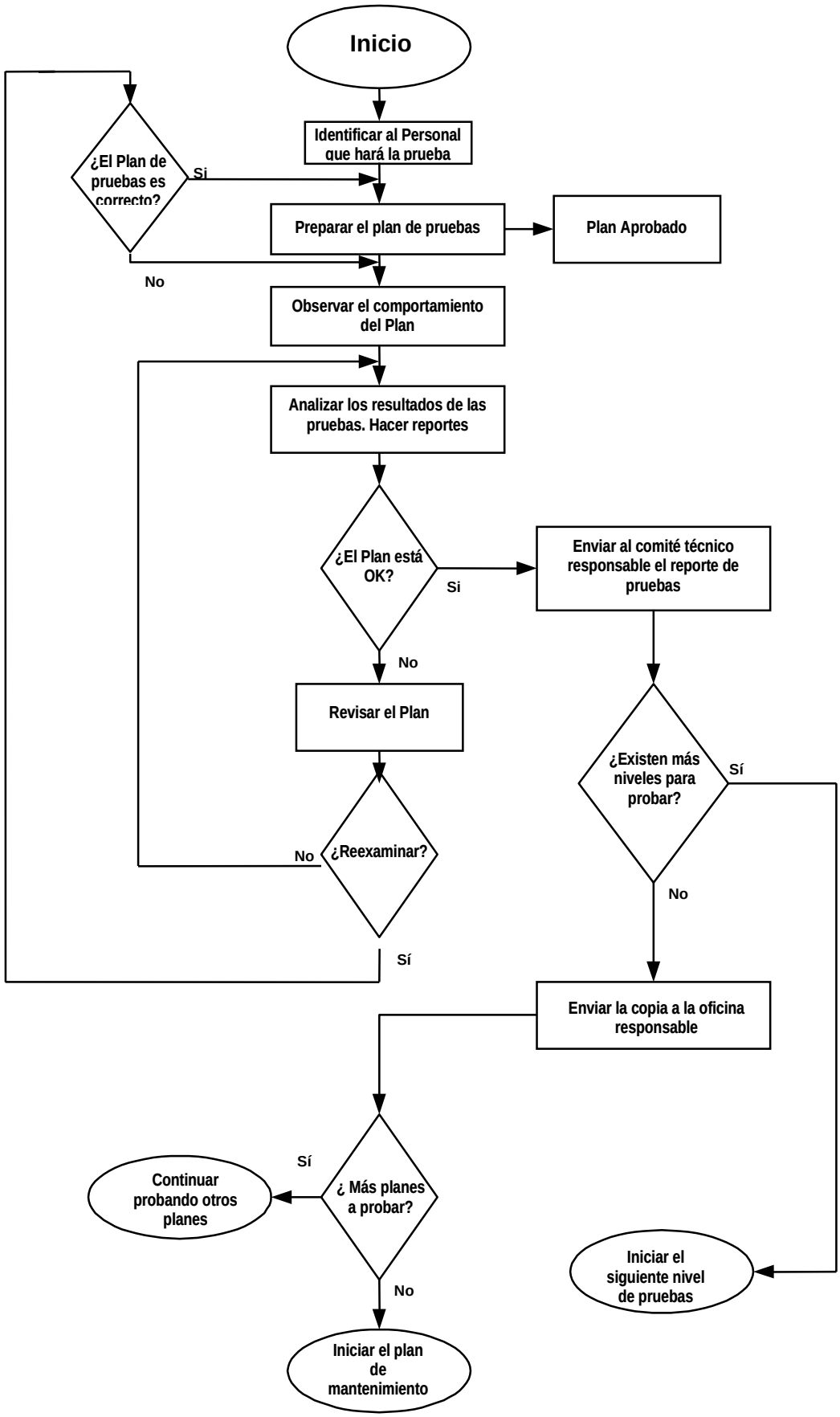
4.6 Comprobación de Plan de Contingencias

La prueba final debe ser una prueba integrada que involucre secciones múltiples e instituciones externas. La capacidad funcional del plan de contingencia radica en el hecho, de que tan cerca se encuentren los resultados de la prueba con las metas planteadas. El siguiente diagrama de bloques representa los pasos necesarios, para la ejecución de las pruebas del plan de contingencias. La figura adjunta muestra los pasos necesarios para hacer la comprobación del Plan de Contingencias.

4.7 Mantenimiento de Plan de Contingencias y Revisiones

Las limitaciones y problemas observados durante las pruebas deben analizarse planteando alternativas y soluciones, las cuales serán actualizadas en el Plan de Contingencias.

PROCESO DE PRUEBAS DEL PLAN DE CONTINGENCIAS



Este formato se propone para describir el escenario real donde se hará la prueba. Documentará el día de la semana y la hora (si es necesario) de ocurrencia del acontecimiento. La "Descripción del Evento/Mensaje" define los eventos del incidente presentados en el departamento, los cuales se deben solucionar. Las soluciones deben ser coincidentes con los planes de contingencia previamente aprobados. El 'ítem #' debe ser utilizado por los observadores y los evaluadores para realizar identificaciones, dar respuestas a los acontecimientos y a los mensajes específicos mientras estos ocurren.

Fecha / Tiempo	Significado del Día	Item #	Descripción del Evento/Mensaje
24/02/01 10.45 a.m.	Día Feriado	*101*	*Se perdieron los accesos a las bases de datos, los documentos se corrompieron; algunos discos duros se borraron totalmente.*
	Día Normal	*102*	*Problemas en las ventas Las facturas no pueden ser generadas.*
		Etc.	

4.8 Entorno de las Pruebas del Plan de Contingencias

La siguiente estructura de entorno se sugiere para la documentación del plan de pruebas:

1. Pruebas de objetivos y alcances.
2. Pruebas metodológicas.
3. Precisar equipos y recursos.
4. Demanda de personal capacitado.
5. Detallar itinerarios y localizaciones.
6. Control del Proceso.
8. Objetivos trazados a partir del control.
10. Control de la evaluación y observaciones.

1.-	*Pruebas de alcances y objetivos*	*El estado que se piensa lograr tras la realización de las pruebas.*
2.-	*Pruebas metodológicas*	*Proporciona una descripción del tipo de prueba que se realizará.*
3.-	*Precisar equipos y recursos*	*Identifica y establece lo necesario.*
4.-	*Demanda de personal capacitado*	*Enumera y describe el personal y las necesidades de capacitación.*
5.-	*Detallar itinerarios y localizaciones*	*Desarrolla las tareas, límites, y las responsabilidades que muestran el plan para la ejecución de la prueba.*
6.-	*Control del proceso*	*Describe la disposición; desarrollo del escenario de ensayo, y procedimientos*
7.-	*Control de la acción del tiempo*	*Detalla la secuencia de eventos para la prueba.*
8.-	*Objetivos trazados a partir del control*	*Define las medidas de éxito para la prueba.*
9.-	*Control de personal*	*Define los procedimientos para terminar, suspender, y reiniciar la prueba..*
10.-	*Pruebas de evaluación y observaciones*	*Detalla los resultados de la evaluación y de la observación, además planes de acción alternados para rectificar fallas.*

RESUMEN DE LA PRUEBA DEL REPORTE DE ESCRITORIO (DESKTOP/TABLETOP EXERCISE)

Obligación de Mitigar los Daños

Es importante recordar que si los sistemas de Información de una compañía fallan y esto da como resultado pérdidas o daños, entonces la compañía tiene una obligación de evitar la acumulación innecesaria de daños adoptando las medidas necesarias para mitigar dichos daños. De igual manera, si ocurren pérdidas a raíz de las acciones de terceros, es posible que la compañía no recupere los daños que a sabiendas permitió que aumentaran. En otras palabras, las compañías no deben confiar en el hecho de que inicialmente no fue su culpa y simplemente suponer que la parte culpable se responsabilizará de todas las pérdidas y daños resultantes. La compañía debe adoptar algún tipo de acción para minimizar el impacto sobre sus negocios, y los daños a la propiedad, resultantes de una falla del sistema de información.

En la práctica, un plan de contingencia puede y debe ser visto como una herramienta para cumplir con esta obligación legal: el plan resumirá los pasos que la compañía dará para mitigar sus daños en caso de que ocurra una falla. Por supuesto que la falta de un plan no eliminará la obligación de mitigar, y el hecho de que no haya un plan podría ser empleado en contra de la compañía en un litigio

subsecuente como evidencia de que no adoptó las medidas suficientes para minimizar el daño incurrido. Los peritos podrían atestiguar que el plan de contingencia para el sistema de información era necesario, y que la ausencia de un plan era irrazonable y que el acusado no debería sufrir las consecuencias.

Para complicar aún más las cosas, un plan de contingencia debería tomar en cuenta también cualquier otro sistema para la determinación de prioridades que pudiera haber sido utilizado por una compañía, u otros procesos utilizados para enfocar los sistemas que tienen una importancia crítica para la misión. El "sistema para determinar prioridades" se refiere a la práctica utilizada durante la guerra de separar a los soldados heridos en categorías, poniendo a un lado a los que probablemente sobrevivirían aún sin atención médica, aquellos que probablemente morirían sin importar lo que se hiciera por ellos, y aquellos para los cuales la atención médica era de importancia crítica; la atención médica se centraba en las personas que se encontraban en esta última categoría.

Suponga que la Compañía X, presionada por el tiempo, ha decidido arreglar ciertos sistemas considerados críticos para su misión, e ignorar otros. Probablemente la compañía X necesitará un plan de contingencia para resolver cualquier problema y que se salven los sistemas considerados críticos para su misión — si los sistemas son tan críticos se necesitan todas las precauciones debidas— ¿pero que ocurre con los sistemas que han sido ignorados? Los sistemas ignorados podrían ocasionar daños y en efecto podrían convertirse en el foco — y tal vez el único foco —de cualquier proceso legal subsecuente. ¿La Compañía X tiene una explicación suficientemente adecuada para ser presentada ante un jurado, para respaldar su decisión de escoger los sistemas que consideraba críticos para su misión?

Por el contrario, para aquellos sistemas que no se consideraban críticos para su misión, ¿la compañía implementó por lo menos un plan para minimizar el impacto de cualquier falla en dichos sistemas? De no ser así, la Compañía X se encontrará en una situación poco envidiable de tratar de explicar potencialmente ante una corte por qué no debería ser responsable por la falla de un sistema de computación que explícitamente decidió no reparar y que sabía que probablemente no funcionaría ante un problema, y simultáneamente no adoptó ninguna acción (a través de un plan de contingencia) para minimizar el impacto de las fallas de los sistemas sobre terceros. Sabíamos que era probable que ocurran problemas, pero no hicimos nada.

Dos lecciones claves surgen. Primero, es importante evaluar los impactos económicos de los sistemas de computación, y utilizar el plan de contingencia como un vehículo para mitigar las pérdidas económicas tanto para el negocio como por razones legales. Segundo, el plan de contingencia debería enfocar no solamente los sistemas considerados críticos para la misión. Debería enfocar todos los sistemas, y hasta cierto grado el plan de contingencia puede ser aún más importante desde el punto de vista legal para las aplicaciones no críticas que se espera que fallen.

Meta : Documentación de un Plan

Por supuesto que un plan de contingencia tiene un valor limitado desde el punto de vista comercial o legal, si no fue redactado por escrito y si no se mantiene adecuadamente en lugares de fácil acceso para el personal clave. Generalmente, para propósitos legales — para evitar y defender cualquier alegato de negligencia o falta de cuidado debido — es de importancia crítica que los planes de contingencia sean revisados apropiadamente para que se adecuen al sistema de información, con los jefes de equipo y los funcionarios y/o los miembros de las juntas directivas y además que dichas acciones sean tomadas con una anticipación suficiente ante cualquier problema, con el fin de permitir el tiempo suficiente para los comentarios, reacciones e implementación de las mismas, ya que un plan de contingencia requiere de negociación y seguimiento. Además, si se decide que no se necesita ningún plan de contingencia, esa decisión debería estar adecuadamente documentada y explicada a la luz de la atención que se está dando actualmente a los planes de contingencia. En última instancia, la compañía querrá evitar cualquier responsabilidad individual de sus directores y funcionarios bajo el reglamento del "juicio de la empresa", aseverando que todas sus decisiones en cuanto a la forma de manejar las contingencias del Sistema de Información fueron debidamente consideradas, y/o que se basó en las opiniones de los expertos en los que la compañía razonablemente confió para formular un plan de contingencia.

Después de la documentación del Plan de Contingencia y su aprobación por el comité técnico a cargo de dicho plan, las copias se distribuyen a todas las áreas de la organización.

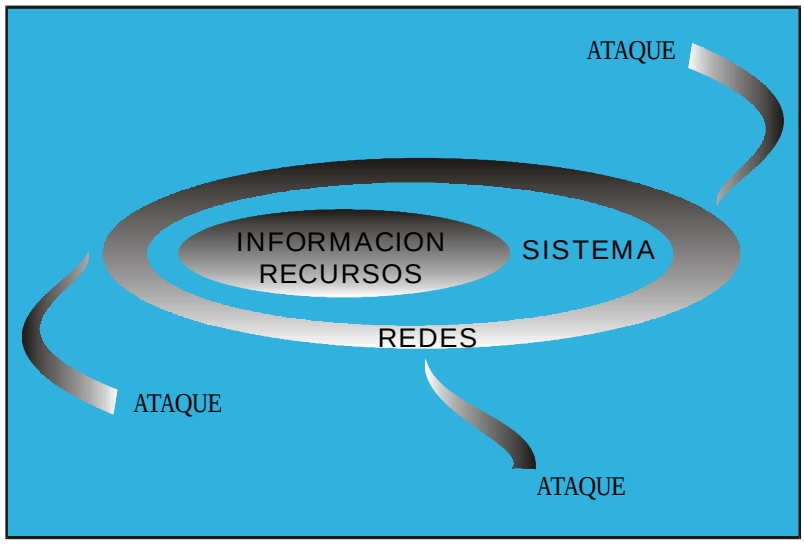
Anexos

CRITERIOS SOBRE SISTEMAS DE INFORMACION EN INTERNET

La seguridad es uno de los aspectos más conflictivos del uso de las tecnologías de la información. Es suficiente comprobar cómo la falta de una política de seguridad global está frenando el desarrollo de Internet en áreas tan interesantes y prometedoras, como el comercio electrónico o la interacción con las administraciones públicas.

Los recientes avances en las telecomunicaciones y en la computación en red han proporcionado la aparición de canales rápidos para la propagación de datos a través de sistemas digitales. Las redes abiertas están siendo utilizadas cada vez más como una plataforma para la comunicación en nuestra sociedad, pues permiten rápidos y eficientes intercambios de información con un bajo coste económico asociado y con una fácil accesibilidad.

El desarrollo actual y las perspectivas de futuro de las "superautopistas de datos" y de una infraestructura global de información, es decir, de Internet y de la World Wide Web (WWW), crean toda una variedad de nuevas posibilidades. Sin embargo, la realización efectiva de tales posibilidades están influidas por las inseguridades típicas de las redes abiertas: los mensajes pueden ser interceptados y manipulados, la validez de los documentos se puede negar, o los datos personales pueden ser recolectados de forma ilícita. Como resultado, el atractivo y ventajas ofrecidas por la comunicación electrónica, tanto en el desarrollo de oportunidades comerciales entre organizaciones privadas como en las interrelaciones entre las organizaciones públicas y los ciudadanos, no pueden ser explotadas en su totalidad.



Es por esto tener en cuenta dentro de nuestro plan de contingencia la operatividad de un firewall para impedir el acceso a usuarios del exterior que no tengan autorización, ya que esto podría ser perjudicial para el servicio de nuestros servidores de red.

CONCLUSION

- Dependiendo del tamaño de la institución u organización se tendrá que realizar paralelamente un plan de contingencia por cada módulo del sistema de Información.

- Adicionalmente al plan de contingencias se debe desarrollar pruebas para verificar la efectividad de las acciones en caso de la ocurrencia de los problemas y tener la seguridad de que se cuenta con un método seguro.

- No existe un plan único para todas las organizaciones, esto depende mucho de la capacidad de la infraestructura física como de las funciones que realiza en CPD (Centro de Procesamiento de Datos) mas conocido como Centro de Cómputo.

BIBLIOGRAFIA

- Y2K *A CONTINGENCY PLANNING GUIDE*
  META Group Inc.

- YEAR 2000 COMPUTING CRISIS: BUSINESS CONTINUITY AND CONTINGENCY PLANNING
  United States General Accounting Office

- CONTINGENCY PLANS FOR THE YEAR 2000 COMPUTER PROBLEM
  Seminar on the year 2000 Computer
  Masahito Nakamura