**CONTINGENCIAS: PREVENCION Y RECUPERACION**

**Concepto de Contingencia:**

* Posibilidad o riesgo de que suceda una cosa
* Hecho o problema que se plantea de forma imprevista
* El término suele referirse a **algo que es probable que ocurra**, aunque no se tiene una certeza al respecto. La contingencia, por lo tanto, es **lo posible** o aquello que puede, o no, concretarse.

Cuando una persona se enfrenta a una contingencia, tiene que modificar su comportamiento previsto o desarrollar una acción específica, motivada por la irrupción de la contingencia en cuestión.

**Plan de Contingencias**

Definicion:

Para determinar el origen etimológico de los dos principales vocablos que dan forma al término que nos ocupa tenemos que ir hasta el latín. Así, en dicha lengua nos encontramos con el hecho de que plan procede de la palabra *planus*que puede traducirse como “plano”.

Mientras, contingencia emana del concepto contingentiaque es fruto de la unión de tres partes: el prefijo con- que es equivalente a “reunión”, el verbo tangereque es sinónimo de “tocar” y finalmente el sufijo –enciaque puede determinarse que su significado es igual a “cualidad”.

Un plan de contingencia es un tipo de  plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas.

El plan de contingencia propone una serie de procedimientos alternativos al funcionamiento normal de una [organización](http://definicion.de/organizacion), cuando alguna de sus funciones usuales se ve perjudicada por una contingencia interna o externa.

Esta clase de plan, por lo tanto, intenta garantizar la continuidad del funcionamiento de la organización frente a cualquier eventualidad, ya sean materiales o personales. Un plan de contingencia incluye cuatro etapas básicas: la evaluación, la planificación, las pruebas de viabilidad y la ejecución.

Los especialistas recomiendan planificar cuando aún no es necesario; es decir, antes de que sucedan los [accidentes](http://definicion.de/accidente/). Por otra parte, un plan de contingencia debe ser dinámico y tiene que permitir la inclusión de alternativas frente a nuevas incidencias que se pudieran producir con el tiempo. Por eso, debe ser actualizado y revisado de forma periódica.

Un plan de contingencia también tiene que establecer ciertos objetivos estratégicos y un [plan de acción](http://definicion.de/plan-de-accion) para cumplir con dichas metas.

En concreto podemos establecer que todo plan de contingencia tiene que estar conformado a su vez por otros tres planes que serán los que establezcan las medidas a realizar, las amenazas a las que se hace frente y el tiempo de establecimiento de aquellas.

En primer lugar, está el plan de respaldo que es aquel que se encarga de determinar lo que son las medidas de prevención, es decir, las que se tienen que llevar a cabo con el claro objetivo de evitar que pueda tener lugar la materialización de una amenaza en concreto.

En segundo lugar, también integra al proyecto de contingencia lo que es el plan de emergencia que, como su propio nombre indica, está conformado por el conjunto de acciones que hay que llevar a efecto durante la materialización de la amenaza y también después de la misma. Y es que gracias a aquellas se conseguirá reducir y acabar con los efectos negativos de aquella.

Y en tercer lugar está el plan de recuperación que se realiza después de la amenaza con el claro objetivo de recuperar el estado en el que se encontraban las cosas antes de que aquella se hiciera real.

**Plan de Contingencia informático**

En la [informática](http://definicion.de/informatica), un plan de contingencia es un programa alternativo para que una empresa pueda recuperarse de un desastre informático y restablecer sus operaciones con rapidez. Estos planes también se conocen por la sigla DRP, del inglés Disaster Recovery Plan.

Un programa DRP incluye un plan de respaldo (que se realiza antes de la amenaza), un plan de emergencia (que se aplica durante la amenaza) y un plan de recuperación (con las medidas para aplicar una vez que la amenaza ha sido controlada).

Objetivo General:

*Garantizar la continuidad de las actividades, ante eventos que podrían alterar el normal funcionamiento de las Tecnologías de la Información y Comunicaciones, a fin de minimizar el riesgo no previsible, críticos o de emergencia, y responder en forma inmediata hacia la recuperación de las actividades normales*.

El Plan está orientado a establecer, junto con otros trabajos de [seguridad](http://www.monografias.com/trabajos/seguinfo/seguinfo.shtml), un adecuado [sistema](http://www.monografias.com/trabajos11/teosis/teosis.shtml) de seguridad [física](http://www.monografias.com/Fisica/index.shtml) y [lógica](http://www.monografias.com/trabajos15/logica-metodologia/logica-metodologia.shtml) en previsión de desastres.

Se define la Seguridad de Datos como un conjunto de medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por [el hombre](http://www.monografias.com/trabajos15/fundamento-ontologico/fundamento-ontologico.shtml). Se ha considerado que para una compañía, la seguridad es un elemento básico para garantizar su supervivencia y entregar el mejor [Servicio](http://www.monografias.com/trabajos14/verific-servicios/verific-servicios.shtml) a sus [Clientes](http://www.monografias.com/trabajos11/sercli/sercli.shtml), y por lo tanto, considera a la Información como uno de los [activos](http://www.monografias.com/trabajos11/contabm/contabm.shtml) más importantes de [la Organización](http://www.monografias.com/trabajos6/napro/napro.shtml), lo cual hace que la protección de esta sea el fundamento más importante de este Plan de Contingencia.

**Fases de la Metodología Para el Desarrollo de un Plan de Contingencia**.

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 (Instituto de Estadísticas e informaticas – Peru).

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:

• **Equipamiento**: computadoras, impresoras, scaners, 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, Documentos, Planillas, Almacén, Ventas, Presupuesto, Personal.

• **Equipos Fijos o 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 preevento, 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.

**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 lasestaciones 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.

**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 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 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.

**4.3.2.2 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.

**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 de Plan de Acción**

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

**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 un 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) quefueron 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 yreforzando 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 siguientes 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.

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 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:

1. Se contará con antivirus para el sistema que aíslan el virus que ingresa al sistema llevándolo a un directorio para su futura investigación
2. El antivirus muestra el nombre del archivo infectado y quién lo usó.
3. Estos archivos (exe, com, ovl, nlm, etc.) serán reemplazados del diskett original de instalación o del backup.
4. 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.

**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 continúa de las aplicaciones.
* Revisión continúa del sistema de backup
* Revisión de los Sistemas de soporte eléctrico del Centro de Procesamiento de Datos.