GUIA PARA LA ELABORACION DE PLANES DE RECUPERACION PARA SISTEMAS DE INFORMACION EMPRESARIAL Y DE NEGOCIOS

Jonathan David Nima Ramos

PIURA - PERÚ

2009

INDICE

DEDICATORIA

A Jehová Dios, el sublime legislador y a mis padres que con esfuerzo y dedicación han logrado inculcar en mi corazón principios de moral elevados que llevo consigo para toda la vida.

El autor

PARTE I. INTRODUCCIÓN

El presente trabajo analiza una metodología práctica para el desarrollo de planes de contingencia de los sistemas de información que comprende: la identificación de riesgos, calificación del impacto del mismo si se hiciera realidad, evaluación del impacto en los procesos críticos y la creación de estrategias de contingencias.

Se trata de identificar los riesgos, cuantificar su probabilidad e impacto, y analizar medidas que lo eliminen lo que generalmente no es posible o que disminuyan la probabilidad de que ocurran los hechos o mitiguen el impacto.

Para evaluar riesgos hay que considerar, entre otros factores, el tipo de información almacenada, procesada y trasmitida, la criticidad de las aplicaciones, la tecnología usada, el marco legal aplicable, el sector de la entidad, la entidad misma y el momento.

El análisis de riesgos es una parte muy importante del proceso de seguridad informática. No se puede proteger algo si no se sabe contra qué hay que protegerlo.

Considero que no sólo es responsabilidad del Área de **Informática** sino de todas las Unidades Orgánicas proteger la información y los equipos que la contienen.

Por ello se pone a disposición el presente trabajo, esperando una vez más contribuir en el desarrollo de la Sociedad de la Información.

El Autor

PARTE II: NORMAS Y ORGANIZACIÓN DE LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

OBJETIVOS

Establecer las Políticas y Normas de Seguridad Informática y definir los responsables de su desarrollo, implantación y gestión.

Analizar los riesgos existentes sobre los Sistemas de Información y establecer las acciones necesarias para su reducción o eliminación.

Establecer la función de Seguridad Informática para gestionar la protección de los Recursos Informáticos y los Activos de Información de la institución.

ANÁLISIS DE RIESGOS

La Seguridad Informática tiene como objetivo el mantenimiento de la Confidencialidad, Integridad y Disponibilidad de los Sistemas de Información.

Es necesario identificar y controlar cualquier evento que pueda afectar negativamente a cualquiera de estos tres aspectos, así como definir e implantar las defensas necesarias para eliminar o reducir sus posibles consecuencias.

Para ello, deben utilizarse métodos formales de análisis de riesgos que lo garanticen.

Componentes

En un proceso de Análisis de riesgos se pueden establecer los siguientes componentes:

• **Sistema de Información.** Son los Recursos Informáticos y Activos de Información de que dispone la institución para su correcto

funcionamiento y la consecución de los objetivos propuestos por la Dirección.

• **Amenaza.** Cualquier evento que, pueda provocar daños en los Sistemas de Información, produciendo a la institución pérdidas materiales o financieras.

• **Vulnerabilidad.** Cualquier debilidad en los Sistemas de Información que pueda permitir a las amenazas para causarles daño y producir pérdidas a la institución.

• **Impacto.** Es la medición (y valoración) del daño que podría producir a la institución la materialización de una amenaza sobre los Sistemas de Información. La valoración global se obtendrá sumando el costo de reposición de los daños tangibles y la estimación, que siempre será subjetiva, de los daños intangibles.

• **Riesgo.** Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del Sistema de Información, causando un impacto en la institución.

• **Defensa.** Cualquier medio, físico o lógico, empleado para eliminar o reducir un **riesgo**. Debe realizarse una valoración cuantitativa de su costo.

La Realización de Análisis

En el proceso de Análisis de riesgos se pueden diferenciar:

1. La Evaluación de Riesgos, orientada a determinar los Sistemas de Información que, en su conjunto o en cualquiera de sus partes, puedan verse afectados directa o indirectamente por amenazas, valorándose todos los riesgos y estableciendo sus distintos niveles a partir de las posibles amenazas, las vulnerabilidades existentes y el impacto que puedan causar a la institución.

- Se trata de identificar los riesgos, cuantificar su probabilidad e impacto, y analizar medidas que lo eliminen lo que generalmente no es posible o que disminuyan la probabilidad de que ocurran los hechos o mitiguen el impacto.

- Para evaluar riesgos hay que considerar, entre otros factores, el tipo de información almacenada, procesada y trasmitida, la criticidad de las aplicaciones, la tecnología usada, el marco legal aplicable, el sector de la entidad, la entidad misma y el momento.

2. La Gestión de Riesgos, que implica la identificación, selección, aprobación y manejo de las defensas (contra medidas) para eliminar, o reducir a niveles aceptables, los riesgos evaluados, con actuaciones tendentes a:

- Reducir la posibilidad de que una amenaza ocurra;
- Limitar el impacto de una amenaza, si ésta se manifiesta;
- Reducir o eliminar una vulnerabilidad existente;
- Permitir la recuperación del impacto o su transferencia a terceros (contratación de seguros).

Un primer análisis de riesgos será mucho más costoso que los sucesivos.

Puede requerir mucho tiempo y la participación de personal cualificado y especializado. El tiempo empleado estará en proporción a los objetivos fijados y a su ámbito de cobertura.

Para resaltar la necesidad de sucesivos análisis de riesgos se deben tener en cuenta las siguientes consideraciones:

• Los elementos que componen los Sistemas de Información de una institución están sometidos a constantes variaciones: nuevo personal informático, nuevas instalaciones, nuevos productos, nuevas aplicaciones, etc.

• Pueden aparecer nuevas amenazas o variar la probabilidad de que ocurra alguna de las existentes, afectando al posible impacto.

• Pueden aparecer nuevas vulnerabilidades o variar (o desaparecer) alguna de las existentes, creando o eliminando posibles amenazas.

En consecuencia, es necesario actualizar periódicamente el análisis de riesgos tomando como base de partida el último realizado y las

defensas implantadas hasta la fecha, por lo que los factores tiempo y medios necesarios para su realización serán menores.

El análisis de riesgos, además de centrarse en los Sistemas de Información existentes, es recomendable aplicarlo en el desarrollo de nuevos Sistemas, asegurándolos desde su creación.

POLÍTICAS DE SEGURIDAD

La Dirección de la institución es responsable de definir y publicar las Políticas de Seguridad como una firme declaración de intenciones, así como de divulgarlas en todo el ámbito de la institución.

El conjunto de las Políticas de Seguridad debe establecer los criterios de protección en el ámbito de la institución y servir de guía para la creación de las Normas de Seguridad.

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

Criterios de Seguridad

- La falta de accesibilidad produce una denegación del servicio, que es uno de los ataques más frecuentes en Internet.

- Cualquier entidad que envía o recibe datos no puede alegar o desconocer el hecho.
- Los dos criterios anteriores son especialmente importantes en el entorno bancario y de comercio electrónico.
- Los usuarios deben saber que sus actividades quedan registradas.

Normas de Seguridad Informática

Basándose en las Políticas de Seguridad, la Dirección de la institución publicará las Normas de Seguridad, en las que se definirá qué hay que proteger y el objeto concreto de esa protección. Una Norma debe ser breve, concisa y redactada en términos claros y comprensibles por todos los empleados, y debe contener como información de control, al menos:

- Fecha de publicación;
- Fecha de efectividad o entrada en vigor;
- Fecha prevista de revisión o renovación;
- Si es aplicable a toda la institución o a un ámbito más reducido;
- Si sustituye a una norma precedente o es nueva.

• Las Normas son de obligado cumplimiento, por lo que deben ser divulgadas, de acuerdo con su ámbito de aplicación, a todos los empleados involucrados, incluido el personal directivo.

La responsabilidad del cumplimiento de las Normas es de todos los empleados, pero especialmente del personal directivo que acumula a su responsabilidad como empleado, la de todos los empleados a los que dirige, coordina o supervisa.

El conjunto de todas las Normas de Seguridad debe cubrir la protección de todos los entornos de los Sistemas de Información de la institución.

Procedimientos de Seguridad Informática

Basándose en las Normas de Seguridad, y dependiendo del ámbito de aplicación, el departamento responsable creará los Procedimientos de Seguridad, en los que se describirá cómo proteger lo definido en las Normas y las personas o grupos responsables de la implantación, mantenimiento y el seguimiento de su nivel de cumplimiento. Un Procedimiento debe cubrir todo los aspectos descritos en la Norma que le soporta, siguiendo de forma detallada y concreta todos los pasos en los que se estructura.

En un Procedimiento se deben declarar todas las actividades que lo componen y definir todos los controles necesarios (y sus indicadores de seguimiento) para cumplir con los requerimientos definidos en la Norma correspondiente. Adicionalmente, debe contener como información de control, al menos: fecha de publicación; fecha de

efectividad ; entrada en vigor; fecha prevista de revisión; renovación; responsable de su revisión y publicación; relación de actividades; responsables de cada actividad; relación de controles por actividad; valores críticos de los indicadores; si sustituye a un procedimiento anterior o es nuevo.

La Calidad en la Seguridad

Teniendo en cuenta criterios de Calidad, los procedimientos, y las actividades que lo componen, pueden estructurarse de tal manera que se podría definir un Proceso por cada procedimiento.

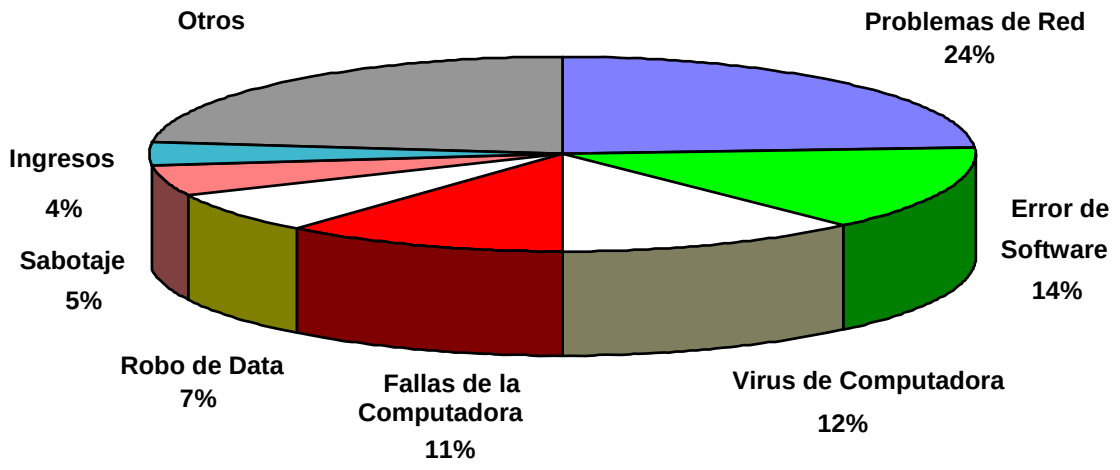
En una segunda fase, las actividades que componen cada procedimiento (ahora proceso) deberían analizarse para evaluar si son, o no automatizables. Posteriormente, se procedería a la automatización de las actividades que se hubieran declarado viables y a un segundo análisis y evaluación de las restantes actividades. De esta forma, paso a paso, se podría llegar a unos niveles de automatización que minimizarían la intervención humana, excepto en alguna toma de decisiones, obteniendo como valor añadido la fiabilidad de estos procesos.

Siguiendo con los criterios de Calidad, los procesos deben ser revisados periódicamente, como Mejora Continua, para la eliminación de defectos y la reducción del ciclo. Finalmente, resumir los objetivos de la aplicación de la Calidad en el área de Seguridad:

• Incrementar la fiabilidad de los controles y sus indicadores, proporcionando alertas automáticas;

• Disminuir la intervención humana, con una reducción adicional del costo de personal; reducir el ciclo de los procesos, permitiendo obtener información más actualizada.

Problemas de Seguridad Relacionados con la Pérdida Financiera



ORGANIZACIÓN EN LA INSTITUCIÓN

La Dirección debe ser consciente de las facilidades que existen para acceder a los Recursos Informáticos y Activos de Información e incluso manipularlos, sin motivos basados en las actividades de la institución, es decir: sin autorización.

Consideraciones Organizativas

Generalmente, la institución tiene una organización jerárquica en forma piramidal, cuyo vértice está ocupado por la más alta dirección. Entre el vértice y la base suele haber varios niveles intermedios, que variarán en número dependiendo del tamaño de la institución.

Un departamento, o grupo de departamentos homogéneos, forma lo que llamaremos una Función (Ejem.: Personal, Finanzas, Administración, etc.) con un director funcional al frente de cada una.

Entre ellas, destacamos la función de Sistemas de Información, entendiendo bajo este nombre a los departamentos encargados de gestionar los Recursos Informáticos y los Activos de Información de las restantes funciones de la institución.

En la medida que cada Función y las actividades de la institución dependa de la información, la necesidad de protección será más perentoria y cada vez tendrá que ser más sofisticada. Para gestionar esta protección, es necesario contar con una Infraestructura de Seguridad Informática con la formación, dedicación y herramientas especializadas adecuadas.

Factores Críticos de Éxito

Para tener unas mínimas garantías de éxito, en la implantación de la Seguridad Informática en la institución, la experiencia ha demostrado que son críticos, al menos, los factores siguientes:

• El compromiso y apoyo visible de la alta Dirección.

• Los objetivos y actividades de Seguridad que deben estar basados en las necesidades de la institución y liderados por la organización responsable de la Seguridad Informática.

• El análisis de riesgos potenciales (y su valoración) para evitarlos o minimizarlos.

• La implantación de controles para la detección de riesgos potenciales y su divulgación en todo el ámbito de la institución.

• La rapidez en la actuación para proteger los Sistemas de Información, con lo que los riesgos serán menores y se reducirá sustancialmente el costo de la Seguridad Informática, a medio y largo plazo.

INFRAESTRUCTURA DE SEGURIDAD INFORMÁTICA

No existe un único modelo predefinido, variará en función del tamaño de la institución, del volumen y tipo de Recursos y Activos a proteger y del nivel tecnológico alcanzado. Normalmente, podrán utilizarse los recursos humanos existentes en la institución.

Hay que tener en cuenta que, dependiendo del tamaño de la institución, algunos puestos no siempre serán cubiertos y que varios puestos pueden ser desempeñados por la misma persona, siempre que no entren en

conflicto con el principio de segregación de responsabilidades. Una organización tipo podría ser de la forma siguiente:

En la Dirección de la Institución

• Comité de Dirección: Formado por los Directores Funcionales y con la responsabilidad del nombramiento de Propietarios, a propuesta del Director Funcional correspondiente.

• Ejecutivo de Seguridad Informática. Habitualmente, el Director de la Función de Sistemas de Información, dependiendo del más alto nivel de Dirección de la institución.

• Comité de Seguridad Informática. Formado por todos los Coordinadores Funcionales y el Director responsable de Seguridad Informática.

En la Función de Sistemas de Información

• El Director de Sistemas de Información, del que depende o el Director de Seguridad Informática; del que, a su vez, dependerán

• El Coordinador de Seguridad Informática;

• El Administrador Central de Seguridad Informática;

• El Administrador de Usuarios y Accesos;

• Los Administradores Locales de Seguridad Informática.

En las Restantes Funciones de la Institución o Coordinador

• Funcional de Seguridad Informática. Dependiendo directamente del Director de la Función correspondiente.

• Especialistas Informáticos, que asesorarán a sus Coordinadores.

Soporte de Especialistas en Seguridad Informática

Cada institución, independientemente de su tamaño, debe poder contar con la utilización de especialistas en Seguridad de Informática. Siempre que sea posible, este soporte debe ser dado por un asesor interno, aunque es habitual la contratación de asesores ajenos a la institución.

Los especialistas deben poder asesorar sobre todos, y cada uno de, los aspectos de la Seguridad Informática. Tienen que valorar el nivel de implantación de las Políticas y Normas de Seguridad

Informática y el nivel de cumplimiento de los procedimientos establecidos. Tienen que poder analizar los riesgos: definiendo las posibles amenazas, detectando las vulnerabilidades existentes y determinando las medidas a tomar para su eliminación o reducción.

Los especialistas de Seguridad Informática deben ser consultados lo mas rápidamente posible cuando se sospechen incidentes o debilidades de Seguridad, para que establezcan planes de actuación y métodos de aislamiento e investigación del problema.

El mantenimiento y mejora de los niveles de Seguridad adquiridos, es una de las más importantes actividades a realizar en la institución. Para ello es preciso establecer diagnósticos periódicos, a realizar por especialistas internos, consultores externos independientes o empresas especializadas en consultorías o asesorías de Seguridad.

ACTORES Y SUS RESPONSABILIDADES

Recomendación

Para conseguir una Seguridad efectiva y completa de los Recursos Informáticos y Activos de Información, es imprescindible delimitar las funciones y definir las responsabilidades de quienes lo utilizan.

Los Recursos Informáticos y Activos de Información son propiedad de la institución, pero es necesario delegar en los actores que desempeñan las distintas funciones en la protección y asignar a cada uno de ellos sus responsabilidades.

Este proceso es de extrema importancia, ya que de él dependerán todas las Políticas y Normas de Seguridad desarrolladas por la institución.

Propietario

Todos, y cada uno, de los Recursos Informáticos y Activos de Información tienen que tener asignado un Propietario que actuará

siempre por delegación de la Dirección de la institución y será responsable de su protección.

En términos de Seguridad, el Propietario es el único que organizativamente tiene la responsabilidad de mantener operativos sus Recursos Informáticos y Activos de Información, determinar su criticidad y clasificación, establecerlos requerimientos de protección y conceder o eliminar derechos de acceso a los usuarios. Son responsabilidades del Propietario:

• Identificar Recursos Informáticos y Activos de Información de su propiedad; o no autorizar, salvo excepciones, el acceso público a sus Activos de Información;

• Determinar los requerimientos de protección durante todas las etapas del ciclo de vida de los Activos de Información: creación, clasificación, calificación, manipulado, proceso automático, edición, reproducción, distribución, transporte, almacenaje, desclasificación y destrucción;

• Asignar y mantener la clasificación a los Activos de Información; o autorizar y mantener la vigencia de los accesos y el nivel de acceso de los usuarios, caso a caso, y siempre por razones de negocio;

• Impulsar las sanciones para los accesos no autorizados, de acuerdo con su naturaleza y con los daños ocasionados; o analizar y definir Activos de Información Sensibles; o analizar y definir Aplicaciones y Activos Críticos para el negocio; participar activamente en la creación del Plan de Recuperación y en sus pruebas periódicas;

• Analizar los resultados de las pruebas del Plan de Recuperación y, si fuera necesario, crear un Plan de Acción y revisar periódicamente su cumplimiento; especificar al Depositario los controles a establecer y las incidencias a comunicar; comprobar el cumplimiento de los controles requeridos al Depositario.

Depositario

El Depositario de los Recursos Informáticos y Activos de Información, generalmente la función de Sistemas de Información, es responsable de

establecer y mantener los controles adecuados al nivel de protección requerido por el Propietario. Son responsabilidades del Depositario:

• No permitir el acceso público a los Activos de Información, salvo excepciones autorizadas;

• Proteger los Activos de Información según la clasificación asignada;

• Establecer y mantener los controles requeridos por el Propietario;

• Controlar los accesos de Usuarios autorizados por el Propietario; o comunicar al Propietario los nuevos controles técnicos que estén disponibles y cualquier desviación o anomalía detectada en los existentes;

• Informar a los Usuarios de los controles establecidos;

• Establecer los controles necesarios para impedir la instalación de productos sin licencia no autorizados por el fabricante;

• Realizar y coordinar el Plan de Recuperación y sus pruebas periódicas;

• Identificar Sistemas de Información Esenciales para los procesos de negocio.

Usuario

Es responsable de conocer el nivel de protección designado por el Propietario y cumplir con los controles establecidos por el Depositario, para todos los Recursos Informáticos y Activos de Información que maneje. Son responsabilidades del Usuario:

• Obtener la autorización formal del Propietario, antes de intentar acceder a cualquier Activo de Información;

• Informar al Propietario, cuando termine la necesidad de acceder a cualquier Activo de Información;

• Conocer la clasificación de los Activos de Información que maneja;

• No divulgar información clasificada sin autorización del Propietario;

• No intentar transgredir ningún control de protección establecido;

• Utilizar los Sistemas sólo para actividades importantes de la institución; o seguir las reglas establecidas para las contraseñas (passwords).

• Informar a Propietario y Depositario de cualquier anomalía de Seguridad detectada; no introducir personalmente ni utilizar ningún producto sin la correspondiente licencia autorización del fabricante.

PLANEACIÓN DE LA TECNOLOGÍA DE INFORMACIÓN

Un aspecto muy importante es el de la planificación de las tecnologías de la información, muchas organizaciones se han resistido a invertir en tecnologías de seguridad de la información no planificando el desarrollo de estos recursos, y en otros casos existe el paradigma referido a la seguridad informática, en el sentido de que la información se encontrará vulnerable por la presencia creciente de intrusos cibernéticos, si hacemos publica la información.

Ante esta situación cabe indicar que, a pesar de la creciente disponibilidad pública de la información y el aumento del número de intrusos potenciales actualmente, también existen las herramientas de seguridad así como la capacitación en dichos temas, con la finalidad de construir defensas efectivas y mejorarlas continuamente.

Con una planificación integral, anticipada, efectiva, es posible responder rápida y apropiadamente cualquier tipo de riesgo que atente en contra de los sistemas de información, sean éstos por intentos de accesos no deseados, eventos inesperados, o cualquier otra acción que atente contra la integridad o disponibilidad de la información. Algunas veces se logra prevenir la mayoría de ellos minimizando el efecto nocivo de los ataques.

Las arquitecturas de hardware y software, deben mantenerse simples. Esto ofrece una ventaja importante en materia de seguridad. En el caso de los sistemas múltiples no importa cuán estrechamente estén integrados, estos ofrecen varios puntos de acceso y requieren mayor administración de seguridad sistemas de apoyo que se traducen en el incremento de costos.
Es ahí donde se debe desarrollar un Plan de Contingencia adecuado a fin de salvaguardar la información que tan valiosa es para nosotros.

Ahora bien ante todo lo expuesto anteriormente, *¿Cómo podemos elaborar un Plan de Contingencia adecuado que nos permita estar preparado ante una eventualidad y asegurar la continuidad de las operaciones*?

Empezare dando el concepto de Plan de Contingencia para luego mencionar los pasos para su elaboración.

PARTE III. PLAN DE CONTINGENCIA

DEFINICION

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.

Consideramos que no sólo es responsabilidad del Área de **Informática** sino de todas las Unidades Orgánicas proteger la información y los equipos que la contienen.

OBJETIVOS

- 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.

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.

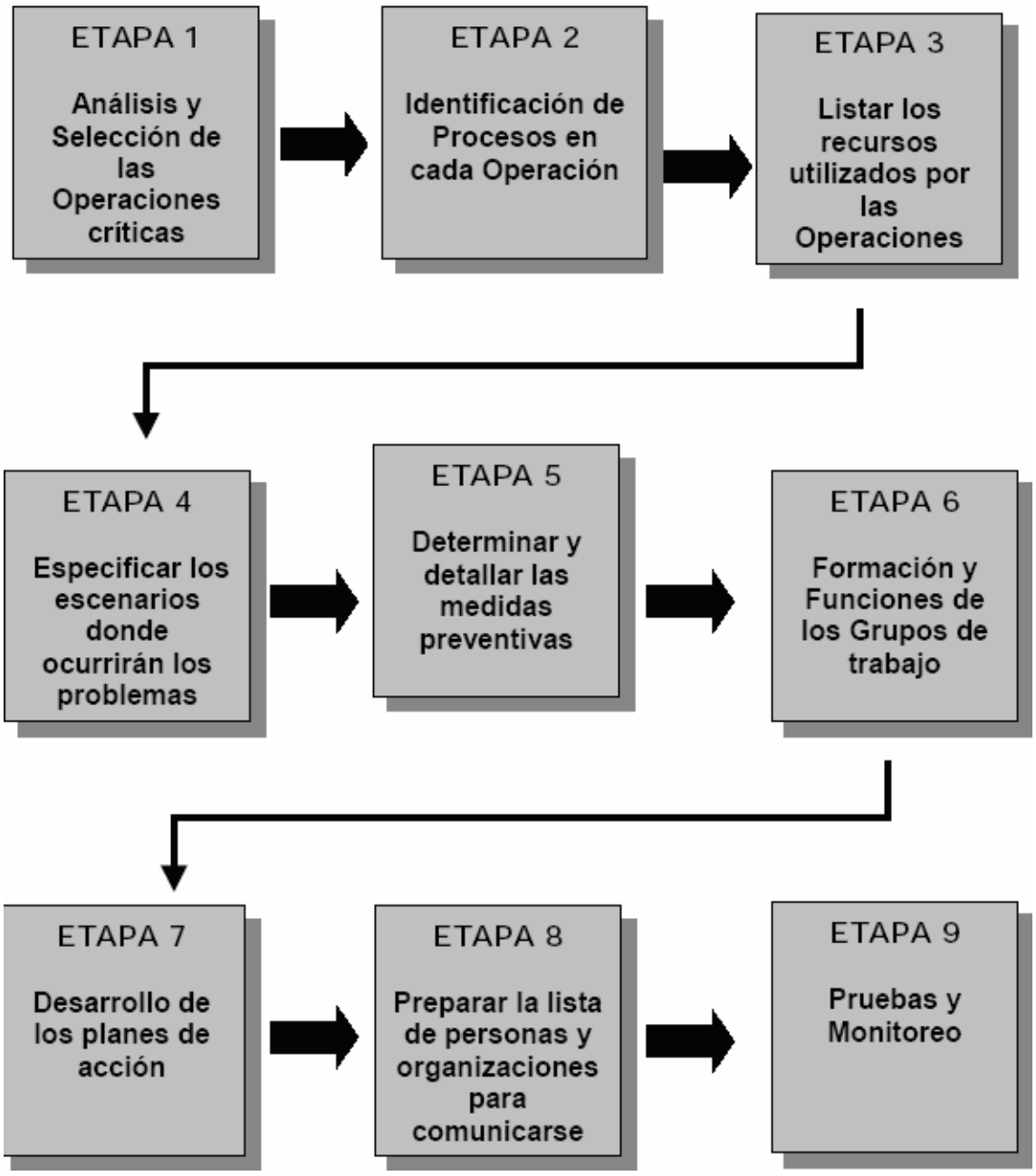
El esquema general del plan de contingencias de los sistemas de información, esta constituido por 3 grandes fases:

1. Fase de Reducción de Riesgos

2. Fase de Recuperación de Contingencia

3. Fase de Organización de un Sistema de Alerta contra Fallas

PARTE IV. PASOS PARA DESARROLLAR EL PLAN DE CONTINGENCIA DE LOS SISTEMAS DE INFORMACION



ETAPA 1. Analizar y Seleccionar las áreas criticas

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 **A** (Alta), **R** (Regular) y **B**(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

Operaciones Críticas Del Sistema De Información

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 LAN	Inventarios Revistas, electrónicas.	**R**
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.	**A**

Procesos Estratégicos Del Negocio

OPERACION PRINCIPAL	CONTENIDO DE LA OPERACION	PRIORIDAD DE LA OPERACIÓN
VENTAS (A)	• Ventas a los clientes	**R**
ESTADÍSTICAS (F)	• Estadísticas mensuales • Estadísticas anuales	**A**
ELABORACION DE INFORMES DE LA ADMINISTRACIÓN (G)	• Elaboración de reportes totales de Administración	**R**

- 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.

Lista De Recursos Utilizados

N° Serie del Recurso	Recurso	Ubicación	Proveedor del Servicio	Recursos de operaciones utilizados por (Proceso)
S1-1	Pc's	Externo	Proveedor A	B-1

S1-2	Pc's	Interno	Soporte técnico	B-1

- 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.

Lista De Periodos Aceptables De Interrupción

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	Mediodía
S1-2	PC´s (Red)	B-1	Cada día	Mediodía
S2-1	Software (Red)	B-1 K-1	Cada día	Mediodía

- Estudia 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.

Lista de problemas probables a ocurrir

N° Serie del	Recurso	Proveedor del	Resultados confirmados	Juicio de compañías

Recurso		Servicio	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	Electrónica O (Fax)	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

ETAPA 2. IDENTIFICAR PROCESOS EN CADA OPERACIÓN

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 nivel de riesgo, como críticos y no críticos.

Procesos Del Área Analizada

Código del Proceso	Procesos	Recursos Utilizados	Código del recurso	Nivel del Riesgo
E- 1	Proceso de los programas	Sistema Eléctrico	R1	Crítico

	que realizan la entrada y salida de la información	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

Como acción seguida se debe 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 una tabla de prioridades.

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 dos.

- 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.

ETAPA 4. ESPECIFICAR 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.

Tabla Matriz De Prioridades De Atención de Riesgos

Se realiza una tabla listando los posibles problemas que se pueden presentar por proceso y/o recurso. Colocando datos tales como:

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

Luego se construye una matriz de prioridad para jerarquizar un posible riesgo en función a su probabilidad de ocurrencia e impacto a la organización, en esta tabla se presenta un posible caso.

Lista de problemas probables a ocurrir

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	

Luego prosigue construir una tabla con medidas preventivas para solucionar los problemas a los posibles riesgos. 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.

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.

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

Los Datos principales que se deben considerar en la construcción de esta tabla son:

- Código del Recurso
- Recurso

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

ETAPA 6. FORMAR Y ESTABLECER FUNCIONES EN 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.

ETAPA 7. DESARROLLAR 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.

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

ETAPA 8. PREPARAR 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

TABLA DE ANALISIS DE RIESGOS

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

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.

ANEXOS

Check List de Registro de Copias de Seguridad

DIARIO DE COPIAS DE SEGURIDAD

Servidor:	**Aplicación de Copias:**
Sistema Operativo:	**Versión:**

OPERACIÓN	
Usuario: _____	Copia Restauración
Fecha: ___/_____/_____	Resultado Ok Error
Hora: _____	Automática Manual

Registro de Pcs

Ubicación				
Usuario				
Tipo de Estación	Pentium Pentium II Pentium III	Multiprocesador Servidor	Otros	Disco: IDE SCSI
Memoria	Cd ROM Si No	Modelo PC	Nº Serie	Nº TCPIP
Impresoras Locales	Números de Serie	Nº Inventario	Impresoras de red Accesibles	
Software Instalado	Sistema Operativo: DOS /Win 3.11	Nº Licencia		Versión

	Windows 95
	Windows 98
	Windows NT
	Windows 2000
	Netware

Proceso de Textos	Nº Licencia	Explorador Internet	Versión
Lotus WordPro			
Microsoft Word 97		Internet Explorer	
Microsoft Word 2000		Netscape Comunicator	Nº
		Opera	Serie

Antivirus	Versión	Cliente Novell	Versión
Panda Software		Si	
Antivirus Toolkit	Fecha	No	
Antivirus Profesional	Actualización		

Otros Aplicativos:

Observaciones

Intervenciones

Formato de Registro de Incidencias de los diversos fabricantes de productos de software y/o Sistemas Operativos

Registro de Consultas al fabricante X. XXX xxx xxx						
Fecha	**nº Consulta**	**Fecha Resolución**	**Consulta**	**Abierta por**	**Persona Contacto**	**Area**
08/01/1999	10849		Descripción del problema y indicación de si genera incidencia			

			para el registro de incidencias general			

Registro de Incidencias Informática						
Fecha Incidencias	**nº de Incidencia**	**Fecha Resolución**	**Descripción Incidencia**	**Abierta por**	**Area**	**Afecta a Planes de Seguridad ó Contingencias**
08/01/2000	1		Descripción del problema y indicación de si genera otras anotaciones en otros registros			Plan Seguridad Si No Plan Contingencias Si No
18/01/2000	2					Plan Seguridad Si No Plan Contingencias Si No
	3					Plan Seguridad Si No Plan Contingencias Si No
	4					Plan Seguridad Si No Plan Contingencias Si No
	5					Plan Seguridad Si No Plan Contingencias Si No
	6					Plan Seguridad Si No Plan Contingencias Si No

	7					Plan Seguridad	Si	No
						Plan Contingencias	Si	No