****

**Plan de Contingencia v1.0**

*Proyecto [Sistema de Matrícula Online]*

*De la [Universidad Tecnológica del Perú]*

Actualizado a Noviembre de 2016

**Historial de Revisiones**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Ítem | Versión | Fecha | Autor | Descripción | Estado | Responsable de Revisión y/o Aprobación |
| 01 | 1.0 | 15/11/2016 | Alex Fernando Rojas | Versión Preliminar | En Revisión | Manuel Sáenz |

**Contenido**

Introducción

PLAN DE CONTINGENCIA 1

I. Definición 1

II. Funciones 2

III. Objetivos 2

IV. Contenido de un plan de contingencia 4

V. Importancia de un plan de contingencia 6

VI. Áreas de aplicación 7

VII. Quienes diseñan el plan de contingencia 7

VIII. Metodología de desarrollo de un plan de contingencia 8

1. Análisis de riesgos 10
2. Evaluación de riesgos 11
3. Jerarquización de las aplicaciones 13
4. Establecimientos de requerimientos de recuperación 14
5. Ejecución 15
6. Pruebas 16
7. Documentación 16
8. Difusión y capacitación 17
9. Mantenimiento 18

IX. Características de un plan de contingencia 19

X. Ejemplo práctico de aplicación 20

**INTRODUCCIÓN**

El propósito del Plan de Contingencia es detallar el conjunto de medidas encaminadas a restaurar la ejecución normal de todas las actividades del proyecto tras la alteración producida por diferentes factores que tienen relación interna o externa con el proyecto.

**PLAN DE CONTINGENCIA**

**I. DEFINICIÓN**

**General:** Un plan de contingencia es el conjunto de procedimientos alternativos a la operativa normal de cada proyecto de software, cuya finalidad es la de permitir el funcionamiento de ésta, aun cuando alguna de sus funciones deje de hacerlo por culpa de algún incidente tanto interno como ajeno al proyecto de software.

**Especifica**: El plan de contingencia debe cubrir todos los aspectos que se van a adoptar tras una interrupción, lo que implica suministrar el desarrollo alternativo y para lograrlo no solo se deben revisar las operaciones cotidianas, sino que también debe incluirse el análisis de los principales distribuidores, clientes, negocios y socios, así como la infraestructura en riesgo. Esto incluye cubrir los siguientes tópicos: hardware, software, documentación, talento humano y soporte logístico; debe ser lo más detallado posible y fácil de comprender.

**II. FUNCIONES**

Los planes de contingencia cumplen las siguientes funciones:

* Determinar acciones preventivas, reduciendo el grado de vulnerabilidad y exposición al riesgo.
* Reducir el tiempo de reacción.
* Dimensionar el riesgo potencial.
* Tomar decisiones rápidas ante anormalidades o falla.
* Generar cultura de seguridad.
* Asegurar la estabilidad de la organización.
* Hacer sistemático, ordenado y eficiente lo que, sin un plan debidamente concebido y ensayado, sería arbitrario, caótico e ineficiente.
* Cumplir con las normativas legales.

**III. OBJETIVOS**

Los objetivos de un plan de contingencia son:

* Reanudar con la mayor brevedad posible las funciones del desarrollo más críticas, en aras a minimizar el impacto de manera que no afecte la planificación, los tiempos establecidos para los entregables acordados además para que los procesos queden garantizados y se conserven los objetivos estratégicos del proyecto.
* Evaluar los riesgos, así como los costos de los procedimientos de contingencia requeridos cuando se presenta una interrupción de las actividades, de forma que sólo se inviertan los recursos necesarios.
* Optimizar los esfuerzos y recursos necesarios para atender cualquier contingencia de manera oportuna y eficiente, definiendo las personas responsables de las actividades a desarrollar antes y durante la emergencia.

Puede concluirse de lo anterior que el aspecto clave es proteger el personal y la información vital para la organización. Esta protección conduce a realizar un análisis de los riesgos a que está sometida dicha información y la forma de minimizar el efecto de esos riesgos.

Esto mismo lleva a desarrollar los mecanismos necesarios que permitan identificar los elementos involucrados y mitigar los efectos del desastre o salir de él lo más exitosamente posible.

IV. CONTENIDO DE UN PLAN DE CONTINGENCIA

El plan de contingencias comprende tres sub-planes. Cada plan determina las contramedidas necesarias en cada momento del tiempo respecto a la materialización de cualquier amenaza:

* El **plan de respaldo**.

Contempla las contramedidas preventivas **antes** de que se materialice una amenaza. Su finalidad es evitar dicha materialización.

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

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

* El [**plan de recuperación**](/wiki/Plan_de_Recuperaci%C3%B3n_ante_Desastres).

Contempla las medidas necesarias **después** de materializada y controlada la amenaza. Su finalidad es **restaurar** el estado de las cosas tal y como se encontraban antes de la materialización de la amenaza.

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.

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.

**V. IMPORTANCIA DE UN PLAN DE CONTINGENCIA**

La necesidad de un plan de contingencia esta relacionada con el impacto potencial que provocaría una interrupción parcial o total de los servicios de información, sobre el desarrollo de las actividades de la organización. Conforme las organizaciones aumentan la automatización de sus operaciones, éstas son más dependientes de la tecnología que capta, almacena y procesa la información vital para su funcionamiento.

Su importancia radica en que:

* Permitirá una respuesta rápida en caso de incidentes, accidentes o estados de emergencia.
* Permitirá ejecutar un conjunto de normas, procedimientos y acciones básicas de respuesta que se debería tomar para afrontar semanera oportuna, adecuada y efectiva, ante la eventualidad de incidentes, accidentes y/o estados de emergencias que pudieran ocurrir tanto en las instalaciones como fuera de ellas.

**VI. ÁREAS DE APLICACIÓN**

Los planes de contingencia tienen una aplicación muy amplia y variada, puede darse tanto para empresas (comerciales o industriales) a nivel gubernamental (como en el caso de emergencias regionales), para casos muy específicos como derrame de petróleo, incendios, escasez de alimentos, administración de proyectos de cualquier índole como: construcciones y desarrollo de software u otros.

**VII. QUIÉNES DISEÑAN UN PLAN DE CONTINGENCIA**

El plan de contingencia debe ser elaborado por los expertos de la prevención (Defensa Civil, Bomberos, Gerencia de Seguridad de una empresa u otros organismos).

Se debe declarar una estructura formal, que se integrará de acuerdo a las necesidades y el tamaño de la institución. Debe definirse claramente sus responsabilidades y funciones, además debe tener la autoridad suficiente para establecer los lineamientos correspondientes.

**VIII. METODOLOGÍA DE DESARROLLO DE UN PLAN DE CONTINGENCIA**

El diseñar e implementar un plan de contingencia para recuperación de desastres no es una tarea fácil; puede implicar esfuerzos y [gastos](http://www.monografias.com/trabajos10/rega/rega.shtml%20\%20ga) considerables, sobre todo si se está partiendo de cero.

Una solución comprende las siguientes actividades:

* Debe ser diseñada y elaborada de acuerdo con las necesidades de la empresa.
* Puede requerir la [construcción](http://www.monografias.com/trabajos35/materiales-construccion/materiales-construccion.shtml) o adaptación de un sitio para los equipos computacionales.
* Requerirá del [desarrollo](http://www.monografias.com/trabajos12/desorgan/desorgan.shtml) y prueba de muchos procedimientos nuevos, y éstos deben ser compatibles con las operaciones existentes.
* Se hará participar a personal de muchos departamentos diferentes, el cual debe trabajar en conjunto cuando se desarrolle e implemente la solución.
* Implicará un compromiso entre [costo](http://www.monografias.com/trabajos7/coad/coad.shtml%20\%20costo), [velocidad](http://www.monografias.com/trabajos13/cinemat/cinemat2.shtml%20\%20TEORICO) de recuperación, medida de la recuperación y alcance de los desastres cubiertos.

Como con cualquier [proyecto](http://www.monografias.com/trabajos12/pmbok/pmbok.shtml) de [diseño](http://www.monografias.com/trabajos13/diseprod/diseprod.shtml), un [método](http://www.monografias.com/trabajos11/metods/metods.shtml) estructurado ayuda a asegurar de que se toman en cuenta todos estos factores y de que se les trata adecuadamente.

El desarrollo de un plan de contingencias conlleva las siguientes etapas:

1. Análisis de riesgos.
2. Evaluación de riesgos.
3. Jerarquización de las aplicaciones.
4. Establecimientos de requerimientos de recuperación.
5. Ejecución.
6. Pruebas.
7. Documentación.
8. Difusión y capacitación.
9. Mantenimiento.

**1. Análisis de riesgos**

Durante esta etapa se identifican los procesos críticos o esenciales y sus repercusiones en caso de no estar en funcionamiento. El primer componente del plan de contingencia debe ser una descripción del servicio y el riesgo para ese servicio.  
  
 Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño producido mediante la evaluación y análisis del problema donde se revisen las fortalezas, oportunidades, debilidades y amenazas, lo que permitirá recuperar en el menor tiempo posible el proceso perdido.

Un diagrama de la arquitectura de todos los componentes del sistema facilitará la realización de un inventario de los elementos que pueden necesitar ser restituidos tras un desastre. No hay que olvidar que también el software necesita ser reemplazado, y que todos los productos software relevantes han de ser identificados.

Una omisión en el inventario fácilmente puede dar lugar a una recuperación fallida tras un desastre. El sistema de aplicación puede no encontrarse preparado para su uso si alguno de sus componentes no está disponible; en tal caso, es aconsejable estar constantemente a la expectativa de los nuevos elementos que pueden haberse olvidado.

Uno de los aspectos menos agradables a tener en cuenta, y que a menudo se pasa por alto, es que las personas esenciales se vean afectadas por el desastre y sea necesario recurrir a otras para realizar sus labores. Una formación diversificada en los sistemas dentro de la organización pude ayudar a reducir el impacto de la indisponibilidad de uno de los colaboradores.

**2. Evaluación de riesgos**

Igualmente se debe determinar el costo que representa para la organización el experimentar un desastre que afecte a la actividad empresarial.En el caso de los sistemas informáticos, la preocupación principal es comprender la cantidad de pérdida financiera que puede provocar la interrupción de los servicios, incluyendo los que se basan en las redes.

Se debe evaluar el nivel de riesgo de la información para hacer:

* Un adecuado estudio costo/beneficio entre el costo por pérdida de información y el costo de un sistema de seguridad.
* Clasificar la instalación en términos de riesgo (alto, mediano, bajo) e identificar las aplicaciones que representen mayor riesgo.
* Cuantificar el impacto en el caso de suspensión del servicio.
* Determinar la información que pueda representar cuantiosas pérdidas para la organización o bien que pueda ocasionar un gran efecto en la toma de decisiones.

Los costos de un desastre pueden clasificarse en las siguientes categorías:

* Costos reales de reemplazar el sistema informático: El costo real de los equipos y el software es fácil de calcular, y depende de si se dispone de un buen inventario de todos los componentes de la red necesarios.
* Costos por falta de producción. La empresa tiene una correcta valoración de la cantidad de trabajo realizado diariamente y su valor relativo.
* Costos por negocio perdido
* Costos de reputación: Son los más difíciles de evaluar. Estos costos se producen cuando los clientes pierden la confianza en la empresa y se llevan su negocio a otro sitio. Los costos de reputación crecen cuando los retardos en el servicio a los clientes son más prolongados o frecuentes.

**3. Jerarquización de las aplicaciones**

Es necesario definir anticipadamente cuales son las aplicaciones primordiales para la organización. Para la determinación de las aplicaciones preponderantes, el plan debe estar asesorado y respaldado por las directivas, de tal forma que permita minimizar las desavenencias entre los distintos departamentos y/o divisiones.

El plan debe incluir una lista de los sistemas, aplicaciones y prioridades, igualmente debe identificar aquellos elementos o procedimientos informáticos como el hardware, software básico, de telecomunicaciones y el software de aplicación, que puedan ser críticos ante cualquier eventualidad o desastre y jerarquizarlos por orden de importancia dentro de la organización. También se deben incluir en esta categoría los problemas asociados por la carencia de fuentes de energía, utilización indebida de medios magnéticos de resguardo o back up o cualquier otro daño de origen físico que pudiera provocar la pérdida masiva de información.

Por ejemplo: el departamento de recursos humanos afirmará que el sistema de nóminas es el más importante, el departamento de ventas dirá que es su sistema de entrada de pedidos, el departamento de producción insistirá en su control de inventario y el departamento de compras asignará el papel de más importante a su sistema de facturación. Desgraciadamente, no todos estos sistemas pueden ser el más importante; por lo tanto, es fundamental que la dirección ayude a determinar el orden en que los sistemas serán recuperados.

***Esta sección del plan debería ser firmada por la dirección para minimizar las desavenencias.*** Es mucho mejor intentar lograr que un sistema pequeño funcione, que no uno más grande, y de esta manera se ahorrará gran cantidad de tiempo en el proceso. De hecho, cuando se está asignando las prioridades a las aplicaciones junto con la dirección, también es posible beneficiarse de la determinación del número mínimo de estaciones de trabajo necesarias para tener el sistema accesible. El tamaño de la red siempre puede incrementarse a posteriori una vez el sistema esté en funcionamiento.

**4. Establecimientos de requerimientos de recuperación**

En esta etapa se procede a determinar lo que se debe hacer para lograr una óptima solución, especificando las funciones con base en el estado actual de la organización. De esta forma es necesario adelantar las siguientes actividades: profundizar y ampliar la definición del problema, analizar áreas problema, documentos utilizados, esquema organizacional y funcional, las comunicaciones y sus flujos, el sistema de control y evaluación, formulación de las medidas de seguridad necesarias dependiendo del nivel de seguridad requerido, justificación del costo de implantar las medidas de seguridad, análisis y evaluación del plan actual, determinar los recursos humanos, técnicos y económicos necesarios para desarrollar el plan, definir un tiempo prudente y viable para lograr que el sistema esté nuevamente en operación.

**5. Ejecución**

Una vez finalizado el plan, es conveniente elaborar un informe final con los resultados de su ejecución cuyas conclusiones pueden servir para mejorar éste ante futuras nuevas eventualidades. En esta fase hay que tener muy presente que el plan no busca resolver la causa del problema, sino asegurar la continuidad de las tareas críticas de la empresa.

En la elaboración del plan de contingencias deben de intervenir los niveles ejecutivos de la organización, personal técnico de los procesos y usuarios, para así garantizar su éxito, ya que los recursos necesarios para la puesta en marcha del plan de contingencia, necesariamente demandan mucho esfuerzo técnico, económico y organizacional.

**6. Pruebas**

Es necesario definir las pruebas del plan, el personal y los recursos necesarios para su realización. Luego se realizan las pruebas pertinentes para intentar valorar el impacto real de un posible problema dentro de los escenarios establecidos como posibles. En caso de que los resultados obtenidos difieran de los esperados, se analiza si la falla proviene de un problema en el ambiente de ejecución, con lo cual la prueba volverá a realizarse una vez solucionados los problemas, o si se trata de un error introducido en la fase de conversión; en este último caso pasará nuevamente a la fase de conversión para la solución de los problemas detectados. Una correcta documentación ayudará a la hora de realizar las pruebas. La capacitación del equipo de contingencia y su participación en pruebas son fundamentales para poner en evidencia posibles carencias del plan.

**7. Documentación**

Esta fase puede implicar un esfuerzo significativo para algunas personas, pero ayudará a comprender otros aspectos del sistema y puede ser primordial para la empresa en caso de ocurrir un desastre. Deben incluirse, detalladamente, los procedimientos que muestren las labores de instalación y recuperación necesarias, procurando que sean entendibles y fáciles de seguir.

Es importante tener presente que la documentación del plan de contingencia se debe desarrollar desde el mismo momento que nace, pasando por todas sus etapas y no dejando esta labor de lado, para cuando se concluyan las pruebas y su difusión.

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.

**8. Difusión y capacitación**

Cuando se disponga del plan definitivo y aprobado, es necesario hacer su difusión y capacitación entre las personas encargadas de llevarlo a cargo. Es necesario asegurar la disponibilidad de copias extra del plan para su depósito en la instalación exterior en cualquier otro lugar además del lugar de trabajo. Manténgase una lista de todas las personas y ubicaciones que tienen una copia del plan. Cuando se actualice el plan, sustituya todas las copias y recoja las versiones previas.

No debe olvidarse que el éxito del Plan en alto grado depende de la disponibilidad y participación de personal bien capacitado, quienes hayan estudiado el plan, recibido el entrenamiento e incluso participado en las modificaciones, si hubo, de tal manera que se sientan que son parte del plan, los motivará a trabajar en situaciones de contingencia.

Además, es necesario que como parte de la capacitación se dé entrenamiento en la seguridad personal, ya que el recurso humano es el más valioso para cualquier organización.

**9. Mantenimiento**

El mantenimiento del plan comienza con una revisión del plan existente y se examina en su totalidad realizando los cambios en la información que pudo haber ocasionado una variación en el sistema y realizando los cambios que sean necesarios. En ese instante, se debe volver a evaluar los sistemas de aplicación y determinar cuáles son los más importantes para la organización. Las modificaciones a esta parte del plan causarán modificaciones consecutivas a los procedimientos de recuperación. Sin embargo, esto no debería verse como un problema porque probablemente la sección de procedimientos tenga que actualizarse de todas formas debido a otros cambios. Si se han realizado modificaciones al sistema de copias de seguridad, hay que cerciorarse de incluir la información sobre el funcionamiento del nuevo o actualizado sistema.

**IX. CARACTERÍSTICAS DE UN PLAN DE CONTINGENCIAS**

El plan de contingencias debe presentar los siguientes atributos:

1. Responder a las necesidades particulares de la organización (autentico)
2. Factible
3. Interdepartamental: que involucre a los departamentos requeridos.
4. Escrito.
5. Suscrito, legitimado: debe tener el apoyo por escrito autorizado por los mandos superiores del a administración.
6. Conocido - divulgado.
7. Actualizado.
8. Probado.

Se debe presentar de forma:

1. Clara y concisa.
2. Esquemática.
3. De vocabulario sencillo.
4. Adaptable - flexible.
5. Modular: que facilite su elaboración, evaluación y actualización.
6. Con cubiertas de material de color llamativo, preferiblemente, para que se pueda distinguir del resto de los manuales.

**X. EJEMPLO PRÁCTICO DE APLICACIÓN DE UN PLAN DE CONTINGENCIA EN UN ÁREA DE TIC.**

Cuando se habla de una contingencia, se debe fundamentalmente al a falta de prevención o a la poca o mala planeación. Lo primero es hacer un **análisis de los riesgos** y la probabilidad de ocurrencia. Esta información puede ser tomada de datos históricos o de estimaciones cualitativas.

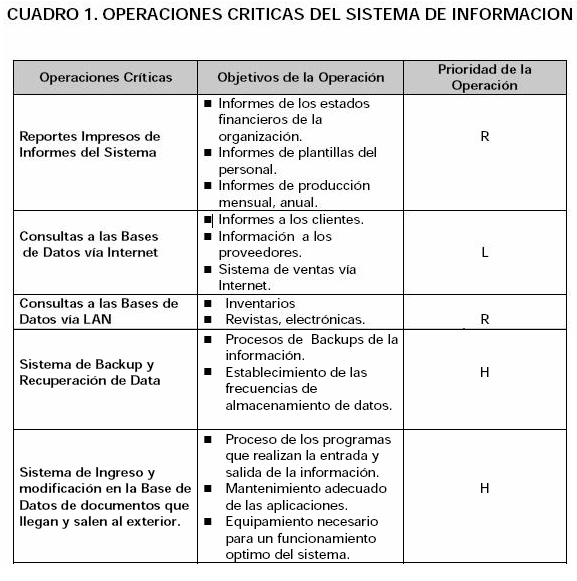
**Análisis y Selección de las Operaciones Críticas**

En esta etapa hay que definir cuáles serán nuestras operaciones críticas y tienen que ser definidas en función a los componentes de los sistemas de información los cuales son:

Datos, Aplicaciones, Tecnología Hardware y Software, instalaciones y personal.

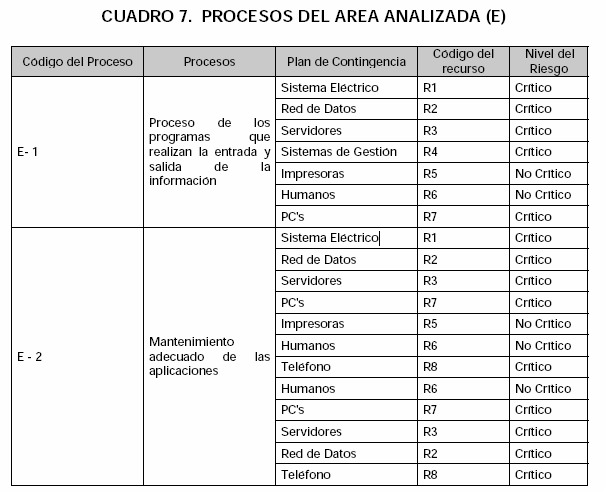
Dentro de las cuales podemos identificar las siguientes, las cuales pueden variar de sistema a sistema:

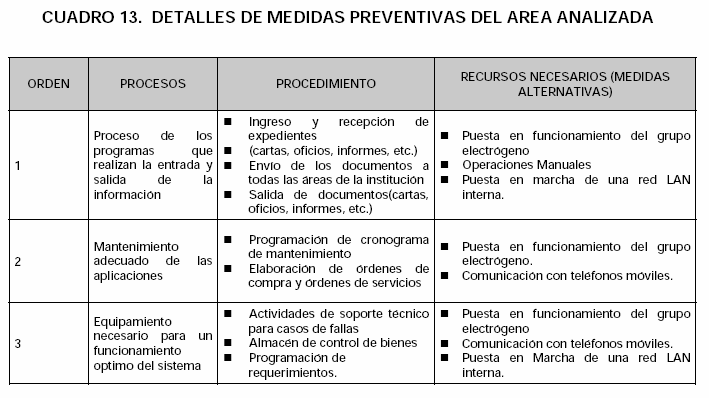
* Reportes Impresos de Informes del Sistema.
* Consultas a las Bases de Datos vía Internet.
* Consultas a las Bases de Datos vía LAN.
* Sistema de Backup y Recuperación de Data.
* Sistema de ingreso y modificación en la Base de Datos de documentos que llegan y salen al exterior.



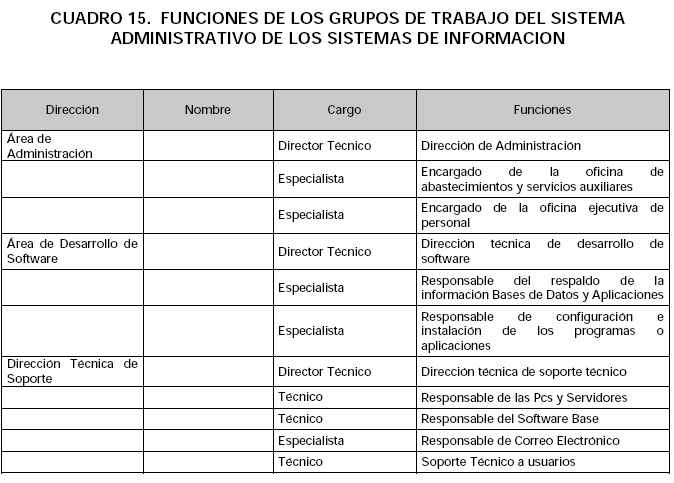
Se ha listado los procesos críticos de manera genérica y evaluado su grado de importancia en función a la magnitud del impacto si los procesos pueden detenerse, y luego clasificados en niveles **H** (Alta), **R** (Regular) y **L** (Bajo)

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









**Cuando el problema es en el servidor**

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.

**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).

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.

**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.

**CONCLUSIÓN**

La reanudación de las actividades ante una calamidad puede ser una de las situaciones más difíciles con las que una organización deba enfrentarse. Tras un desastre, es probable que no haya posibilidades de regresar al lugar de trabajo o que no se disponga de ninguna de los recursos acostumbrados. Incluso, es posible que no se pueda contar con todo el personal. La preparación es la clave del éxito para enfrentar los problemas. No existe un plan único para todas las organizaciones, esto depende mucho de la capacidad de la infraestructura física como de las funciones que realiza.

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

El desarrollo de un plan de este tipo es costoso, involucra tiempo y una total disposición de la administración de la organización. Es justificable desde el punto de vista de costo en que se incurre si sucede una contingencia que afecte significativamente las operaciones vitales y no se está preparado para hacerle frente a esa situación.

El plan debe ser revisado periódicamente. Generalmente, la revisión será consecuencia de un nuevo análisis de riesgo.