

INTRODUCCIÓN

Las políticas y procedimientos de respaldo de la información de una empresa dedicada a la fabricación de determinados productos, cuyo consumo sea masivo, con sucursales diseminadas por todo (o la mayoría) del territorio nacional y un sistema de cómputos centro distribuido, no puede coincidir totalmente con las políticas y procedimientos de una empresa de servicios cualquiera que sólo posee dos sucursales en todo el territorio nacional. Ahora bien, cien criterios permanecen invariables, lo que cambiará la aplicación de los mismos.

PLANEACIÓN DE CONTIGENCIA

El tiempo esperado máximo de duración del plan. Los roles, responsabilidad y autoridad son las claves para una marcha exitosa, determinando cual es el rol de cada uno de los sectores ante la contingencia y como se alterna los procedimientos habituales para dar lugar a los procedimientos de contingencia y que recursos son necesarios para operar en modo de contingencia y cuales son los habituales utilizados que no se deben utilizar, obviamente esto debe estar debidamente documentado y verificado lo más profundamente posible.

Un detalle muy importante es la capacitación al personal que debe intervenir en el caso de que el incidente se produzca. De igual manera hay que prever como será la recuperación de los datos de operación durante la contingencia.

El propósito de un Plan de Contingencia es salvar o reducir los efectos de una falla, por medio de ejecución de un conjunto de acciones, previamente definidas y conocidas por el personal correspondiente. Se entiende que estas acciones se realizan inmediatamente ocurrida la falla.

El Plan de Contingencia apunta a las consecuencias de situaciones de fallas o situaciones inesperadas, imprescindibles, no complementadas o inesperadas. Los Planes de Contingencia también deben considerar situaciones que están más allá del control de la empresa, por ejemplo; fallas en los proveedores, el entorno o los propios clientes.

En la generalidad de los casos los empresarios y los administradores se olvidan de elaborar los mecanismos alternos, los documentos de soporte, dar los entrenamientos y crear la infraestructura tecnológica adecuada que permita la supervivencia del negocio.

COMISIONES DE TRABAJO, UBICACIÓN Y RESPONSABILIDAD.

Se reúne el grupo consultor, lo cual contiene las siguientes personas:

- Coordinador centro de respaldo.
- Un supervisor sala de máquina.
- Operador sala de máquina.
- Administrador de sistema operativo/base de datos.
- Encargado de aplicaciones.
- Analista de integridad de sistema.

Una vez reunido dicho grupo planifica todos los puntos a desarrollar, y existe un líder que se encarga de asignar las diferentes tareas que se van a desarrollar en un proyecto.

A través de los Backup, para de esta forma poder subir el sistema en el momento requerido, adiestramiento del personal y tenerlo disponible.

- Comité
- Plan de Contingencia
- Presidente
- Vice-presidente
- Tres Ingenieros

FORMACIÓN DEL EQUIPO.

- Plan de Contingencia
 - Director del área de informática
 - Sub-director de procesamiento electrónicos de datos.
 - Gerente de departamento
 - Gerente de centro de cómputo
 - Gerente de administración de información
 - Gerente de programación
 - Gerente de Cementación
-
- Auditores internos y externos de informática
 - Gerente Soporte Técnico
 - Operadores

PRUEBA DEL PLAN DE CONTINGENCIA

Se realizan haciendo simulacros de desastres durante el cual se aplicarán las medidas previstas en el Plan de Contingencia.

Cada prueba varía dependiendo del desastres que se quiere reguardar el sistema.

ETAPAS DE UN PLAN DE CONTINGENCIA

- Identificar las situaciones para las cuales es necesario planificar y priorizar de ser necesario.
- Considerar la posibilidad de agrupar dichas situaciones de modo de reducir el tiempo de planificación.
- Considerar los cursos de accion de factibles.
- Seleccionar el curso de acción más apropiado.
- Decidir el criterio a utilizar para determinar cuales acciones se tendrán en cuenta.
- Dividir las acciones en grupos.
 - Acciones de prevención deben tener prioridad.
 - Acciones de contingencia se ejecutan sólo si el evento ocurre.
 - Acciones complementarias se ejecutan si no ocurren el evento.
- Si las situaciones de posibles causas de fallas son identificables, documentarlas. Puede ser mucho más difícil identificar cuando la crisis ocurre.
- En caso de identificar causas posibles de falla (Por ejemplo: el fenómeno del año 2000), considerar métodos para la identificación exacta del problema y las maneras de solucionarlo.
- Crear documentación para el personal que se responsabilizará de atender la situación de crisis.

VENTAJAS DE LA PLANEACIÓN CONTINGENCIA

– En un plan contra desastre que permite la continuación o el reinicio de las operaciones si presentan algún problema.

- La idea es no ser la única entidad que posea equipo de determinadas marca en el país. Esto es peligroso, ya que en caso de averías o fallas del equipo puede ser difícil y en algunos casos hasta imposible seguir operando sus sistemas de información.
- La idea es no ser la única entidad que posea equipo de determinada marca en el país. Esto es peligroso, ya que en caso de averías o fallas del equipo puede ser difícil y en algunos casos hasta imposible seguir operando sus sistemas de información.
- Tener conocimientos de si dentro de los posibles Backups, existen empresas dispuestas a respaldar el conjunto de las operaciones de la entidad en sus instalaciones.
- Verificar cuales empresas comparten la tecnología usada por la compañía para la cual labora, con miras a concertar acuerdos de respaldo con ellas.
- La base tecnológica global, entiéndase: red de comunicaciones, software ambiental y entrenamiento de personal debe estar cubierta. Es decir nada ni nadie debe ser imprescindible.
- Tener instalada la infraestructura para trasladar las operaciones de un edificio a otro.

DESVENTAJAS DE LA PLANEACIÓN CONTINGENCIA

- En la medida en que los recursos de contingencia son globales, aumentan los costos de su operación, debido a que los ingredientes deben estar representado uno a uno.
- Se pueden tener diferentes niveles de contingencia. Estos consisten en cómo enfrentar las operaciones de la empresas y dependerán de los recursos que la empresa este dispuesta a asignar y el grado que esta haya definido que va a satisfacer el servicio a los clientes. Por ende, los costos estarán relacionados con el nivel de servicios.
- El entorno del edificio debe contar con la seguridad física apropiada, aislado de otras edificaciones en los alrededores. El motivo de esto que bajo ciertas circunstancias especificas en riesgo la integridad de la planta física del centro de Computo.

ESTRATEGIA DE LA CONTINGENCIA

El entorno del edificio debe contar con la seguridad física apropiada, aislado de otras edificaciones en los alrededores. El motivo de esto que bajo ciertas circunstancias especificas en riesgo la integridad de la planta física del centro de Computo.

Debe acordarse con los bomberos la ubicación de hidrantes en los alrededores de los edificios. La instalación eléctricas debe ser técnicamente calificada; es decir estar toda tubulada, deben existir planos de la misma, etc.

Todas las líneas eléctricas y de servicio telefonico deben ser soterradas desde la calle hasta la entrada del edificio, a fin de evitar que

los accidentes de tránsito puedan interrumpir el servicio.

Los cristales usados en edificación deben ser aislantes, es decir, capaces de resistir el fuego; igualmente los mismos deben resistir el impacto del proyecto belísticos.

El acceso a las instalaciones deben ser automático; es decir capaces de resistir un documento de administración de control electrónico que opere las puertas del Centro de Computo.

El sistema de producción debe contar con una bitácora continua para registrar todos los procesos que se efectúan en el Centro de Operaciones. Es importante la bitácora, pues en ciertas ocasiones pueden contribuir a que se descubra que o quién lo ocasionó la contingencia, cuando se originó la misma y a partir de que punto, etc.

Otros recursos de tipo tecnológico que deben considerarse con los siguientes.

La infraestructura eléctrica, la cual debe ser instalada por expertos, tomando en cuenta en todos los casos la redundancia. Esto equivale a decir: Energía del sector público o de uso (en nuestro caso la suministrada por la Corporación Dominicana de Electricidad (CDE) Suministro de energía por generadores deben de tener su propio respaldo y estar sincronizados; Los interruptores deben de tener su propio respaldo para transferencia en secuencia. Las unidades de Energía Interrumpida (UPS por su siglas en Inglés) deben de estar en cascada y operar en secuencia.

Con base en todos los aspectos supra-indicados, se establece planes de contingencia alternativos según los diferentes tipos de desastres y sus magnitudes (parciales / recuperación a corto plazo, considerable / recuperación a mediano plazo, totales / recuperación a largo plazo). Dichos planes deben incluir estadísticas aproximadas del tiempo requerido para restaurar los diversos sistemas en otra instalación física, teniendo además dos personas para cada sistema. Es decir, un sistema de cobros debe tener como responsables a una persona del Centro de Computos (ó Departamento de servicios de información, o como se le denomina a dicho departamento, centro o división en la empresa en cuestión) y a una persona del área de usuarios correspondientes, que en este caso sería el Gerente o Encargado de Cobros.

Además, el plan debe incluir un diagrama de flujo de datos y una estimación del volumen diario de datos a procesar. Es recomendable que complete un renglón de los útiles y materiales de oficina necesarios (tales como: máquinas calculadoras, perforadoras, grabadoras, fotocopadoras, formularios reimpresos y documentos fuentes), los cuales deben estar disponibles para la operación normal del sistema.

¿QUÉ ES UN PLAN DE CONTINGENCIA?

Es un programa de procedimientos alternativos a la forma de operar normal de su empresa. Esta herramienta le ayudará a que los procesos críticos de su empresa y organización continúen funcionando a pesar de una posible falla en los sistemas computarizados derivados del problema informático del año 2000.

El plan de contingencia es parte integral de un proyecto de convención año 2000, no lo sustituye. La contingencia sólo es aplicable, por su propia naturaleza, por un período de tiempo corto y bajo condiciones de emergencia.

El que en su organización tenga un plan de contingencia no afecta su reputación o la de su equipo de trabajo abocado a las tareas de conversión con miras al año 2000. al contrario, la adopción de un plan de contingencia significa que su organización es provisorio y que está cubriendo ante cualquier eventualidad informática que conlleve la llegada del año 2000.

El plan de contingencia es, por tanto, parte integral de un proyecto

Y2K, ya que un proyecto de conversión informática año 2000 no estará completo si carece de dicho plan.

La decisión de elaborar un plan de contingencia debe partir de este nivel directivo ya que está en juego la supervisión de la propia empresa u organización.

¿POR QUÉ ES NECESARIO DESARROLLAR UN PLAN DE CONTINGENCIA?

Un proyecto de conversión informático le ayuda administrar el riesgo a la llegada del año 2000. en la medida que tenga un mejor proyecto Y2K, Usted minimiza el riesgo. Sin embargo ni aún el mejor proyecto Y2K posible, elimina totalmente el riesgo relacionado con la llegada del año 2000 debido a que el problema informático implica:

- Un gran número de impacto que no puede ser conocidos con anticipación.
- Muchos de esos impactos caen del control en su empresa u organización.

¿EN QUE CASO SE REQUIERE APLICAR UN PLAN DE CONTINGENCIA?

- Si falla alguno de sus sistemas críticos y/o si se contamina alguno de sus sistemas críticos con información no compatible proveniente del exterior.
- Si falla algún sistema de telecomunicaciones o enlace.
 - Si falla alguno de sus proveedores informáticos clave.
 - Si falla alguno de sus otros proveedores clave.
 - Si falla algún servicio básico.
 - Si se presentan fallas encadenadas y generalizadas

Es decir en todos los casos que se requiera un proyecto Y2K, pero tendrá mayor prioridad su desarrollo si:

- Su empresa u organización tiene sistemas y/o equipos críticos auto matizados no compatibles con el año 2000 y aún no cuenta con un proyecto de conversión Y2K, se recomienda desarrollar un plan de contingencia a la par que inicie su proyecto Y2K, ya que en este caso es muy probable que no tenga tiempo suficiente para concluir a tiempo la conversión de dichas tareas básicas antes del 2000.
- Ya cuenta con un proyecto Y2K, pero visualiza que sus sistemas y/o equipos críticos no estarán convertidos para cuando llegue el año 2000.
- Ya concluyó su proyecto año 2000 o está plenamente seguro de que su proyecto año 2000 estará listo para antes de que arribe dicho, pero no está seguro de que sus principales clientes y proveedores tengan convertido a tiempo sus respectivos sistemas o equipos.

¿CÓMO PUEDO HACERLO?

La siguiente guía le orientan cómo elaborar un plan de contingencia. Esta consiste en dos partes cada una con varios pasos los cuales deben adecuarse al caso específico de su empresa u organización.

• DESARROLLO Y PRUEBAS:

Paso 1. Identificación del problema

Paso 2. Preparación del plan

Paso 3. Pruebas y afinación del programa.

• PUESTA EN PRACTICA:

Paso 1. Ejecución en tiempo real.

Paso 2. Retorno a las actividades normales.

• **DESARROLLO Y PRUBAS:**

Toma conciencia.

La autorización de desarrollar el plan debe darse la más alto nivel de su empresa u organización. Debe ser coordinadas por las personalidades idóneas.

• **JERARQUICE PRIORIDADES:**

Detectados todos los procesos críticos y los sistemas y equipos autorizados de su organización que los apoyan, incluyendo las interconexiones con sus principales proveedores y clientes, clasifique las tareas críticas en dos categorías.

- Aquellas que no estarán listas para cuando llegue el año 2000.
 - Aquellas que se prevé estarán listas para cuando lluegue el año 2000.
 - Entre otras tareas.
 - Elabore un manual sencillo sobre el plan de contingencia y asegúrese de que lo conozca todo el personal de su organización. El manual debe contener, al menos, lo siguiente:
 - Objetivos del plan. Defina si el plan permitirá continuar la operación de tareas críticas por ejemplo:
 - Continuar las actividades en forma normal.
 - Continuar las actividades con un deterioro aceptable en la calidad y productividad.
 - Diferir las actividades por razones económicas o de seguridad.
 - Calcule el tiempo requerido para elaborar el plan.
 - Estime los recursos humanos y materiales que requiere el plan.
 - Tome en cuenta las fechas críticas para realizar el plan (desde fase de pruebas hasta retorno a las actividades normales).
 - Establezca un centro físico de información sobre el desarrollo del plan.
 - Defina criterios para iniciar y terminar la contingencia
 - Incluya el nombre y forma de contactar al responsable del plan y en su caso a los integrantes del equipo de contingencia.
- **CONTRIBUYA A GENERAR UN AMBIENTE DE CONFIANZA PREVENIENDO EL COMPORTAMIENTO SOCIAL ANTE LA LLEGADA DEL AÑO 2000.**

En este sentido se recomienda que:

- Informe periódicamente a sus empleados, proveedores y clientes sobre las medidas que su organización está realizando para enfrentar el reto informático del año 2000.
- Recopile información sobre el estado de avance de la conversión en áreas estratégicas como servicios bancarios, abasto de energía, de alimentos básicos, red telefónica, etc, hágala del conocimiento de su

empleados, clientes y proveedores.

• **ORIENTE LAS PRUEBAS DE SU PLAN PRINCIPALMENTE A:**

- Preservar y proteger sus bases de datos, ya sea mediante un resguardo ante de que se presente las fallas o mediante una impresión de la base.
- Detectar oportunidades la generación de datos críticos erróneos debido al uso de fechas que involucran el cambio del año 2000.
- Asegurar mediante mecanismos alternativos que funcionen las tareas críticas que dependen de las interconexiones tanto al interior de su organización.