Esquema para la Elaboración de un Plan de Continuidad de Negocios de una Organización

RESPONSABLE: *Lic.* Wilder Roger Miñano León

MIEMBRO: *Ing.* Edgard Melquiades Pilco Apaza

RESUMEN. ***En el presente trabajo se presenta un esquema para la elaboración de un Plan de Continuidad de Negocios de una Organización que comprende aspectos generales tales como los objetivos, recuperación tras siniestros, la continuidad en los negocios; aspectos específicos tales como el concepto de la gestión de la continuidad de negocios, costos, planes y una guía para la elaboración de un Plan de Continuidad de Negocio. Asimismo, se describen los pasos-clave para la formulación de un Plan de Continuidad de Negocio; y para mayor ilustración se presentan dos ejemplos.***

ABSTRACT ***In the present work is presents a Scheme for the Elaboration of a Plan of Continuity of Business of an Organization who understands general aspects such as objectives, sinister recovery after, the continuity in the businesses; specific aspects such as the concept of the management of continuity of business, costs, plans and a guidance for the elaboration of a plan of business continuity it also, describes the key steps for the formulation of a Plan of Continuity of Business; and for greater illustration one appears two examples.***

INTRODUCCIÓN. La epidemia que actualmente vivimos podría prolongar y profundizar la crisis económica que atravesamos, y detener o frenar la operación de algunas empresas.

Dada la tendencia humana de ver siempre el lado positivo de las cosas, muchos empresarios tienden a no hacer caso a la necesidad de prepararse ante una situación adversa, debido principalmente a que un desastre aparenta ser un acontecimiento inverosímil, a pesar de que la experiencia y las estadísticas demuestran lo contrario.

Una de cada dos empresas tiene la experiencia de algún tipo de eventualidad o desastre, y a 35% de las empresas un suceso no previsto le ha costado entre US$100.000 y US$5 millones.

Ante un panorama mundial como el que enfrentamos hoy, desafortunadamente nos encontramos que los planes de contingencia en las empresas están fundamentalmente enfocados a proteger la información (datos) y la infraestructura central de Tecnologías de Información (TI).

A este concepto se le denomina Disaster Recovery Plan (DRP). Solo la base de estudios realizados por KPMG, solo el 23% de las empresas tiene un Plan Integral de Continuidad de Negocios. Sin embargo, esta situación en un caso como el que vivimos hoy resulta insuficiente.

CONTINUIDAD DE NEGOCIO

¿Quién Asume la Responsabilidad?

Muchos ejecutivos senior y directores empresariales consideran que la continuidad empresarial es responsabilidad del departamento de IT. Sin embargo, ya no es suficiente ni práctico que la responsabilidad recaiga en un solo grupo. La informática distribuida y la informática basada en la Web han descentralizado los procesos empresariales y los han hecho más complejos.

Es más, está en juego la reputación de la empresa, su base de clientes y, por supuesto, sus ingresos y beneficios. Por lo tanto, todos los ejecutivos, directores y empleados deben participar en el desarrollo, implantación y soporte permanente de la evaluación y planificación de la continuidad. Las mismas tecnologías de la información que impulsan la aparición de nuevas ventajas competitivas han originado nuevas expectativas y puntos débiles. En la Web, las compañías poseen el potencial de satisfacer inmediatamente las demandas de millones de personas o de no satisfacerlas.

En los entornos ERP y de cadena de suministros, las organizaciones se benefician de la mejora de la eficiencia o se ven afectadas por una interrupción de uno de los procesos integrados.

Qué es la Gestión de Continuidad de Negocios

La Gestión de la Continuidad del Negocio, llamada "Business Continuity Management" o BCM por sus siglas en inglés es el conjunto de todos los procesos y técnicas gerenciales que buscan proveer los medios para mantener una operación constante de los procesos esenciales del negocio bajo cualquier circunstancia.

En la práctica, es un conjunto de planes que asiste a la gerencia para restaurar el curso normal de los procesos, cuando se está bajo circunstancias extremas o difíciles, e incluye las habilidades que pueden ser requeridas para ejecutar esos planes. Si bien la gerencia de las organizaciones generalmente es capaz de resolver problemas operacionales de escala menor, los practicantes de la continuidad del negocio extienden esta capacidad para comprender los problemas más severos y de mayor escala.

El entorno de hoy ha desarrollado una serie de características que favorecen al cliente discriminatorio y al proveedor consciente. Más publicidad y transparencia en la operación crea un cliente capaz de discernir, y la globalización da más alternativas de proveedores. La falla en la operación puede tener consecuencias catastróficas que resulten en pérdida de clientes, pérdida de activos, o deterioro de relaciones. Muchos de estos riesgos de operación generalmente se materializan alguna vez en la vida de una organización y es necesario tener la preparación adecuada.

Costos Ocultos y Riesgos Durmientes

Es generalmente aceptado que cualquier negocio dependiente en un sistema (combinación de procesos, tecnología, organización, gente) está en riesgo cuando su operación no está disponible por un periodo de tiempo extendido o no planeado. Por otro lado, las compañías asumen que cuando su operación está disponible o en su curso normal, no están en riesgo. Sin embargo, esto no ocurre por un efecto llamado "la trampa del backlog".

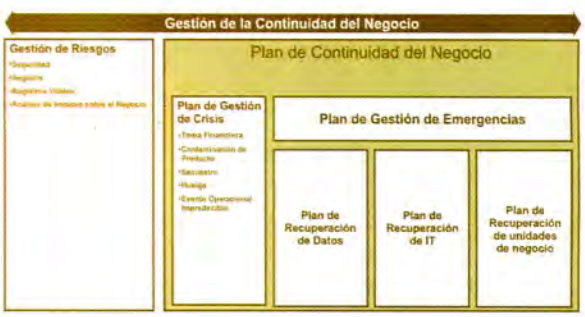
El retorno a la operación "normal" desde un estado de "sistema caído" toma al menos cinco veces el tiempo de la duración. Este cálculo está basado en información de que una persona debe incrementar su tasa de trabajo efectiva en un 25% para poder librar el *backlog:* el trabajo acumulado mientras la operación está caída.

La carga de trabajo existente y el "tiempo de respuesta" comienzan a crecer inmediatamente apenas se cae la operación; o como coloquialmente dicen, se cae el sistema. Esto ocurre porque la necesidad de negocio que atiende la organización si continúa, esta no se detiene. El *backlog* aceptable, es decir, la suma de todos los tiempos de respuesta aceptables se convierte en una constante que toca ejecutar y tiene un impacto directo en el flujo de caja y la rentabilidad del negocio.

El Plan de Continuidad de Negocios

Buenos planes de continuidad del negocios son herramientas de soporte que permiten a las personas responsables actuar efectivamente en situaciones extraordinarias. Habilitan a los gerentes para gestionar en situaciones difíciles. Asisten a los directores para dirigir cuando las probabilidades están en su contra. Soportan a los supervisores cuando los equipos, servicios, provisiones o procesos de su departamento están faltando o fallando.

Para tener una idea clara sobre qué debe ir en un Plan de Continuidad de Negocios es esencial comprender la estructura organizacional y dónde es utilizado el Plan dentro de la estructura. Diferentes personas querrán diferentes tipos de información requerida para tomar sus decisiones. También pueden requerir diferentes tipos de herramientas de decisión. Es necesario proveerles criterios y parámetros negociados para permitirles hacer juicios racionales y defendibles bajo condiciones anormales. Estas personas necesitan poder hacer esto sin referencia a una autoridad mayor u otros factores de demora.



Guía General para Elaborar un Plan de Contingencias

Análisis y valoración de riesgos. El proyecto comienza con el análisis del impacto en la organización. 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, igualmente se debe determinar el costo que representa para la organización el experimentar un desastre que afecte a la actividad empresarial.

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.

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.

Jerarquización de las aplicaciones. Es perentorio definir anticipadamente cúales 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.

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.

Ejecución. Una vez finalizado el plan, es conveniente elaborar un informe final con los resultados de su ejecución cuyas conclusiones pueden servir para mejorar este 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.

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.

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.

Difusión y mantenimiento. Cuando se disponga del plan definitivo ya probado, es necesario hacer su difusión y capacitación entre las personas encargadas de llevarlo a cargo. 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.

MATERIAL Y MÉTODOS UTILIZADOS

Material Utilizado

- Internet
- Biblioteca
- Normatividad del Estado peruano
- Libros y revistas afines

TÉCNICAS Y MÉTODOS DE TRABAJO

- Sesiones de trabajo diarias
- Discusión y prueba de la información obtenida.

Procesamiento y Análisis de Datos

Recolectados los datos acerca de las operaciones a realizar.

CONCLUSIONES

1. Un Plan de Continuidad de Negocios de una organización representa la preservación de sus principales activos para su sostenibilidad.

2. En función del tamaño de la institución u organización se tendrá que realizar un Plan de Continuidad de Negocios a través de un análisis de costo/beneficios del mismo.

RECOMENDACIONES

1. Aplicar la continuidad de negocios considerando la relación costo/beneficio.

2. Involucrar a los usuarios en la importancia de contar con un Plan de Continuidad de Negocios.

REFERENCIAS BIBLIOGRAFÍA

AGROASEMEX. (999): *Glosario de Términos.* Comisión Nacional de Seguros y Fianzas, México.

Aliber Z. R.(1983): *Riesgo de cambio y financiación en la empresa.* Edit. Pirámide, Madrid, Capítulo 2.

Alonso A.(2007): *Procedimiento para evaluar los riesgos.*

BLANCO C., B. (2007): "Aplicación del método Fuzzy Delphi a la evaluación de los riesgos empresariales de operación". Ponencia presentada al evento 45 Aniversario de los Estudios Económicos en la Universidad de la Habana", La Habana.

BODIE Z. y MERTON R. C. (1999). *Finanzas.* Prentic Hall, México.