PLAN DE CONTINGENCIAS INFORMÁTICO
Una tabla de salvación

JOHNNY A. TAMAYO ARIAS[1], ALONSO TAMAYO ALZATE[2]
[1] Doctorando Ingeniería de Proyectos
Universidad Politécnica de Catalunya. Barcelona
[2] Profesor Asociado. Departamento de Informática y Computación.
Universidad Nacional de Colombia. Sede Manizales

PC: Contingencia, sistemas de información, riesgo, desastre.

RESUMEN

El uso cada vez más creciente de las tecnologías de la información por parte de las diversas empresas y demás organizaciones también se refleja en nuestro medio, donde son más frecuentes las oficinas, empresas y entidades sistematizadas o en proceso de sistematización, lo que ha dado lugar en la mayoría de los casos a la dependencia de frágiles sistemas informáticos y redes de datos para soportar las funciones más críticas de la actividad empresarial; pero lamentablemente no existe una amplia conciencia sobre la importancia de garantizar en la misma medida, la seguridad de los recursos involucrados. Por lo general, no es un tema que se considere en forma apropiada por los directivos de las empresas, la importancia y el apoyo que se le brinda es relativamente poco o ninguno.

Es bueno tener presente que muchos de los riesgos no provienen únicamente del exterior de la empresa como los robos, fraudes, sabotaje, vandalismo, interrupción de actividades, pérdida de información, sobrecargas eléctricas, tempestades y demás desastres naturales, sino que se originan al interior del mismo centro de informática o áreas usuarias, como por ejemplo la presencia de errores, omisiones, concentración de funciones administrativas y operativas, empleados desmotivados, descuidados, mal remunerados, deshonestos, etc., lo cual ha originado un compromiso cada vez

mayor sobre la necesidad de tomar medidas para poder continuar con las actividades y procesos de la organización a pesar del advenimiento de una catástrofe. La decisión sobre estas medidas a optar tiene que seguir una serie de pasos estructurados que se deben plasmar en lo que se conoce como Plan de Contingencias.

ABSTRACT

The more and more growing use of the technologies of the information on the part of the diverse companies and other organizations is also reflected in our means, where every time they are more the offices, companies and systematized entities or in systematizing process, what has given place in most from the cases to the dependence of fragile computer systems and nets of data to support the most critical functions in the managerial activity; but regrettably a wide conscience doesn't exist about the importance of guaranteeing in the same measure, the security of the involved resources. In general, it is not a topic that it is considered in form adapted by the directive of the companies, the importance and support that he is offered it is relatively little or none.

It is good to have present that many of the risks don't only come from the exterior of the company like the robberies, frauds, sabotage, vandalism, interruption of activities, loss of information, electric flight attendants, tempests and other natural disasters, but rather they originate to the interior of the same computer science center or areas users, such us the presence of errors for example, omissions, concentration of functions administrative and operative, used desmotivados, careless, not well remunerated, immodest, etc., that which has originated a commitment every time bigger envelope the necessity to take measures to be able to continue with the activities and processes of the organization in spite of the coming of a catastrophe. The decision on these measures to opt has to follow a series of structured steps that they should be captured in what is known as Plan of Contingencies.

INTRODUCCIÓN

Desde los inicios de los sistemas de información se comprendió que las contingencias forman parte inherente de los mismos sistemas. Las amenazas a la información pueden ser de diverso origen y con el pasar del tiempo surgen diferentes formas tanto de origen natural (terremotos, tormentas, etc.), de origen humano (retaliaciones, celos profesionales, competencia, huelga, problemas laborales, entre

otros), como de origen técnico (fallas del hardware, del software, con el suministro de energía, etc.). Y es casi siempre una situación no prevista la que regularmente provoca una crisis y las consecuencias de la misma, según su impacto y extensión, pueden ser catastróficas para los intereses de cualquier organización.

Los fallos técnicos y humanos han hecho recapacitar a las organizaciones sobre la necesidad de auxiliarse en herramientas que le permitan garantizar una rápida vuelta a la normalidad ante la presencia de cualquier eventualidad, por lo tanto, el hecho de diseñar y preparar un plan de contingencias no implica un reconocimiento de la ineficiencia en la gestión de la empresa, sino todo lo contrario, los mecanismos de seguridad de la información buscan proteger a la información de las diversas amenazas a las que se ve expuesta y supone un importante avance a la hora de superar todas aquellas adversidades que pueden provocar importantes pérdidas, no solo materiales sino aquellas derivadas de la paralización del negocio durante un período más o menos prolongado. Todo esto conlleva a que la función de definir los planes a seguir en cuestión de seguridad se conviertan en una tarea realmente compleja y dispendiosa.

OBJETIVOS

- Reanudar con la mayor brevedad posible las funciones empresariales más críticas, en aras a minimizar el impacto de manera que la correcta recuperación de los sistemas y procesos quede garantizada y se conserven los objetivos estratégicos de la empresa.
- Evaluar los riesgos así como los costos de los procedimientos de contingencia requeridos cuando se presenta una interrupción de las operaciones, 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.

DEFINICIÓN

Consiste en la identificación de aquellos sistemas de información y/o recursos informáticos aplicados que son susceptibles de deterioro, violación o pérdida y que pueden ocasionar graves trastornos para el desenvolvimiento normal de la organización, con el propósito de estructurar y ejecutar aquellos procedimientos y asignar

responsabilidades que salvaguarden la información y permitan su recuperación garantizando la confidencialidad, integridad y disponibilidad de ésta en el menor tiempo posible y a unos costos razonables.

El plan de contingencia debe cubrir todos los aspectos que se van a adoptar tras una interrupción, lo que implica suministrar el servicio 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.

GUÍA GENERAL PARA ELABORAR UN PLAN DE CONTINGENCIA

Los conceptos básicos son los siguientes:

- Análisis y valoración de riesgos.
- Jerarquización de las aplicaciones.
- Establecimientos de requerimientos de recuperación.
- Ejecución.
- Pruebas.
- Documentación.
- Difusión y mantenimiento.

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 la actividad empresarial.

responsabilidades que salvaguarden la información y permitan su recuperación garantizando la confidencialidad, integridad y disponibilidad de ésta en el menor tiempo posible y a unos costos razonables.

El plan de contingencia debe cubrir todos los aspectos que se van a adoptar tras una interrupción, lo que implica suministrar el servicio 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.

GUÍA GENERAL PARA ELABORAR UN PLAN DE CONTINGENCIA

Los conceptos básicos son los siguientes:

- Análisis y valoración de riesgos.
- Jerarquización de las aplicaciones.
- Establecimientos de requerimientos de recuperación.
- Ejecución.
- Pruebas.
- Documentación.
- Difusión y mantenimiento.

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 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 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.

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 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.

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 efectuando los cambios que sean necesarios.

CONCLUSIONES

- Un Plan de Contingencia es la herramienta que cualquier empresa debe tener, para desarrollar la habilidad y los medios de sobrevivir y mantener sus operaciones, en caso de que un evento fuera de su alcance le pudiera ocasionar una interrupción parcial o total en sus funciones. Las políticas con respecto a la recuperación de desastres deben de emanar de la máxima autoridad institucional, para garantizar su difusión y estricto cumplimiento.

- Deben realizarse pruebas para determinar la eficacia del plan de contingencia y de los procedimientos de recuperación ante desastres. Las deficiencias deben resolverse y comprobarse inmediatamente. En un plan de contingencia, el objetivo consiste en ejecutar varias tareas en el menor tiempo posible. Cualquier deficiencia en la documentación, capacitación o, incluso, en los aspectos administrativos, pone en peligro la continuidad del negocio.

- La puesta en marcha de los planes a seguir es responsabilidad del encargado de la seguridad, pero también debe existir un compromiso por parte de los usuarios del sistema de información, ejecutivos y todas las personas que de alguna u otra forma ayudan a que el sistema cumpla con los requerimientos para el que fue diseñado, manteniendo sobre todo la integridad y confidencialidad de la información.

- El plan de contingencias tiene diferentes niveles de complejidad y flexibilidad según las necesidades y características de los grupos, empresas u organizaciones. Nunca se contará con los recursos suficientes para estar totalmente preparados, de ahí que el proceso deba ser paulatino e ir evolucionando según el contexto.

- El cambio es inevitable en la construcción de sistemas basados en computadoras; por ello se deben desarrollar mecanismos de evaluación, control e implementación de modificaciones al sistema, ocasionadas por nuevos requerimientos de los usuarios, por disposiciones internas de la organización y/o gubernamentales, para corregir errores, para aprovechar los nuevos avances tecnológicos, para satisfacer nuevas necesidades o para mejorar los sistemas en funcionamiento.

- Se debe tener una adecuada seguridad orientada a proteger todos los recursos informáticos desde el dato más simple hasta lo más valioso que es el talento humano, motor de desarrollo y vida de los sistemas de información; pero no se puede caer en excesos diseñando tantos controles y medidas que desvirtúen el propio sentido de la seguridad, por consiguiente, se debe hacer un análisis de costo/beneficio evaluando las consecuencias que pueda acarrear la pérdida de información y demás recursos informáticos, así como analizar los factores que afectan negativamente la productividad de la empresa.

BIBLIOGRAFÍA

ECHENIQUE, José Antonio. *Auditoría en informática.* Editorial Mc. Graw Hill. 2001

HERNÁNDEZ, HERNÁNDEZ Enrique. *Auditoría en informática.* Editorial Cecsa. 2000

PIATTINI, Mario G. *Auditoría Informática. Un enfoque práctico.* Editorial Alfaomega. 2001

www.davislogic.com/latcm/technet/

www.microsoft.com/latcm/technet/

www.lafactoriadeinternet.com

www.guia.hispavista.com/informatica/

www.hispasecurity.com

www.inei.gob.pe

www.unam.edu.

www.udec.cl/~paquezad/plan_progra.doc