Universidad Latinoamericana de Ciencia y Tecnología (ULACIT)

Facultad de Ingeniería

Escuela de Ingeniería Informática

Artículo científico presentado para optar por el grado de licenciatura en Ingeniería Informática con énfasis en gestión de recursos tecnológicos

Tema:
"Análisis de opciones de procesamiento alterno en Costa Rica"

Sustentante: Dennis M. Mora Menjívar
Cédula 1-1079-0235

Profesor Tutor: Miguel Pérez Montero

II Cuatrimestre 2006

Agradecimiento

Le agradezco primero a Dios, por haberme brindado la capacidad y actitud para efectuar este trabajo. Fue Él quien estuvo siempre ahí conmigo, guiándome por el buen camino, para poder alcanzar el éxito.

A mi familia por haberme dado el apoyo necesario para llevar a cabo esta investigación, ya que sin ellos todo hubiera sido mucho más difícil.

Agradezco a todos mis profesores, ya que, sin saberlo, fueron instrumento utilizado por Dios, por haberme enseñado durante diferentes épocas de mi vida, que fueron importantes en mi desarrollo integral tanto en la carrera como la vida misma.

Tabla de Contenido

Resumen Ejecutivo

En las últimas décadas, se ha generado una revolución tecnológica y científica como nunca la humanidad había vivido y todavía hay suficientes resultados en los laboratorios de investigación para asegurar que habrá nuevos productos en cantidades semejantes al pasado reciente.

Muchos autores entienden por tecnologías de información (TI), aquellas que utilizan en sus actividades dispositivos de cómputo y telecomunicaciones. Es una definición muy amplia pero así también es el ámbito que los equipos electrónicos digitales modernos impactan.

Por lo anterior y a fin de lograr que el desarrollo tecnológico sea homogéneo y racional, pero a la vez rico en posibilidades, se facilita la interconexión entre equipos y sistemas a través de la red global de comunicaciones, que garantice su máximo tiempo de vida y se evite la obsolescencia prematura de la tecnología.

Esto a su vez produce la necesidad de las organizaciones de brindar un servicio continuo que les garantice un 99,999 % de disponibilidad, en donde su infraestructura tecnológica tenga la capacidad de soportar cualquier eventualidad, sin necesidad de dejar sus operaciones diarias.

El presente documento ha sido desarrollado con el objetivo de indagar sobre las opciones que ostentan las empresas en cuanto al procesamiento alterno de información en Costa Rica, en donde se identifican las etapas del proceso de planeación de la continuidad del negocio, el desarrollo de procedimientos alternos de trabajo y los procedimientos de recuperación y recomendaciones.

Abstract

In the last decades, a technological and scientific revolution has taken place as never before and there are still enough results in the investigation laboratories to secure that there will be new products in quantities similar to the recent past.

Many authors understand as information technologies (IT), those that use in their activities computer devices and telecommunications. It is a very wide definition but, likewise, it is the environment that impacts the modern digital electronic equipments.

For the above-mentioned and in order to achieve a homogeneous and rational technological development, rich in possibilities at the same time, the interconnection is facilitated between equipments and systems through the global net of communications that guarantees its maximum life time and avoid the premature outdate of the technology.

This, at the same time, produces the necessity of the organizations to offer a continuous service that guarantees them 99,999% of readiness where their technological infrastructure has the capacity to carry out any eventuality, without leaving its daily operations.

The present document has been developed with the purpose of investigating the options the companies show as for the alternating information prosecution in Costa Rica, where are identified the planning process stages of the business continuity, the development of alternating procedures of work and the recovery procedures and recommendations.

Introducción

Durante las últimas décadas hemos sido testigos y partícipes de lo que se ha denominado la revolución tecnológica en torno a la comunicación, basada en los dramáticos avances en tecnología de la información (T.I.). Los adelantos en las capacidades de cómputo y procesamiento de datos han cambiado las reglas del juego en los negocios, esto permite, entre otras cosas, crear múltiples y novedosas formas de relacionar a los clientes con los proveedores, mejorar el proceso de toma de decisiones, con información veraz y oportuna, desarrollar nuevas estructuras y bases de competitividad en varias industrias y apoyar la gerencia del conocimiento.

Resulta, entonces, natural y razonable, el interés que hoy manifiestan diversos tipos de empresas en tecnologías relacionadas con el uso y transmisión de información, y el aumento en las inversiones que realizan en Tecnologías de Información. Por otra parte, esta revolución tecnológica ha servido también de catalizador al proceso de globalización. El nacimiento de la red mundial de información, Internet, y su acelerada y constante evolución, se ha convertido quizás en la expresión más genuina y tangible de tal afirmación.

La información en los negocios, el procesamiento, la distribución y la transmisión de la información resultan ser, en la actualidad, actividades críticas para los negocios. De allí la importancia que adquiere la disponibilidad de una plataforma tecnológica orientada a procesar y transmitir la información corporativa, llevando a pensar en conceptos tales como alta disponibilidad, redundancia, continuidad operativa o sistemas de respaldo.

Acontecimientos desafortunados e impredecibles, tales como los ocurridos el 11 de Septiembre del 2001 en los Estados Unidos de Norteamérica, constituyeron

una prueba extrema para muchas empresas en este sentido. Por ello se ha concienciado a un creciente número de compañías y organizaciones sobre el impacto que pueden tener "eventos" de naturaleza imprevista sobre la continuidad operativa e inclusive la supervivencia de una organización, al ser afectada su plataforma de Tecnologías de Información.

En tal sentido, algunas empresas se han volcado a servir a este creciente mercado, preocupado por la continuidad y la supervivencia de los negocios, ofreciendo la "tercerización" de infraestructura y plataformas tecnológicas del tipo de procesamiento alterno (Centros de Datos), con lo cual permiten a los clientes concentrarse en sus actividades medulares en diferentes lugares geográficos, a este y muchos elementos más se le conoce como planeación.

¿Qué es la planeación?

La planeación tiene muchos y variados enfoques; sin embargo, su común denominador sería, “Es el arte de diseñar un entorno, con el objetivo de lograr el eficaz desempeño de cada una de las personas que forman parte de un área específica y así contribuir con el buen funcionamiento de toda organización, donde la tarea más importante es comprobar que todas las personas involucradas conozcan cuáles son los propósitos, los objetivos del grupo y los métodos para lograrlos.” (García, 1999,Pág.24)

¿Qué es un plan de continuidad?

Al igual como lo vimos anteriormente la planeación es diseñar un entorno con un objetivo en especifico para esto se necesitan acciones que brinden el aseguramiento de éste tales como un plan de continuidad.

El plan de continuidad es una estrategia constituida por un conjunto de recursos ideados con el propósito de servir de respaldo, cuenta con una organización de emergencia y con procedimientos de actuación, encaminados a conseguir una restauración progresiva y ágil de los servicios de negocio, efectuados por una paralización total o parcial de la capacidad operativa de la empresa. Sin embargo muchos escritores catalogan un plan de continuidad como "El propósito del plan, es proveer orientación para reducir el tiempo y agilizar la toma de decisiones, durante las operaciones que se efectúan en el restablecimiento de los servicios, también, resumir rápidamente los servicios críticos y facilitar el restablecimiento de los servicios normales en el menor tiempo posible, y 'relativamente' a un bajo costo financiero." (García, 1999, Pág.26)

Tal estrategia, puntualizada en un manual, es resultado de todo un proceso de análisis y definiciones que dan lugar a las metodologías. A su vez, las metodologías existentes versan sobre el proceso necesario para obtener dicho plan.

Es muy importante tener en cuenta que el concepto a considerar es “la continuidad en el negocio”. Estudiar todo lo que pueda en un momento dado paralizar la actividad y producir pérdidas. Todo lo que no considere estos criterios no podrá ser nunca un plan de continuidad.

Continuidad del negocio

Proteger la infraestructura de tecnología de información es un objetivo de máxima prioridad. Interrumpe, destruye, o apaga las redes de información, para ver cómo desconecta un área geográfica, es algo que ya se ha vivido, se ha sentido, se ha experimentado, como lo detallan expertos en ésta materia en donde dicen: “La tecnología de información impregna todos los aspectos de nuestra vida diaria, de nuestra nación: el envío de bienes, las telecomunicaciones, los servicios de

emergencia, la entrega de electricidad y agua a nuestros hogares. Todos los aspectos de nuestra vida dependen de una infraestructura cada vez más compleja y crítica.” (Yamile, 2006)

Es necesario prevenir las interrupciones, y cuando ellas ocurran, asegurar que sean cortas, infrecuentes, y controlables. Muy pocas empresas evalúan el costo de reanudar el negocio, la pérdida de tiempo y dinero, ante eventuales hechos que afecten la información y los equipos.

Después de los ataques del 11 de septiembre, se planteó un nuevo problema sobre la recuperación de desastres y la continuidad del negocio, frente a catástrofes naturales o atentados terroristas de grandes magnitudes. Se presentan dos situaciones en cuanto a los costos en que incurre una compañía ante un desastre: la primera, cuando la empresa sobrevive, gracias a sus planes de continuidad con el empleo que le dio a la información y centros de cómputo y otra, cuando la destrucción de los equipos la lleva a la quiebra.

Las organizaciones ven en la planificación de los sistemas informáticos una necesidad, pues deben prever situaciones inesperadas, para proteger los negocios. Deben establecer e identificar los recursos de las áreas críticas y expuestas a cualquier alteración. Lo principal es hacer un plan de recuperación que tenga éxito, para que la compañía continúe funcionando sin contratiempos, en el menor tiempo posible.

Las empresas que utilizan tecnologías de información deben entender que la continuidad del negocio después de un desastre es vital para la compañía, en cuanto a los costos que se generan, debido a los tiempos de caída de los sistemas, pérdida de clientes y la credibilidad de la empresa.

Un buen plan de continuidad debe incluir la réplica o copia de todos sus datos (protección de la información) y el establecimiento de un lugar donde ubicarse, en caso de que las instalaciones de la compañía queden dañadas (centros de procesamiento alterno).

¿Cómo enfrentar el aseguramiento en la continuidad del negocio?

En los últimos años, los negocios que no pueden parar y deben estar disponibles las 24 horas, durante los siete días de la semana, se han convertido en un común denominador en la industria. Está relacionado con la prestación de servicio continuo.

Volviendo al ejemplo que ha venido comentado, luego de la catástrofe descrita en los Estados Unidos y hasta en los países latinoamericanos, en constante situación de zozobra e inseguridad, las áreas de informática han sido cuestionadas por los directivos y administradores de las compañías y se ha puesto en duda la capacidad para garantizar que la organización sobreviva ante cualquier desastre.

Esto pareciera ser un 'pellizco' temporal, si se mira la historia de los procesos utilizados en la implantación de soluciones. Los gerentes han sido siempre escépticos con relación a la necesidad de invertir en la infraestructura que asegure la continuidad del negocio. Es más cómodo pensar que "lo malo le ocurre al vecino, pero a mí no". Bajo este punto de vista montar una solución de tales características, continúa mirándose como un lujo o un desperdicio.

Ya existen muchas compañías de seguros que han incluido en sus pólizas descuentos del 5% al 15%, para aquellas compañías que demuestren acciones adecuadas dirigidas a proteger los activos que generan la información.(ACIS, 2006).

El punto es cuestionar el nivel de preparación que tienen las empresas para afrontar eventualidades realmente complejas que hagan tambalear el negocio.

Los desastres son eventualidades suscitadas que ocasionan interrupciones en los recursos críticos de información produciendo inoperancia por un periodo, que impacte adversamente las operaciones del negocio, el cual podría ser desde varias horas hasta varios días, dependiendo de la criticidad del recurso de información.

Más importante aún, los desastres requieren tomar acciones para recuperar su estado operativo, que en el peor de los casos, conllevaría al uso de una instalación alterna de procesamiento, donde se podría requerir la restauración del software y de los archivos de datos provenientes de copias almacenadas o protegidas en otros sitios. Es necesario que el centro alterno esté disponible hasta que la instalación de procesamiento de información original se restablezca.

Un desastre puede ser causado por calamidades naturales, como por ejemplo terremotos, inundaciones, tornados, tormentas eléctricas severas, incendios y otros, que causan daños extensos a la instalación de procesamiento y a la localidad en general. Otros eventos desastrosos que causen interrupciones pueden ocurrir cuando los servicios esperados ya no son suministrados a la compañía, como por ejemplo, el suministro de energía eléctrica, las telecomunicaciones, el suministro de gas natural u otros servicios suministrados por externos, donde un desastre puede ser causado por eventos de índole humana como ataques terroristas, *"hackers"*, huelgas y otros.

En estos casos, pueden requerir que se tomen acciones para recuperar el estado operativo a fin de reanudar el servicio. Para esto se necesita un buen plan de continuidad del negocio, que tomará en cuenta todos los tipos de acontecimientos

que impacten tanto las instalaciones de procesamiento de los sistemas de información críticos como las funciones normales de operación del negocio.

¿Qué es la planeación de continuidad del negocio?

El proceso de planeación de la continuidad del negocio puede dividirse en las etapas siguientes:

- Análisis de riesgo
- Análisis del impacto sobre el negocio
- Desarrollar estrategias de recuperación del negocio
- Desarrollar un plan detallado
- Implementar un plan
- Probar y mantener el plan

Análisis de riesgo

En esta etapa se evalúan los perjuicios financieros, técnicos, jurídicos y operativos totales, que pudieran ocurrir como resultado de la continuidad. El riesgo abarcaría perjuicios potenciales a los clientes y organizaciones. También se deben analizar amenazas a la seguridad y los perjuicios que potencialmente podrían ocasionar a varios departamentos y operaciones. El software de administración de riesgos a la seguridad, puede ayudar al personal de tecnología de información a evaluar el impacto de las amenazas a la seguridad de la entidad.

Análisis del impacto sobre el negocio

En esta etapa se deben identificar los diversos eventos que podrían impactar sobre la continuidad de las operaciones y su impacto sobre la organización. Para afrontar esta con éxito se debe lograr un entendimiento de la organización, de los procesos clave del negocio y de los recursos del área de tecnología de

información usados por la organización para soportar los procesos clave. En esta etapa se debe determinar la criticidad de los recursos de información (aplicaciones, datos, redes, software de sistema, instalaciones o centros de procesamiento), que brindan soporte a los procesos críticos.

Para efectuar un análisis del impacto, se utilizan varios métodos, el más utilizado es el cuestionario. Esto implica desarrollar un cuestionario detallado y circularlo a los usuarios clave y la información recopilada es tabulada y analizada.

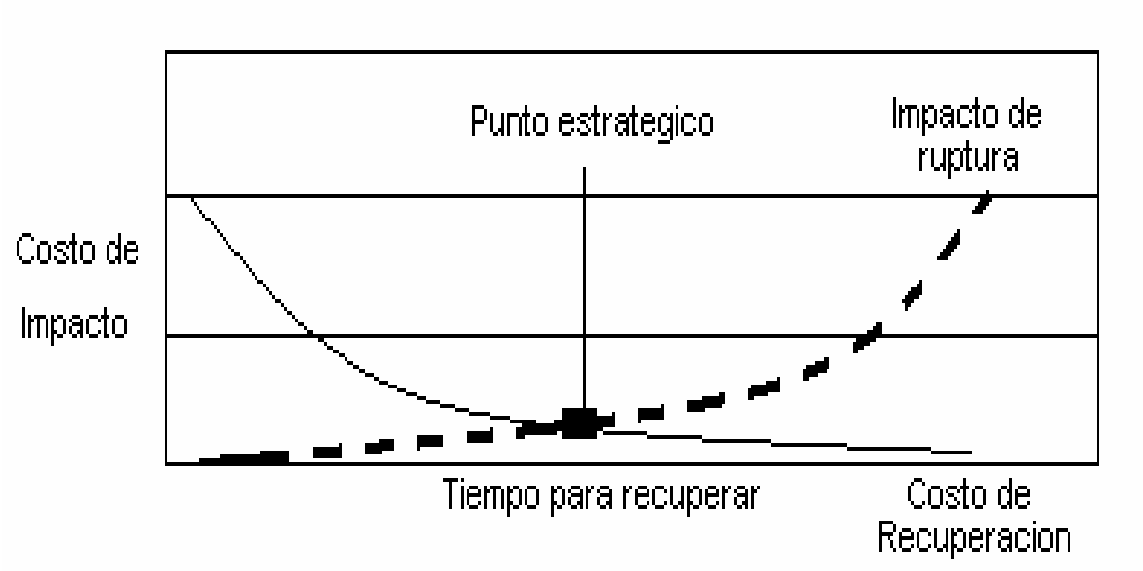
Dentro de las diversas preguntas que se deben considerar se incluyen las siguientes:

1. ¿Cuáles son los recursos de información relacionados con los procesos críticos del negocio de una organización?

2. ¿Cuál es el periodo de recuperación crítico para los recursos de información, en el cual se debe restablecer el procesamiento del negocio antes de que se experimenten pérdidas significativas o inaceptables? Como se muestra en la Figura 1

3. ¿Cuál es la clasificación de los sistemas considerando los riesgos?

Figura 1
Impacto de la interrupción vs. Costo de recuperación



Fuente: ISACA, 2004

Clasificación de los sistemas

Los sistemas se pueden clasificar de muchas formas, una de ellas se efectúa por categorías tales como:

- *Crítico:* estas funciones no pueden realizarse a menos que sean reemplazadas por capacidades idénticas. Las aplicaciones críticas no pueden ser reemplazadas por métodos manuales. La tolerancia a la interrupción es muy baja, por lo tanto, el costo de interrupción es muy alto.

- *Vital:* estas funciones pueden realizarse manualmente pero solo por un periodo. Hay mayor tolerancia a la interrupción que con los sistemas críticos, por lo tanto, los costos de interrupción son un poco más bajos, considerando que las funciones son restauradas dentro de un marco de tiempo determinado.

- *Sensitivo:* estas funciones se pueden realizar manualmente, a un costo tolerable y por un periodo. Aún cuando se pueden realizar manualmente, por lo general, es un proceso difícil y requiere de personal adicional para llevarlas a cabo.

- *No crítico:* estas funciones pueden ser interrumpidas por un periodo prolongado, a un costo muy pequeño o nulo para la compañía y requiere de poco o ningún esfuerzo para ponerse al día cuando son restauradas.

Desarrollo de estrategias de recuperación

Una estrategia de recuperación identifica la mejor forma de reestablecer un sistema en caso de desastre y provee orientación basada en qué procedimientos detallados de recuperación se pueden desarrollar. La alta gerencia debe seleccionar la estrategia más apropiada de las alternativas ofrecidas, la cual debe ser usada para desarrollar el plan detallado de continuidad del negocio.

La selección de una estrategia de recuperación dependerá de la criticidad del proceso del negocio y las aplicaciones que soportan los procesos:

- Costo
- Tiempo requerido para recuperarse
- Seguridad

La estrategia apropiada es aquella con un costo para un tiempo aceptable de recuperación que también es razonable con el impacto y probabilidad de ocurrencia que se determinó en el análisis de impacto sobre el negocio.

Se debe seleccionar la alternativa más apropiada en términos de velocidad de recuperación y de costos de recuperación, basado en el nivel relativo identificado en el análisis de impacto sobre el negocio.

Alternativas de recuperación

Las interrupciones más prolongadas y más costosas, en particular los desastres que afectan la instalación física primaria, requieren alternativas de recuperación en un sitio distinto a la ubicación primaria (*Offsite*). Los tipos de instalaciones de respaldo de hardware *Offsite* que existen son (ISACA, 2004):

- *Hot sites:* se configuran totalmente y están listos para operar en varias horas. El equipo y software del sistema deben ser compatibles con la instalación primaria que está siendo respaldada.

  Los costos asociados con el uso de un *hot site* de terceros, por lo general, son elevados, pero con frecuencia son costos justificables para las aplicaciones críticas. Cuando se planea apropiadamente, la cobertura de seguro por lo general compensará los costos incurridos por usar este tipo de instalación.

  Los costos incluyen un cargo básico de suscripción, una cuota mensual, costos de activación cuando el sito es usado para una emergencia real y cargos por uso por hora o por día. Las estructuras de precios varían entre proveedores. Algunos proveedores de *"hot site"* imponen un derecho elevado de activación para desalentar el uso innecesario de la instalación.

  El *"hot site"* está destinado para operaciones de emergencia durante un periodo limitado y de uso no prolongado. El uso prolongado afectaría la protección de otros suscriptores. Por lo tanto, el *"hot site"* deber ser considerado como un medio para lograr la continuación de operaciones esenciales, por un período de hasta varias semanas una vez que ha ocurrido un desastre o emergencia mayor. Planes adicionales son necesarios para atender las operaciones posteriores.

- *Warm sites:* están parcialmente configurados, por lo general con conexiones de red y equipo periférico seleccionado, como por ejemplo unidades de disco, unidades de cinta y controladores, pero sin la computadora principal. A veces un *"warm site"* está equipado con una CPU menos potente que la que se usa generalmente. El supuesto detrás del concepto de *"warm site"* es que la computadora puede, por lo general, obtenerse rápidamente para una instalación de emergencia y como la computadora es la unidad más cara, dicho arreglo es menos costoso que un *"hot site".*

  Después de la instalación de los componentes que se necesitan, el sitio puede estar listo para el servicio dentro de horas; sin embargo, la ubicación y la instalación de la CPU y de otras unidades faltantes podrían tomar varios días o semanas.

- *Cold sites:* tienen sólo el ambiente básico (cableado eléctrico, aire acondicionado, piso), para operar una instalación de procesamiento de información. El "*cold site*" está listo para recibir equipo, pero no ofrece ningún componente en el lugar antes que se requiera su uso. La activación del lugar puede llevar varias semanas.

- Instalaciones duplicadas de procesamiento: son lugares de recuperación dedicados, desarrollados por la empresa que se prepara para la interrupción, que pueden respaldar las aplicaciones críticas. Pueden variar desde un "*hot site"* en espera hasta un contrato recíproco para el uso de la instalación de otra compañía.
- Acuerdos recíprocos: se pueden presentar entre dos o más organizaciones con equipos o aplicaciones similares. Bajo el acuerdo típico, los participantes

prometen proveerse mutuamente tiempo de computadora cuando surja una emergencia.

Desarrollando un plan detallado

Basado en la estrategia de recuperación seleccionada por la gerencia, se debe desarrollar un plan detallado de recuperación de desastres. Se deben resolver todos los problemas implicados en la recuperación de un desastre.

Los diversos factores que se deben considerar mientras se desarrolla el plan son:

- Estar preparado antes de un desastre
- Procedimientos de evacuación
- Cómo declarar un desastre
- La identificación de los procesos del negocio y los recursos que se deben recuperar
- La clara identificación de las responsabilidades en el plan
- La clara identificación de las personas responsables de cada función en el plan
- La explicación, paso por paso, de la opción de recuperación

El plan debe estar documentado y escrito en un lenguaje sencillo, comprensible para todos. Es común identificar los equipos de personal que son responsables de tareas específicas en caso de desastre.

Dicho plan debe contener los equipos, con sus responsabilidades asignadas, en el caso de un desastre. Para implantar estrategias que se han desarrollado para la recuperación del negocio, se debe identificar el personal de toma de decisiones. Estas personas, por lo general, lideran equipos creados en respuesta a una función crítica o tarea definida en el plan. Los equipos pueden ser:

- Acción de emergencia.
- Evaluación de daños.
- Administrador de la emergencia.
- Seguridad
- Operaciones de emergencia.
- Comunicaciones.
- Soporte administrativo

Evaluación de sitios geográficos

Con respecto a la geografía de Costa Rica, algunos sectores han sufrido daños importantes en tiempos históricos como consecuencia de desastres naturales (terremotos, inundaciones entre otros). Debido a esto, organizaciones como la Comisión de Nacional de Emergencia (CNE), en conjunto con el Observatorio Vulcanológico y Sismológico de Costa Rica (OVSICORI), han efectuado estudios y, con ello, han determinado ciertos lugares seguros para la construcción de un centro alterno del procesamiento. Entre estos lugares están: (Comisión Nacional de Emergencias, 2001)

- Padaure: ubicada en San Antonio de Belén, el cual presenta un bajo nivel de microsismicidad para la zona oeste del Valle Central, y no existen fallas superficiales activas en un radio de 7 y 10 kilómetros a la redonda.
- Birrí de Heredia: presenta dos alternativas localizadas muy cerca una de la otra, las cuales no tienen actividad sísmica, ni existen fallas activas alrededor de unos 7 a 9 kilómetros y por ende se puede recomendar dicha localidad.
- San José de la Montaña: se encuentra a unos 6 Km. al este de los sitios ubicados cerca de Birrí de Heredia.
- Concepción de San Isidro de Heredia: ubicada en la provincia de Heredia en el cantón de San Isidro.

- Aserrí: ubicada en la provincia de San José, a unos 21 Km. de la capital.
- San Isidro de Coronado: ubicada en la provincia de San José.

Como se muestra en las figuras número 2 y 3, de la sección de anexos.

El papel de los seguros en un plan de continuidad del negocio

El plan de continuidad del negocio debe contener información clave de los seguros de la organización. La política de tener seguros para los equipos de procesamiento de los sistemas de información, que por lo general, es de riesgos múltiples, diseñado para proveer diversos tipos de cobertura de los sistemas.
Los tipos específicos de cobertura disponible son:

- Equipo e instalaciones de tecnología de información: provee cobertura de daños físicos al sitio de procesamiento de información y al equipo de su propiedad.
- Reconstrucción del software: cubre daños a los medios del sistema que sean propiedad del asegurado y del cual el asegurado sea responsable.
- Gastos adicionales: están diseñados para cubrir los costos adicionales que ocasionan la continuidad de las operaciones luego de los daños o de la destrucción en el sitio de procesamiento de información.
- Interrupción del negocio: cubre la pérdida de las ganancias debido a la interrupción de la actividad de la compañía, por causa de algún mal funcionamiento de los sistemas de la organización.
- Cobertura de fidelidad: adquiere la forma de fianzas generales o colectivas. Cubre pérdidas originadas por actos deshonestos o fraudulentos de los empleados. Esta es la que prevalece en las instituciones financieras que operan su propio centro de procesamiento.

Prueba del plan de continuidad y recuperación

La mayoría de las pruebas de la continuidad del negocio no llegan a una totalidad de las porciones operativas de la organización. Esto no debe excluir la realización de pruebas totales o parciales, porque uno de los fines de la prueba de continuidad es determinar si el plan funciona bien o qué partes del plan necesitan ser mejoradas.

La prueba debe ocuparse de todos los componentes críticos y simular las condiciones reales de procesamiento en el periodo más activo, aun si se lleva a cabo fuera de horas laborales. Una buena prueba debe cumplir las siguientes tareas:

- Verificar si el plan de continuidad del negocio es completo y preciso.
- Evaluar el desempeño del personal involucrado en el ejercicio.
- Evaluar el entrenamiento y el conocimiento de los miembros del equipo de continuidad.
- Medir la habilidad y capacidad del lugar de respaldo para llevar a cabo el procesamiento prescrito.
- Evaluar la capacidad de recuperación de los registros vitales.
- Medir el desempeño general de actividades operativas y de procesamiento de los sistemas de información relacionadas con el mantenimiento de la entidad de negocio.

Durante cada etapa de la prueba, se debe emplear documentación detallada de las observaciones, problemas y soluciones. Esta documentación sirve como información histórica importante que puede facilitar la recuperación real durante un desastre real. También, la documentación ayuda a efectuar un análisis detallado, tanto de las fortalezas como de las debilidades del plan.

La responsabilidad de mantener el plan de continuidad del negocio, a menudo recae en el coordinador del plan. Sus responsabilidades específicas incluyen:

- Desarrollar un programa para revisión y mantenimiento periódico del plan, informando a todo el personal.
- Examinar las revisiones, comentarios y actualizar el plan dentro de los 30 días siguientes a partir de la fecha de revisión.
- Hacer arreglos y coordinar las pruebas programadas y no programadas del plan para evaluar si son adecuadas.
- Mantener registros de las actividades de mantenimiento del plan de negocio.

Impedimentos para el éxito

La planeación de la continuidad en su mayoría será sujeta de circunstancias que harán que ésta posea obstáculos entre ellas están:

- El impacto financiero o las implicaciones legales, son subestimadas y, lo que es peor, son desconocidas por la gerencia.(ACIS, 2006)
- La mayor parte de los procesos de negocios son de misión crítica o muy integrados con otras funciones, de modo que cuando algo va mal, el impacto se expande. El riesgo es ignorado hasta que algo ocurra.
- La infraestructura existente puede no soportar los niveles de disponibilidad demandante y las necesidades de continuidad de la compañía.
- La falta de conocimiento para definir una correcta estrategia de continuidad de negocio hace más complicado el proyecto. Cuando las opciones internas se mezclan con otras soluciones en la modalidad de "*outsourcing*", el control del proceso de T.I., está en manos de terceros.

- Hoy, las infraestructuras del negocio están más interrelacionadas y hacen que la ocurrencia de un problema de continuidad tenga un impacto en cadena e incremente los niveles de vulnerabilidad.
- Afirmar que “esto no puede pasar” o “le puede ocurrir a la competencia, pero a mí no”, se graba en el ambiente e impide asumirlo como un proyecto real. En esas condiciones es muy difícil divulgarlo en la organización.

Costos de un centro de procesamiento alterno

En las empresas que brindan estos servicios, los costos incluyen una suscripción básica, una cuota mensual, costos de activación cuando el sitio es usado para una emergencia real y cargos por uso por hora o día. Las estructuras de precios varían entre los proveedores, algunos proveedores imponen un derecho elevado de activación para desalentar el uso innecesario de la instalación; otros no cobran derecho de activación y estimulan el uso de la facilidad para fines que no son desastre, por ejemplo, el procesamiento cuando el sitio primario está sobrecargado.

A continuación se desglosan los diferentes tipos de costos para la adquisición de un centro de procesamiento alterno.

- Deposito de garantía: éste se puede considerar como el costo de arrendamiento de un espacio físico en el edificio de la compañía, su valor es de $5,000.00 (cinco mil dólares), es una sola cuota, y la entidad lo puede retirar cuando se termine el lazo comercial o finalice el contrato respectivo.
- Bóveda digital: es un cuarto especializado en donde nada más se guarda información (respaldos), la cual está custodiada y bajo condiciones óptimas para dicha información. El costo de la misma está entre $100.00 (cien dólares) y $500.00 (quinientos dólares) mensuales, lo que depende del espacio físico.

- *Cold site*: este cuenta con un ambiente básico que proporciona aire acondicionado, piso, puertas de seguridad y cableado eléctrico; es un espacio físico que se encuentra listo para recibir equipo. Sus costos oscilan entre $1000.00 (mil dólares) y $ 1500.00 (mil quinientos dólares) mensuales.
- *Warm site*: esta solución cuenta con el ambiente básico (aire acondicionado, piso, puertas de seguridad, cableado eléctrico). Además cuenta con servidores de prueba y otros tipos de componentes tales como conexiones de red, unidades de disco y cintas; sus precios se encuentran entre $3000.00 (tres mil dólares) y $4000.00 (cuatro mil dólares) mensuales.
- *Hot site*: ésta opción cuenta con el ambiente básico. Además se tienen otros componentes tales como cableado estructurado, planta eléctrica, UPS, estaciones de trabajo y unidades de disco; sus precios se encuentran desde $5000.00 (cinco mil dólares) en adelante, según los “extras” que requiere el centro alterno.

Algunas entidades financieras cuentan con su propio centro de procesamiento alterno, el cual se encuentra en otro edificio de la organización desplazado geográficamente, dedicado a reemplazar al equipo principal, en caso de una anomalía y brindar la continuidad del negocio; para muchas instituciones, este tipo de adquisición es de un costo muy elevado, ya que tienen que contar con el equipo óptimo que respalde las aplicaciones críticas, y brindar el recurso humano adecuado, donde en promedio el costo de adquisición de un centro alterno, varía de acuerdo a la cantidad transaccional que efectúe la entidad y el entorno financiero que la rodea. Similar a un porcentaje estimado de la inversión actual del equipo según la criticidad del negocio (ACIS,2006).

Conclusiones

A fin de asegurar la continuidad de los servicios, las organizaciones que dependan de sistemas informáticos, deben elaborar el respectivo plan para minimizar el efecto de las interrupciones, tanto internas como externas que se pueden presentar. Este plan debe estar basado en el plan estratégico de tecnología de información y debe cumplir con la estrategia de la institución, basado en normativas o procedimientos establecidos por un ente dedicado a la prevención de desastres, tal como la Comisión Nacional de Emergencia, Bomberos de Costa Rica o la Cruz Roja Costarricense; por lo tanto, el proceso de desarrollar y mantener un buen plan de continuidad ante un desastre le concierne a todo el personal de la institución.

La entidad debe efectuar, inicialmente, un análisis de riesgo exhaustivo, en el que se identifiquen, clasifiquen y evalúen la totalidad de riesgos inherentes, tanto internos como externos de la misma y el entorno que la rodea, con el fin de mitigar el impacto sobre el negocio ante cualquier situación anómala que perjudique los intereses de la institución, con el fin de escoger la estrategia más apropiada para recuperar, por lo menos, los sistemas más críticos o indispensables y que éstos puedan funcionar hasta que estén disponibles todas las instalaciones del sistema principal, sin afectar la continuidad del negocio.

La implantación del plan ayudará a minimizar los costos y gastos operativos en los que incurren las instituciones, cuando se presenta un desastre, con esto se logra la continuidad de las labores fundamentales de la organización.

Se concluye que en todas las organizaciones independientemente de su actividad, se establece que su razón de ser es el cliente, y si le brindan un servicio continuo y sin interrupciones, éste estará identificado con dicha organización.

Se deben evaluar los planes de continuidad del negocio para determinar si son adecuados y si están actualizados con los estándares apropiados o con las reglamentaciones de la entidad reguladora. Usualmente las organizaciones no efectúan revisiones periódicas de su plan de continuidad. Esto puede acarrear riesgos, los planes se pueden desactualizar muy fácilmente y con ello incrementar el riesgo operativo de la organización. Además, las organizaciones no cuentan con la supervisión o asesoramiento propio de un ente especializado para evaluación o revisión de su plan de continuidad, y con esto se incrementa la probabilidad de materialización de los riesgos que pueden sufrir las instituciones.

Los planes de continuidad deben ser efectivos para asegurar que las capacidades de procesamiento de la información puedan ser reanudadas prontamente, después de una interrupción imprevista, brindando la continuidad del negocio.

Dado los alcances o rangos de destrucción de los fenómenos naturales lo ideal sería que el centro alterno esté a una distancia promedio del edificio que albergue el centro de cómputo principal de la entidad para brindar un buen desempeño del centro alterno, pero debido a la geografía del país, esto es casi imposible de realizar, ya que un 60% del entorno socio-económico se sitúa en el valle central y con esto aumenta el riesgo y la vulnerabilidad de toda organización.

Recomendaciones

A la hora de elaborar el plan estratégico del área de tecnología de información, se deben tomar en consideración los aspectos más relevantes, que permitan brindar el aseguramiento de la continuidad del negocio. Uno de esos aspectos es la implantación de un plan de continuidad, el cual debe contener:

- Análisis de riesgos
- Análisis del impacto del riesgo
- Desarrollar estrategias de recuperación
- Desarrollar un plan detallado
- Implantar un plan
- Probar el plan
- Mantener un plan

Si se siguen estos pasos concientemente, se puede asegurar un alto porcentaje de probabilidad de que el plan de continuidad sea efectivo, para con esto, brindar confianza y seguridad a la institución a la hora de efectuar las labores cotidianas.

La institución que elabore un plan de continuidad, debe formar un comité o grupo encargado de velar por la revisión, evaluación y actualización del mismo. Este grupo, a su vez, debe buscar asesoría por parte de un ente especializado en desastres (naturales, humanos o tecnológicos), tal como la Comisión Nacional de Emergencia, Bomberos de Costa Rica o la Cruz Roja Costarricense, que brinden el apoyo necesario para la buena implantación del plan de continuidad.

Se debe brindar un buen programa de capacitación para todo el personal de la organización, desde la alta gerencia hasta el empleado de menor cargo, brindándole las herramientas necesarias para que se pueda desempeñar de la

mejor manera en caso de imprevistos, y se debe hacer conciencia y crear un compromiso serio hacia la organización para brindar unión y solidez, si ocurre un evento anómalo.

Es importante resaltar que se debe contar con una bitácora de pruebas, la cual, al menos, debe especificar lo siguiente:

- Tipo de prueba
- Hora
- Fecha
- Objetivos
- Limitaciones
- Alcances
- Resultados
- Responsables

Estos aspectos determinarán el mejoramiento del plan de continuidad y las pruebas que se deben ejecutar deben ser muy rigurosas para observar la calidad y la cantidad que pueden soportar las aplicaciones o componentes ante un desastre.

A la hora de contratar los servicios externos de un centro de procesamiento alterno, se debe asegurar que este es adecuado, inspeccionando la instalación y revisando su contenido, la seguridad, los controles ambientales y todo lo estipulado según lo establecido en el contrato firmado con la empresa proveedora del servicio.

Se recomienda efectuar diferentes tipos de estudios tales como factibilidad, costos, requerimientos, geográficos y otros a la hora de construir o implantar un centro de procesamiento alterno. Se debe buscar asesoría de organizaciones

dedicadas a este tipo de proyectos, ya que de esto dependerá la mejor decisión de implantación.

No se recomienda que el centro de procesamiento alterno esté a una distancia inferior a los 50 km, ya que en caso de un eventual desastre y dependiendo del tipo de desastre no se aplicaría el propósito de dicho centro, lo que ocasionaría más bién pérdidas para la organización.

Bibliografía

Asociación Colombiana e Ingenieros en Sistemas, ACIS.(2006). Artículos investigaciones . Recuperado el 20 de mayo de 2006, de: http://www.acis.org.co/Paginas/publicaciones/investigaciones83.html

Comisión Nacional de Emergencias.(2006). Documentación. Recuperado el 10 de junio de 2006, de : http://www.cne.go.cr

Information Systems Audit and Control Association.(2004).Manual de preparación para el exámen CISA.Pág.(335)

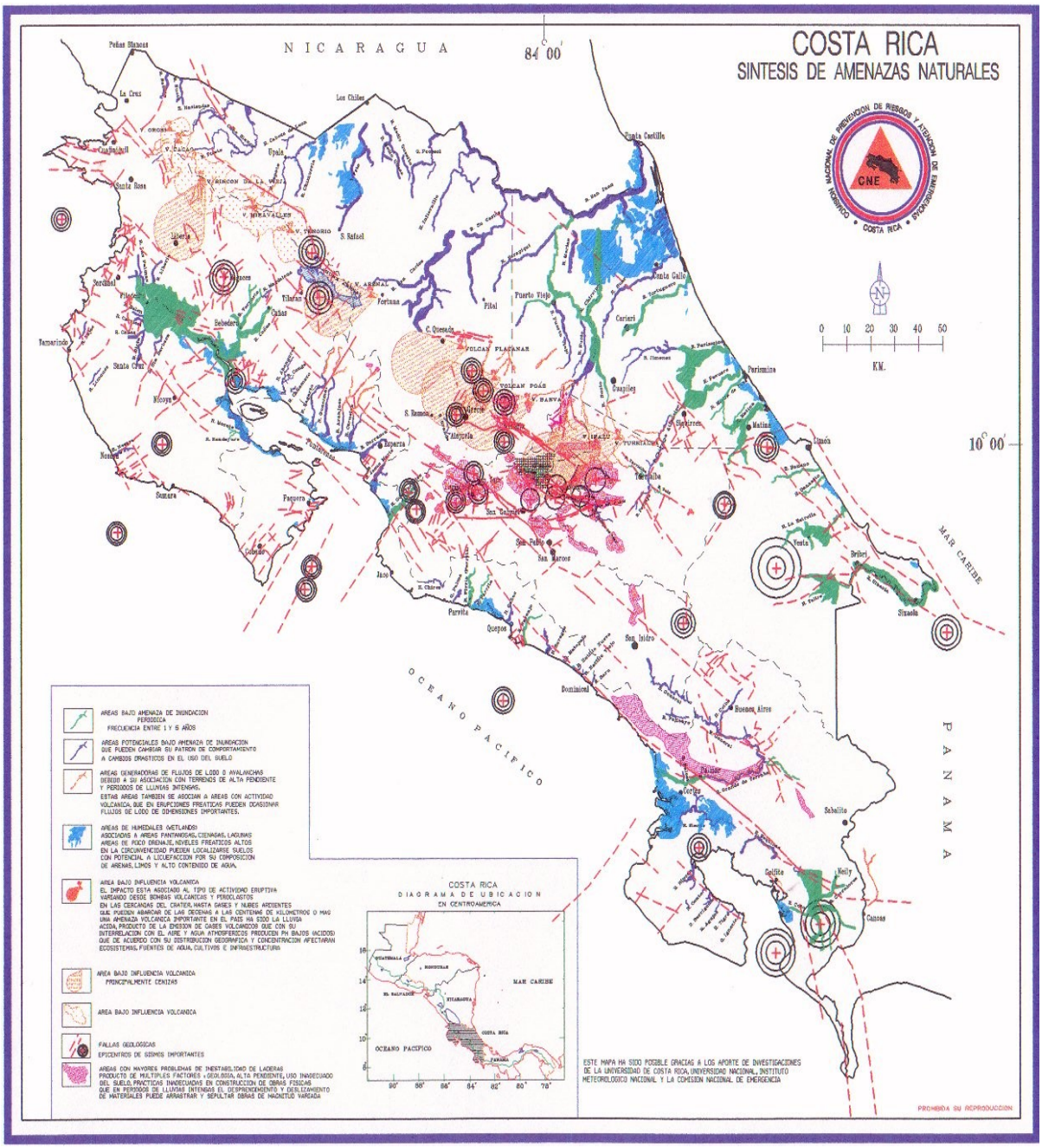
Noticias(2006).Documentación. Recuperado el 15 de junio, de: http://www.noticias.com

Yamile, Osma.(2006) Ingeniera de Sistemas. Informática Organizacional en Heinsohn Software House. Recuperado el 25 de mayo de 2006, de www.noticias.com

Anexos

Figura 2

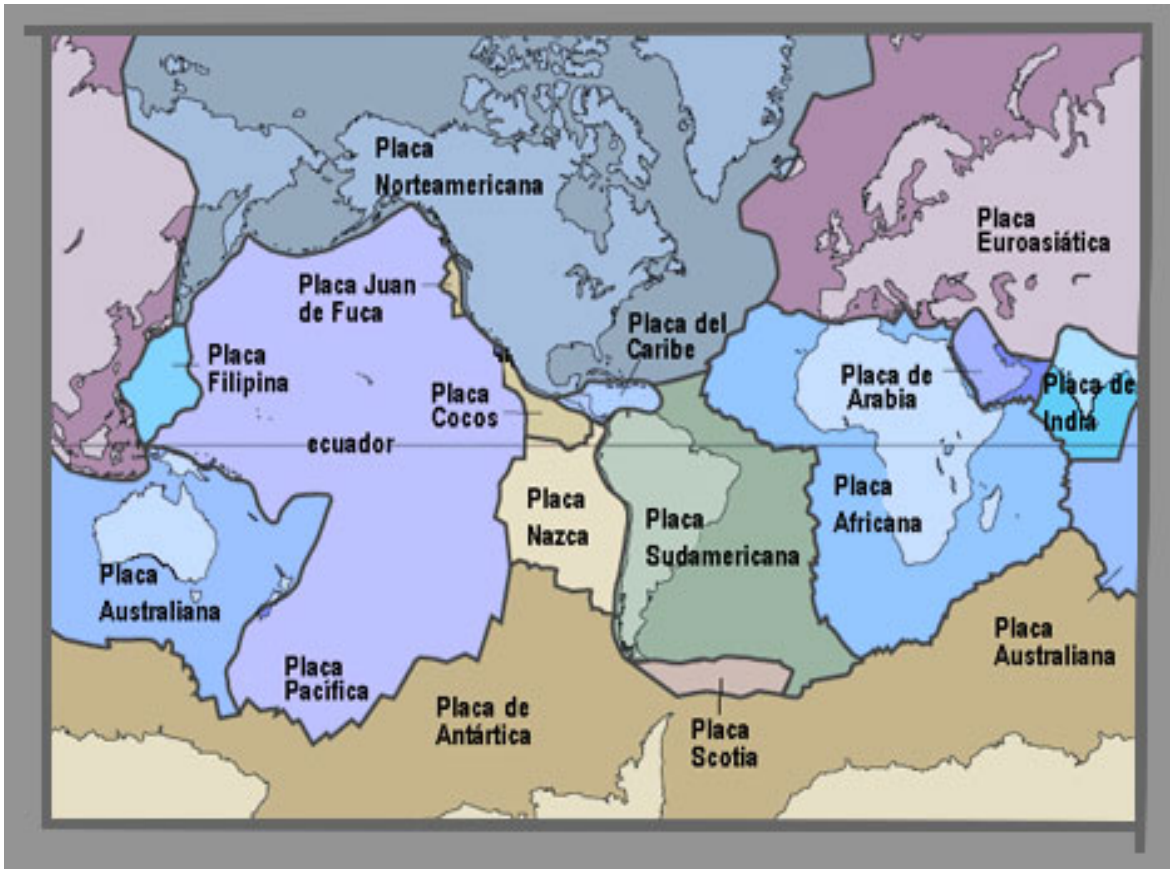
Mapa de Costa Rica Síntesis Amenazas Naturales



Fuente: Comisión Nacional de Emergencia de Costa Rica

Figura 3

Mapamundi, Placas del Planeta Tierra



Fuente: Comisión Nacional de Emergencia de Costa Rica