Universidad Latinoamericana de Ciencia y Tecnología

Facultad de Ingeniería

Escuela de Ingeniería Informática

Trabajo Final para Optar por el grado de Licenciada en Informática con Énfasis en Gestión de Recursos Tecnológicos

Aprovechamiento de los Centros de Cómputo Alternos

Sustentante

Paola Acevedo Vargas

Cédula 1 11720657

Tutor:

Miguel Pérez M

I Cuatrimestre 2007

Índice

Índice de Ilustraciones

Introducción

Actualmente no se concibe el mundo sin ciertos servicios que aunque algunos no son tan indispensables para el diario vivir, si lo son para que "gire" el entorno. Dentro de estos servicios se encuentran los que brindan los bancos o empresas, en el caso de Costa Rica; como el ICE, los cuales son de suma importancia para que se encuentren brindando servicio constantemente a sus clientes por diferentes motivos, por ejemplo, en el caso de una institución financiera es realmente vital tanto para la institución como para el cliente que se realicen ciertas transacciones, o si se ve desde el punto de un Instituto de Electricidad, es vital para muchas otras empresas como hospitales, negocios, y demás, que ésta se mantenga en funcionamiento debido a que una pérdida del fluído eléctrico por un período prolongado pueda significar pérdidas cuantiosas para la misma.

Además, es indudable que la mayoría de las empresas de cierto tamaño, recurren a centros de cómputo para su funcionamiento. Estos centros de cómputo se encuentran equipados con la infraestructura necesaria para brindar los servicios "en el momento preciso" para sus clientes. Así por ejemplo, un Banco necesita mantener su página *Web* siempre en línea para que los clientes puedan realizar, ya sea transferencias, pagos, etc. a cualquier hora del día. Ahora es prácticamente inimaginable una institución financiera que no llegue a brindar este tipo de servicios como el pago de recibos telefónicos desde la comodidad de su hogar. Esto es una pequeña prueba de lo importante que es la tecnología en la actualidad y que prácticamente todos los negocios se encuentran girando con base en este elemento que muchas veces parece ser tan transparente debido a que se ve como parte del diario vivir y que para los clientes no posee mayor relevancia, pero es el corazón de los negocios, ya que mueven y son el motor que produce o genera los insumos para muchas de las actividades cotidianas.

Es por estas razones (la tecnología y la perpetua presencia de ciertos servicios) que se genera un tema que con tanto auge y que al parecer está

teniendo tanta acogida en el país desde hace unos cinco o más años: La creación de Centros de Cómputo de Contingencia o respaldo.

Continuando con el ejemplo de la página *Web* de una institución financiera, es bastante obvia la necesidad que se crea, si se llegara a presentar el caso en el que la página se encuentra constantemente caída "abajo" por problemas en el equipo en el que se obtienen los datos, es muy probable que los clientes de esta institución busquen una que le brinde mejores servicios. O si existiera alguna catástrofe donde se encuentra el centro de cómputo principal de un banco, es de esperar que los clientes entren en pánico y piensen que el recuperar la información de sus finanzas sea un gran problema, esto lo sería si no existieran los Centros de Cómputo Alternos o hasta se puede hablar de Cintotecas[1] Alternas, por medio de las cuales se puede llegar a recuperar la información o datos, haciendo el problema casi imperceptible para los clientes.

Un Centro de Cómputo de Contingencia, es un Centro de Cómputo muy similar al principal de una organización, debe poseer equipos que soporten, por cierto tiempo, la producción, esto quiere decir que deben ser compatibles con el principal, y se debe encontrar en óptimas condiciones para recibir la carga de trabajo que se puede presentar si existen fallos en la Central, debe cumplir con requisitos de lejanía e infraestructura. Aunado a esto, debe existir un buen plan para realizar la migración de manera eficiente y eficaz desde un centro de cómputo al otro.

A continuación se va a describir la importancia de los Centros de Cómputo Alternos, y la forma en que se puede optimizar cada vez su uso, ya que se considera que es una inversión bastante grande la que se debe hacer para poder contar con este tipo de contingencia.

[1] Centro de Almacenamiento de medios de Respaldo que poseen información relevante para la Empresa.

Riesgos[2]

Riesgo es el daño potencial que puede surgir por un proceso presente o evento futuro. Diariamente en ocasiones se lo utiliza como sinónimo de probabilidad, pero en el asesoramiento profesional de riesgo, éste combina la probabilidad de que ocurra un evento negativo y el daño que éste causaría.

El riesgo es usualmente vinculado a la probabilidad de que ocurra un evento no deseado. Generalmente la probabilidad de que ocurra dicho acontecimiento y algún asesoramiento sobre el daño que se espera de él, deben ser unidos en un escenario creíble que combine el riesgo y las probabilidades de arrepentimiento y recompensa en un valor esperado. Hay muchos métodos informales que se usan para asesorar sobre el riesgo (o para "medirlo", aunque esto no suele ser posible) y otros formales.

En el análisis de escenarios, el "riesgo" es distante de lo que se llama "amenaza". Una amenaza es un evento serio, pero de poca probabilidad - cuya probabilidad puede no ser determinada por algunos analistas en un asesoramiento de riesgo porque nunca ha ocurrido, y para la cual ninguna medida preventiva está disponible. La diferencia es más claramente ilustrada por el principio de precaución que busca disminuir la amenaza reduciéndola a una serie de riesgos bien definidos antes de que una acción, proyecto, innovación o experimento sea llevado a cabo.

En seguridad de la información (se llamará así a la protección de cualquier tipo de información, no solo a la los sistemas informáticos) el riesgo es definido como la función de tres variables: la probabilidad de que haya una amenaza, de que haya debilidades y el impacto potencial. Si cualquiera de estas variables se aproxima a cero, el riesgo total también.

Existen riesgos por eventos naturales que son cualquier hecho o proceso que produzca en forma directa o indirecta un daño sobre la población y sobre

---

2 Wikipedia, La enciclopedia libre
Riesgo. Recuperado el 24 de febrero 2007
http://es.wikipedia.org/wiki/Riesgo

sus bienes en una zona. En función de ese hecho se puede hablar de riesgos naturales, mixtos o antrópicos (Debido a la acción o intervención directa o indirecta del hombre)[3].

De aquí la importancia de un Centro de Procesamiento Alterno, ya que al ocurrir algún tipo de riesgo o daño en el Centro de Procesamiento central o primario, es necesario trasladar las operaciones del centro actual a uno que se encuentre en las mejores condiciones para recibirlas y continuar con la operación normal de la organización.

Centro de respaldo[4]

Un Centro de respaldo es un eje, sede o foco de proceso de datos (CPD) específicamente diseñado para tomar el control de otro CPD principal en caso de contingencia.

Se denomina centro de proceso de datos a aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de información de una organización. También se conoce como centro de cálculo. Dichos recursos consisten esencialmente en unas dependencias debidamente acondicionadas, computadoras y redes de comunicaciones. Los centros de proceso de datos se suelen denominar por su acrónimo: CPD. En inglés, se denomina *Data Center*.

Un CPD[5] consiste en un edificio usado para mantener en él una gran cantidad de equipamiento electrónico. Suelen ser creados y mantenidos por grandes organizaciones con objeto de tener acceso a la información necesaria para sus operaciones. Por ejemplo, un banco puede tener un *data center* con el propósito de almacenar todos los datos de sus clientes y las operaciones

---

[3] Navarro F. (2004). La enciclopedia. Madrid España: Editorial Salvat Editores

4 Wikipedia, La enciclopedia libre
Centro de respaldo. Recuperado el 06 de febrero 2007
http://es.wikipedia.org/wiki/Centro_de_respaldo

5 Wikipedia, La enciclopedia libre
Centro de proceso de datos. Recuperado el 22 de febrero 2007
http://es.wikipedia.org/wiki/Centro_de_proceso_de_datos

que éstos realizan sobre sus cuentas. Prácticamente todas las compañías que son medianas o grandes tienen algún tipo de CPD, y las más grandes llegan a tener varios.

Grandes organizaciones, tales como Bancos o Administraciones Públicas, no pueden permitirse la pérdida de información ni el cese de operaciones, ante un desastre, en su centro de proceso de datos. Terremotos, incendios o atentados en estas instalaciones son infrecuentes, pero no improbables. Por este motivo, se suele habilitar un centro de respaldo para absorber las operaciones del CPD principal en caso de emergencia

Diseño de un centro de respaldo

Un centro de respaldo se diseña bajo los mismos principios que cualquier CPD, pero con algunas consideraciones más. En primer lugar, debe elegirse una localización totalmente distinta a la del CPD principal, con el objeto de que no se vean ambos afectados simultáneamente por la misma contingencia. Es habitual situarlos entre 20 y 40 kilómetros del CPD principal. La distancia está limitada por las necesidades de telecomunicaciones entre ambos centros.

En segundo lugar, el equipamiento electrónico e informático del centro de respaldo debe ser absolutamente compatible con el existente en el CPD principal. Esto no implica que el equipamiento deba ser exactamente igual. Normalmente, no todos los procesos del CPD principal son críticos. Por este motivo no es necesario duplicar todo el equipamiento. Por otra parte, tampoco se requiere el mismo nivel de servicio en caso de emergencia. En consecuencia, es posible utilizar hardware menos potente. La pecera de un centro de respaldo recibe estas denominaciones en función de su equipamiento:

- **Sala blanca** cuando el equipamiento es exactamente igual al existente en el CPD principal.
- **Sala de** *back-up* cuando el equipamiento es similar, pero no exactamente igual.

En tercer lugar, el equipamiento *software* debe ser idéntico al existente en el CPD principal. Esto implica exactamente las mismas versiones y parches del software de base y de las aplicaciones corporativas que estén en explotación en el CPD principal. De otra manera, no se podría garantizar totalmente la continuidad de operación.

Por último, pero no menos importante, es necesario contar con una réplica de los mismos datos con los que se trabaja en el CPD original. Este es el problema principal de los centros de respaldo, que se detalla a continuación.

El sincronismo de datos

Existen dos políticas o aproximaciones a este problema:

- La copia síncrona sincrónica de datos. Se asegura que todo dato escrito en el CPD principal también se escribe en el centro de respaldo antes de continuar con cualquier otra operación.
- La copia asíncrona asincrónica de datos. No se asegura que todos los datos escritos en el CPD principal se escriban inmediatamente en el centro de respaldo, por lo que puede existir un desfase temporal entre unos y otros.

La copia asíncronica puede tener lugar *off-line* o fuera de línea. En este caso, el centro de respaldo utiliza la última copia de seguridad existente del CPD principal. Esto lleva a la pérdida de los datos de operaciones de varias horas (como mínimo) hasta días (lo habitual). Esta opción es viable para negocios no críticos, donde es más importante la continuidad del negocio que la pérdida de datos. Por ejemplo, en cadenas de supermercados o pequeños negocios. No obstante, es inviable en negocios como la banca, donde es impensable la pérdida de una sola transacción económica.

En los demás casos, la política de copia suele descansar sobre la infraestructura de almacenamiento corporativo. Generalmente, se trata de redes SAN[6] y cabinas de discos con suficiente inteligencia como para implementar dichas políticas.

[6] **SAN** corresponde al concepto *Storage Area Network* (Red de área de almacenamiento), es una red concebida para conectar servidores, arreglos (*arrays*) de discos

Tanto para la copia sincrónica como asincrónica, es necesaria una extensión de la red de almacenamiento entre ambos centros. Es decir, un enlace de telecomunicaciones entre el CPD y el centro de respaldo. En caso de copia asincrónica es imprescindible que dicho enlace goce de baja latencia. Motivo por el que se suele emplear un enlace de fibra óptica, que limite la distancia máxima a decenas de kilómetros. Existen dos tecnologías factibles para la copia de datos en centros de respaldo:

- iSCSI.
- Fiber Channel.

La copia sincrónica es esencial en negocios como la banca, donde no es posible la pérdida de ninguna transacción. La copia asincrónica es viable en la mayoría de los casos, ya que el desfase temporal de la copia se limita a unos pocos minutos.

Aprovechamiento de un Centro de Respaldo

Existen diferentes formas de darle un uso adecuado a un Centro de Cómputo de Contingencia, esto con el fin de aprovechar la inversión que se presenta al acondicionar un espacio con las características de un Centro de Cómputo con el fin de que éste pueda asumir la carga de trabajo de la organización. A continuación se describirán tres diferentes opciones para el adecuado aprovechamiento de un Centro de Cómputo de Respaldo, estas son: mediante un Plan de Contingencias en caso de una eventualidad, la Delegación de Procesos y el Balanceo de Carga de los equipos.

---

y librerías de respaldo principalmente. Su función es la de conectar de manera rápida, segura y confiable los distintos elementos que la conforman.

Wikipedia, La enciclopedia libre

Storage Area Network. Recuperado el 12 de febrero 2007

http://es.wikipedia.org/wiki/SAN

Plan de Contingencias[7]

Un centro de respaldo por sí sólo no basta para hacer frente a una contingencia grave. Es necesario disponer de un Plan de Contingencias corporativo. Este plan contiene tres sub-planes que indican las medidas técnicas, humanas y organizativas necesarias en tres momentos clave:

- El plan de respaldo. Contempla las actuaciones necesarias antes de que se produzca un incidente. Esencialmente, mantenimiento y prueba de las medidas preventivas. Incluye la correcta realización de cada uno de los respaldos de la información necesaria para realizar las recuperaciones, las actualizaciones en los equipos, es el asegurarse que el equipo de contingencia se encuentre realmente compatible con el principal y que posee lo necesario para recibir la producción en caso de existir alguna falla.
- El plan de emergencia. Contempla las actuaciones necesarias durante un incidente. Incluye cada uno de los pasos que se van a realizar para determinar cómo se va a hacer el traslado de las operaciones al Centro de Respaldo, además, del traslado o preparación del personal para recibir la producción, debe ser un plan detallado y efectivo. Se debe hacer en la menor cantidad de pasos o tareas posibles para asegurar su clara y eficaz implementación.
- El plan de recuperación. Contempla las actuaciones necesarias después de un incidente. Incluye las actividades por medio de las cuales se va a realizar la vuelta de la producción hacia el equipo principal, es revertir, con mayor seguridad y confianza el plan de emergencia para dejar "todo como estaba" antes del incidente, sin haber dejado de brindar el servicio y volver a aplicar las transacciones realizadas cuando la producción se encontraba en

[7] Wikipedia, La enciclopedia libre
Plan de Contingencias. Recuperado el 24 de febrero 2007
http://es.wikipedia.org/wiki/Plan_de_Contingencias

el Centro de Cómputo Principal. Básicamente, indica cómo volver a la operación normal.

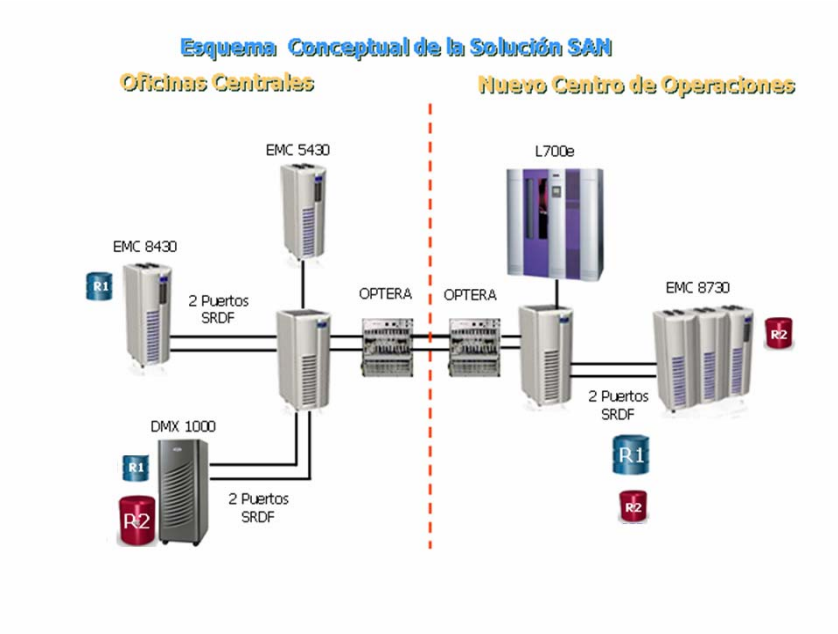
Un Plan de contingencias es un instrumento de gestión para el buen gobierno de las Tecnologías de la Información y las Comunicaciones en el dominio del soporte y el desempeño

Dicho plan debe garantizar la continuidad del negocio y las operaciones de una compañía. Un plan de contingencias es un caso particular de procedimiento de continuidad aplicado al departamento de informática o tecnologías. Otros departamentos pueden tener planes de continuidad que persiguen el mismo objetivo desde otro punto de vista. No obstante, dada la importancia de las tecnologías en las organizaciones modernas, el plan de contingencias es el más relevante.

A continuación se muestra un esquema conceptual de una solución para asegurar la continuidad del negocio, de esta manera, existirían dos centros de cómputo casi en iguales condiciones, los cuales se comunican por medio de la tecnología de *Unisys*, este esquema aunado a un Plan de Contingencias permite la continuidad de la operación del Centro de Cómputo Principal hacia el secundario.

Ilustración 1

Esquema Conceptual de la Solución SAN



Fuente: Continuidad del Negocio, EMC

Continuidad del Negocio[8]

El desarrollo de un programa efectivo de continuidad del negocio requiere una comprensión del negocio, la flexibilidad para satisfacer requerimientos cambiantes y una profunda experiencia técnica en toda la infraestructura.

La continuidad del negocio debe ser capaz de:

- Sobrevivir a un desastre y reiniciar la empresa
- Detectar de manera proactiva los daños en los datos y minimizar la exposición y el riesgo
- Probar nuevas aplicaciones con datos reales y en entornos del mundo real
- Acortar los tiempos de backup y restore
- Realizar mantenimiento y upgrades de hardware y software no disruptivos
- Mover y migrar datos
- Proteger sitios remotos
- Proporcionar protección continua en múltiples sitios

Un buen programa de continuidad del negocio comienza cuando los participantes del negocio y de TI se ponen de acuerdo claramente con respecto a sus necesidades y requerimientos particulares.

Pasos para una efectiva planeación para garantizar la Continuidad del Negocio:

- Evaluación del nivel de servicio: identifica las fortalezas y debilidades de su actual programa de continuidad del negocio y evalúa su capacidad para satisfacer los requerimientos del negocio; todo a través de una completa revisión de planes, procesos y validación de los niveles de servicio mediante pruebas.

8 EMC Coporation. Teorías de hoy para continuidad del negocio, 3-6

- Definición de requerimientos: determina los impactos financieros y operacionales que tienen en su negocio el *downtime* o la pérdida de los datos de aplicaciones y procesos claves y determina los niveles de servicio de sus sistemas de negocio críticos.
- Evaluación de alternativas: decisión informada acerca de las disyuntivas de costo/beneficio para su programa de continuidad del negocio.
- Diseño de infraestructura: realiza un análisis detallado para determinar la estrategia de recuperación de aplicaciones interdependientes con los mismos requerimientos y efectúa la asignación a las infraestructuras de destino. Los resultados incluyen especificaciones de arquitectura detalladas con diagramas de infraestructura, definiciones y supuestos.
- Servicios de implementación: las mejores prácticas
- Planificación de la implementación: desarrolla un plan de implementación detallado para la construcción de la infraestructura, que incluye criterios de selección de productos, procedimientos de implementación y un plan detallado del proyecto que enumera todas las tareas, dependencias, recursos, plazos, hitos, productos y costos.
- Implementación de tecnología: integra y prueba en su entorno los productos y tecnologías de continuidad del negocio especificados.
- Desarrollo del plan de recuperación: crea procedimientos y *scripts* detallados para la recuperación desde el sitio primario a sitios alternativos y de regreso al sitio primario cuando esté disponible. Los resultados abarcan completos planes de recuperación/disponibilidad que incluyen software de automatización, procedimientos y programas de mantenimiento.
- Pruebas de integración: realiza pruebas en el nivel de sistema en todas las aplicaciones, infraestructura y validación de usuarios. Los resultados incluyen pautas de pruebas, *scripts* y escenarios

de pruebas con metas, criterios de éxito, procedimientos para presupuestos y auditoría, resultados de pruebas documentados y un plan de pruebas para 12 meses.

- Servicio de definición del programa de recuperación: desarrolla o actualiza todos los materiales de comunicaciones internas y externas, políticas, procedimientos y acuerdos de nivel de servicio para que reflejen el programa de disponibilidad y recuperación mejoradas.
- Administración de servicios: los buenos programas de continuidad del negocio evolucionan junto con las necesidades de su negocio. Estos servicios aseguran que sus procesos, procedimientos y documentación se adapten a sus cambiantes requerimientos.
- Servicios de operaciones y administración: desarrolla sistemas de organización, niveles de dotación de personal, presupuestos, métricas y *reporting* y cambia los sistemas de administración necesarios para operar el programa de continuidad del negocio a lo largo del tiempo.

Ciclo de vida

El plan de contingencias sigue el conocido ciclo de vida iterativo "*plan-do-check-act*", es decir, "planifica-actúa-comprueba-corrige". Nace de un análisis de riesgos en donde, entre otras amenazas, se identifican aquellas que afectan a la continuidad del negocio.

Sobre dicha base se seleccionan las contramedidas más adecuadas entre diferentes alternativas, siendo plasmadas en el plan de contingencias junto con los recursos necesarios para ponerlo en marcha.

El plan debe ser revisado periódicamente. Generalmente, la revisión será consecuencia de un nuevo análisis de riesgos. En cualquier caso, el plan de contingencias siempre es cuestionado cuando se materializa una amenaza, actuando de la siguiente manera:

- Si la amenaza estaba prevista y las contramedidas fueron eficaces: se corrigen solamente aspectos menores del plan para mejorar la eficiencia.
- Si la amenaza estaba prevista pero las contramedidas fueron ineficaces: debe analizarse la causa de la falla y proponer nuevas contramedidas.
- Si la amenaza no estaba prevista: debe promoverse un nuevo análisis de riesgos. Es posible que las contramedidas adoptadas fueran eficaces para una amenaza no prevista. No obstante, esto no es excusa para evitar el análisis de lo ocurrido.

Finalmente, se modifica el plan de contingencias de acuerdo a las revisiones aprobadas y, de nuevo, se inicia el ciclo de vida del plan.

Por otra parte, el plan de contingencias no debe limitarse a estas medidas organizativas. También debe expresar claramente:

- Qué recursos materiales son necesarios.
- Qué personas están implicadas en el cumplimiento del plan.
- Cuáles son las responsabilidades concretas de esas personas y su rol dentro del plan.
- Qué protocolos de actuación deben seguir y cómo son.

Delegación de Procesos

Cuando se poseen centros de Cómputo Alternos, es importante que tomen en cuenta las diferentes formas en que este se puede y se debe aprovechar. Una de ellas es la Delegación de Procesos del Centro de Cómputo Principal al Alterno.

Sin embargo, ¿qué es esto y cómo se puede hacer?

Delegar es el enviar algo de un lugar a otro, es hacer que, por ejemplo, un subordinado, realice ciertas funciones que el superior no puede atender en el momento. Así, delegar procesos significaría el enviar los procesos que para el Centro de Cómputo Principal no son tan “importantes” al Centro de Cómputo Alterno para que este se encargue de realizarlo.

De este modo se pueden realizar varios procesos que permitan "desahogar" el centro principal y enfocar este en procesos más pesados y transaccionales para así no perder el enfoque del mismo.

Algunos de los ejemplos de estos procesos son:

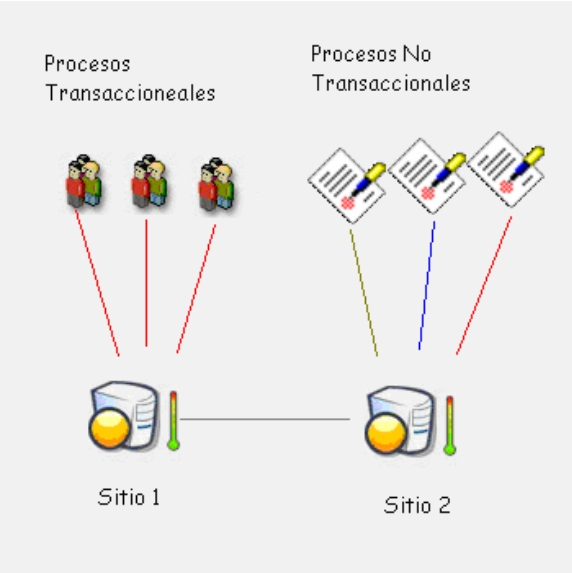
1. Procesos que realizan lecturas: existen procesos transaccionales que son realmente pesados para un procesador y otros, los procesos que solamente realizan lecturas a las Bases de Datos, estos algunas veces no son tan pesados y en cualesquiera de los dos casos pueden ser remitidos al Centro de Respaldo para que este y el personal que se mantiene en él, los administren, mientras que el Procesador principal se encarga de la atención directa de los primeros.
2. Procesos de Respaldo en Caliente: Existen muchos respaldos que se realizan en un Centro de Cómputo, cuando las Bases de Datos que estos Centros comparten son réplicas exactas en todo momento, es posible que se realicen los diferentes respaldos de la información en un Centro Alterno.
3. Procesos de Respaldos Comunes: Muchas veces los respaldos que se realizan de diferentes archivos y procesos generan mucha mensajería y consumen mucho del CPU de un computador, además, que existen respaldos que no son en caliente, sino de información anterior, que por uno u otro motivo se deben realizar, por lo que es importante que todos estos tipos de respaldos se ejecuten en el centro de cómputo alterno para que no afecte la atención a los clientes en cuanto al uso y consumo del CPU.
4. Procesos de Revisiones: Cuando un Centro de Cómputo se encuentra constantemente en atención de sus clientes, las revisiones no son la prioridad, son revisiones como el espacio en disco, consumo del CPU, etc. Todas estas revisiones se deben enviar a un Centro de Respaldo para que mediante la tecnología que poseen de comunicación estos Centros de Cómputo, se

puedan estar realizando las diferentes revisiones que son necesarias para el óptimo desempeño de ambos lugares.

En la figura adjunta, se muestran los sitios o Centros de Cómputo, en el Sitio 1 (Centro de Cómputo Principal) se atienden los procesos transaccionales de los clientes, mientras que en el Sitio 2 (Centro de Cómputo de Respaldo) se atienden los demás procesos como lecturas, respaldos, revisiones, etc.

Ilustración 2

Delegación de Procesos en dos Centros de Cómputo



Fuente: Paola Acevedo Vargas (2007, 12 marzo)

Balanceo de Carga

Una forma importante para aprovechar un Centro de Respaldos es utilizando el método de Balanceo de Carga.

El Balanceo de Carga consiste en dividir entre los dos centros de cómputo toda la carga de trabajo que realiza la organización, desde los respaldos hasta los procesos transaccionales.

El balance o balanceo de carga es un concepto usado en informática que se refiere a la técnica usada para compartir el trabajo a realizar entre varios procesos, ordenadores, discos u otros recursos. Está íntimamente ligado

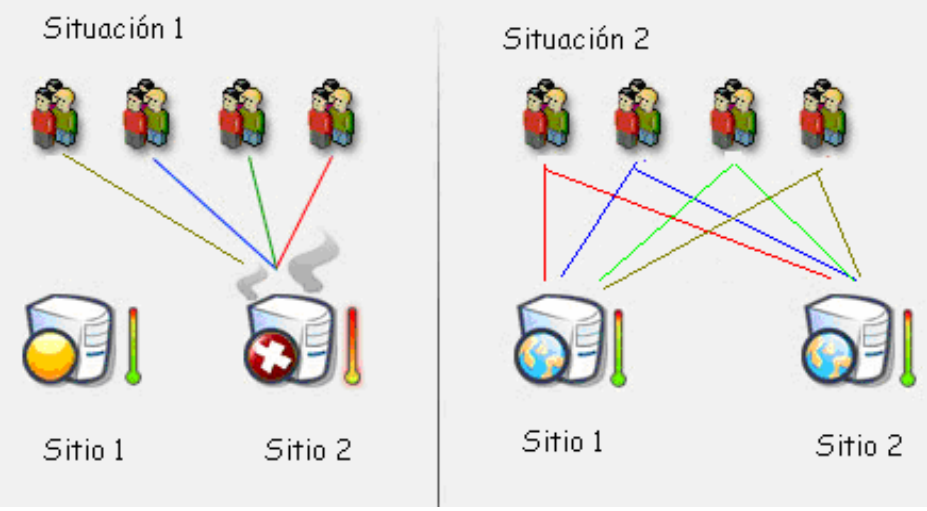
a los sistemas de multiprocesamiento, o que hacen uso de más de una unidad de procesamiento para realizar labores útiles.

El balance de carga se mantiene gracias a un algoritmo que divide de la manera más equitativa posible el trabajo, para evitar los así denominados cuellos de botella que es el objetivo del multiprocesamiento.

En la figura adjunta se muestran dos tipos de situaciones, en el primero, el Centro de Cómputo Principal asume toda la carga de trabajo y solamente en caso de que este deba acudir al plan de contingencia para la continuidad, el sitio 2 entra en funcionamiento. En la Situación 2 ambos centros de Cómputo se encuentran en atención de procesos transaccionales, si se llegara a presentar alguna eventualidad en el Sitio 1, el sitio 2 es completamente capaz de asumir la carga de trabajo de ambos lugares. Esto sería posible en caso de que ambos centros se mantengan con la capacidad de manejar el negocio por sí solos durante cierta cantidad de tiempo.

Ilustración 3

Balanceo de Carga



Fuente: Paola Acevedo Vargas (2007, 12 Marzo)

Ventajas y desventajas de un Centro de Cómputo de Respaldo

Los Centros de Cómputo de Respaldo son bastante útiles para las organizaciones, sin embargo, tienen algunos aspectos en contra. A

continuación se muestra el Cuadro 1, el cual presenta algunas ventajas y desventajas de la utilización de un Centro de este tipo.

Cuadro 1

Ventajas y desventajas de un Centro de Cómputo de Respaldo

Ventajas	Desventajas
Se posee un Centro en Caso de emergencias, siniestros, desastres al cual recurrir si es necesario	Costos: Los costos llegan a ser muy elevados
Se pueden dividir funciones, ahora no solamente el centro de cómputo principal realiza todas las funciones, sino que se tiene uno alterno.	Capacitación: Es importante capacitar al personal en la administración del Centro Alterno ya que normalmente son tecnologías que requieren capacitación extra.
Se puede "desahogar" el Centro de Cómputo Principal: al pasar ciertas funciones el procesador principal se puede centrar en ciertos otros procesos.	Duplicación de Funciones/ Funcionarios: No se debe manejar solamente un Sitio sino que ahora son dos por lo que se puede llegar a ocupar mayor cantidad de personal y por ende las funciones se pueden duplicar.
Se puede llegar a garantizar el servicio: si es posible trasladar las operaciones normales, en caso de desastre se garantiza que se continúe dando el servicio	Actualizaciones: Se deben realizar por partida doble, ya que tendrían dos centros con características similares, pero diferentes en varios aspectos.
Personal Especializado: los funcionarios se llegan a capacitar de manera importante para el manejo de ambos centros de Cómputo	Se llega a depender del proveedor: ya que siempre debe brindar el mantenimiento necesario para que ambos centros de cómputo se encuentren en funcionamiento.

Fuente: Paola Acevedo Vargas (2007, 12 marzo)

Conclusiones

Conforme pasa el tiempo es cada vez más imperiosa la necesidad de las empresas de encontrar cómo hacerse conocer, cómo brindar los servicios de manera continua para encontrar la manera de producir más, atraer más clientes y por supuesto ser más rentables.

La tecnología, como se vio anteriormente, brinda muchas facilidades para realizar cada uno de los objetivos de los empresarios, sin embargo, como todo lo realizado por el hombre, es factible que ésta falle por diferentes razones, desde siniestros hasta accidentes en los computadores.

Los centros de cómputo son agrupaciones de procesadores, tecnologías, software y demás, que permiten darle mantenimiento al negocio procesando el activo más importante de éste que son sus datos.

La mayoría de las empresas de mediano a gran tamaño, cuentan con centros de cómputo para realizar sus procesos diarios y para atender a sus clientes. Otras de un tamaño mayor, poseen centros de cómputo aparte del principal para realizar diferentes procesos, sin embargo, esto es un poco costoso, ya que si un solo Centro de Cómputo es una inversión cuantiosa, dos centros lo son el doble y muchas veces más que esto. Es por esta razón que es importante, como se describió en el desarrollo del tema, que se le busque una buena utilización a este centro que no está de más, pero que debe contar con muchos requisitos importantes.

Las tres opciones que se describieron para darle un adecuado aprovechamiento a un Centro de Cómputo de respaldo, muestran un panorama amplio y utilizable del mismo. La utilización de este centro para la continuidad del negocio, la cual se considera la más importante, ya que permite su utilización al cien por ciento mediante las pruebas que se pueden realizar y los diferentes sucesos que se pueden dar en el transcurso del tiempo. Además, se encuentra también la Delegación de Procesos la cual es bastante provechosa para poder “desahogar” el Centro Principal de procesos que no son tan importantes para él, pero sí pueden generarle mucho consumo de su procesador y recursos innecesariamente. Por último, el Balanceo de

Carga permite que los procesos sean distribuidos adecuadamente entre ambos centros de cómputo para que los recursos y la utilización de los mismos en los dos, permita un óptimo desempeño y aprovechamiento.

Como es de conocimiento de los profesionales en Sistemas de Información, la tecnología, si bien es cierto es muy importante en el mundo actual y futuro, también es completamente verdadero el hecho de que ésta nos es nada barata, al contrario, los costos cada vez son mayores debido a la actualización y mejores usos que se le da a la misma. Es por estas dos razones (la necesidad y los costos) que un Centro de Cómputo de Contingencia es sumamente importante para la Continuidad del Negocio, pero con todo esto es muy necesario que estos centros tengan un adecuado uso, para que se pueda aprovechar al máximo la inversión presentada.

Creo que esta investigación ha sido bastante enriquecedora porque ha permitido la adquisición de conocimientos importantes sobre la necesidad de un Centro de Cómputo de Respaldo y como es posible aprovecharlo: desde su utilización para nivelar las cargas de trabajo, hasta como centro de Contingencia para el caso de algún desastre presentado en el Centro Principal.

Bibliografía

Wikipedia, La enciclopedia libre

- Centro de respaldo. Recuperado el 06 de febrero 2007

http://es.wikipedia.org/wiki/Centro_de_respaldo

- Storage Area Network. Recuperado el 12 de febrero 2007

http://es.wikipedia.org/wiki/SAN

- Centro de proceso de datos. Recuperado el 22 de febrero 2007

http://es.wikipedia.org/wiki/Centro_de_proceso_de_datos

- Plan de Contingencias. Recuperado el 24 de febrero 2007

http://es.wikipedia.org/wiki/Plan_de_Contingencias

- Riesgo. Recuperado el 24 de febrero 2007

http://es.wikipedia.org/wiki/Riesgo

EMC Coporation. Teorías de hoy para continuidad del negocio, 3-6

Paola Acevedo (2007, 12 marzo). Entrevista con Jorge Mejía Suárez, soportista de la plataforma de MCP, Banco Nacional de Costa Rica, San José Costa Rica.

Computing, el Seminario de las TIC

- El IAM ultima su centro de contingencia, Recuperado el 22 de febrero, 2007

http://www.computing.es/Actualidad/An%E1lisis/Inform%E1tica_profesional/Empresas/20061219049

Sun Microsystems

- Acerca de PS IT Consulting, recuperado el 22 de febrero 2007

http://es.sun.com/services/ps/AcercaPS/descripcionyventajas.html

Navarro F. (2004). La enciclopedia. Madrid España: Editorial Salvat Editores

Anexos

Anexo1

El IAM ultima su centro de contingencia Contrata con Telvent el *housing* de equipos.[9]

Desde hace un tiempo, el organismo autónomo Informática del Ayuntamiento de Madrid (IAM) está trabajando en la construcción de un centro de respaldo con el fin de duplicar su infraestructura y aplicativos más importantes, garantizando así la disponibilidad en caso de desastre.

Como explica a COMPUTING Enrique Martín Cabrera, gerente del IAM, "se trata de ir construyendo un centro espejo donde soportar las aplicaciones del Ayuntamiento más críticas para recuperarlas en caso de fallo o desastre, de forma que en un par de años casi todos los elementos estén duplicados".

Para ello, el IAM ha optado por la opción de `*housing*´, "ya que el alquiler de un centro especializado supone ahorros de tiempo y dinero". Eso sí, los equipos que se van a duplicar pertenecen al Ayuntamiento.

Esta arquitectura se ha ido adquiriendo por fases, y consiste tanto en los antiguos *mainframe* heredados del área de Gobierno, las diversas agencias y delegaciones del Ayuntamiento de Madrid, como de nuevos equipos que se han comprado por concurso o negociación en los dos últimos años.

En el primer caso, el IAM gestiona diversos servidores AS/400, un gran elenco de equipos Wintel (principalmente dedicados al entorno ofimático y

---

[9] Computing, el Seminario de las TIC

El IAM ultima su centro de contingencia, Recuperado el 22 de febrero, 2007

http://www.computing.es/Actualidad/An%E1lisis/Inform%E1tica_profesional/Empresas/20061219049

logístico como el soporte *web* y de correo electrónico), otros de menor tamaño y el *host* basado en equipos IBM zSeries.

Con respecto a las últimas adquisiciones, se han comprado servidores Itanium provistos por IBM, en los que se corren aplicaciones críticas como es el caso de SAP, ERP que administra todo el entorno de Recursos Humanos.

"Ahora mismo estamos inmersos en una política de concentración y consolidación de servidores y aplicativos" -continúa Martín Cabrera- "sobre todo con el fin de migrar viejos equipos y dotar a las aplicaciones de una orientación hacia servicios *web*".

Anexo 2

Sun[10]

Sun ha desarrollado una metodología estándar que cuenta con los siguientes pasos a la hora de dotar a nuestros clientes de continuidad en sus procesos críticos de negocio.

Fase I: Análisis de Impacto en el Negocio Este análisis (*Business Impact Analysis o BIA*) es una pieza fundamental para ayudar a nuestros clientes en el análisis de sus procesos de negocio, para evaluar los riesgos que pueden incidir en la continuidad de sus negocio y poder estudiar sus requisitos mínimos de recuperación de los procesos que se identifiquen como críticos y que serán la base del Plan de Continuidad que se defina.

Fase II: Diseño del Entorno de Contingencia Una vez desarrollado el BIA, el siguiente paso en la elaboración de un Plan de Continuidad de Negocio consiste en la selección y diseño de la estrategia de recuperación adecuada para cada uno de los procesos de negocio identificados como críticos en dicho BIA.

---

10 Sun Microsystems
Acerca de PS IT Consulting, recuperado el 22 de febrero 2007
http://es.sun.com/services/ps/AcercaPS/descripcionyventajas.html

Fase III: Instalación y Configuración del Entorno de Contingencia Una vez definido y aprobado el diseño del entorno de contingencia, se procede a instalar y configurar todos sus componentes. Sun PS ofrece un amplísimo catalogo de servicios de instalación y configuración que cubren todas las posibles necesidades al respecto. Este catálogo incluye servicios de:

- Instalación y configuración de plataforma base

- Implantación de soluciones "*hot site*" basadas en replicación de datos

- Implantación de soluciones "*cold site*" basadas en *Backup/Restore* (Librerías, SW, Tercera copia, etc.)

Fase IV: Elaboración del Plan de Contingencia El Centro de Contingencia tendrá dos escenarios completamente diferentes de funcionamiento. En el primero, en el que se puede decir que el centro está en Modo Espera/Replicación, está simplemente recogiendo las variaciones de la información que se producen en el Centro de Producción o, simplemente, a la espera de ocurrencia de evento desastre. El segundo escenario, denominado Modo Contingencia, se activa en caso de parada prolongada del Centro de Producción como consecuencia de un desastre.

El Plan de Contingencia contiene todos y cada uno de los procedimientos organizativos, operativos y técnicos para pasar el Centro de Contingencia desde el Modo Espera/Replicación al Modo Contingencia de una forma ordenada, sin riesgos y consistente.

Fase V: Proceso de Simulacros Tras presentar y acordar el alcance y objetivo del Plan de Pruebas de Recuperación, se ejecuta dicho plan con el fin de validar la adecuación del Plan de Recuperación elaborado a las necesidades del cliente expresadas en el BIA.

VENTAJAS PARA EL CLIENTE

- Sun PS está cualificado de forma única para determinar los requisitos de su solución de contingencia debido a su probada base de conocimiento, su amplio historial de liderazgo en el sector y sus soluciones de servicios y productos, extremo a extremo

- A diferencia de muchos proveedores de tecnología, Sun PS ofrece un servicio y un soporte completo para ayudarle a asegurar que su implantación funcionará correctamente en caso de evento desastre, o lo que es lo mismo,

las necesidades de su negocio en cuanto continuidad se refiere, serán satisfechas por la solución de contingencia diseñada, elaborada e implantada

Los puntos clave que se pueden destacar de la solución aportada por Sun PS son:

- Analizar los requerimientos del cliente, en cuanto a continuidad se refiere, de sus procesos críticos de negocio

- El conocimiento único de cómo elaborar un Plan de Continuidad completo, que cubre el diseño e instalación de la solución, así como la redacción del Plan de Contingencia

- La capacidad de enfocar la solución desde los puntos de vista de negocio, tecnológico y operacional

- Los consultores de Sun PS proporcionan una autoridad experta en consultoría de planes de contingencia y sus servicios de integración de sistemas