TRABAJO ESPECIAL DE GRADO

AMBIENTE TOLERANTE A FALLAS PARA EL SISTEMA SAP R/3 CONSIDERANDO UN CENTRO DE DATOS ALTERNATIVO PARA SINCRUDOS DE ORIENTE SINCOR C.A.

Presentado ante la ilustre Universidad
Central de Venezuela para optar al título
de Especialista en Comunicaciones y
Redes de Comunicación de Datos
por el **Ing. Lenin A. Simancas Graterol**

Caracas, octubre 2004

Hecho el Depósito de Ley
Depósito legal lft487200462048

ÍNDICE GENERAL

ÍNDICE DE TABLAS Y FIGURAS

RESUMEN

Simancas G., Lenin A

AMBIENTE TOLERANTE A FALLAS PARA EL SISTEMA SAP R/3 CONSIDERANDO UN CENTRO DE DATOS ALTERNATIVO PARA SINCRUDOS DE ORIENTE SINCOR C.A.

Tutor Académico: Prof. Carlos Moreno. Tesis. Caracas, UCV. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Especialización en Redes de Comunicaciones y Comunicaciones de Datos. Año 2004, 108 p.

Palabras claves: Recuperación de desastres, Continuidad de negocios, Contingencia, SAP R/3.

Resumen: Sincrudos de Oriente, SINCOR C.A. posee una amplia infraestructura tecnológica distribuida entre las diferentes localidades donde la empresa tiene operaciones. La mayor parte de esta infraestructura tecnológica se encuentra en la sede principal ubicada en Caracas, lo cual implica que gran cantidad de usuarios se conecta remotamente desde las diferentes dependencia para hacer uso de los sistemas administrativos y aplicaciones operativas.

En SINCOR la mayor parte de las actividades administrativas procesos relacionados con finanzas, mantenimiento de planta, manejo de materiales, mostos y comercialización son ejecutados a través del sistema SAP R/3, esto lo convierte en uno de los sistemas vitales para la organización; siendo necesario garantizar la continuidad operativa de este sistema ante cualquier tipo de falla.

Como consecuencia la organización decidió diseñar e implantar un plan que permita mantener las operaciones del sistema SAP R/3 en condiciones de desastre mayor de la infraestructura que soporta el sistema de producción ubicado en Caracas, tales como daño a los servidores del ambiente SAP R/3, daño total o parcial de los respaldos en cinta, problemas eléctricos o cualquier otro factor que pudiera interrumpir las operaciones del sistema por largo periodo de tiempo.

El plan de recuperación de desastres para el sistema SAP R/3 está basado en la preparación de un ambiente tolerante a fallas en el cual se realice la replicación de archivos de transacciones desde el centro de datos primario ubicado en las oficinas principales de SINCOR hacia el Centro de datos secundario ubicado en el Complejo Mejorador de crudo. Esta replicación se realiza a través de la WAN de SINCOR.

El enfoque primario de este proyecto es proveer un plan que responda a un eventual desastre que pueda afectar severamente la operatividad del sistema SAP R/3. El objetivo es restaurar la operatividad del sistema con los datos más recientes disponibles y esto en el menor tiempo posible.

INTRODUCCIÓN

A medida que las organizaciones se han vuelto cada vez más dependientes del procesamiento de datos para manejar sus negocios y seguir siendo competitivas, la alta disponibilidad de instalaciones y sistemas que permitan el procesamiento de datos se ha vuelto crucial.

Actualmente, la mayoría de las empresas necesitan un nivel alto de disponibilidad en el procesamiento de datos. Como consecuencia, a la mayoría de los negocios les resultaría extremadamente difícil funcionar sin procesamiento de datos. Los procedimientos manuales, si es que existen, sólo serían prácticos por un corto período. Una interrupción prolongada de los servicios en un ambiente de computación puede llevar a pérdidas financieras significativas. Lo más importante es que se puede perder la credibilidad con los clientes y, como consecuencia, la participación en el mercado. En algunos casos, esas pérdidas pueden llevar el negocio al fracaso total.

Si bien el seguro de la empresa puede cubrir los costos materiales de los activos de una organización en caso de desastre, no servirá para recuperar el negocio, al igual que no ayudará a conservar a los clientes y, en la mayoría de los casos, no proporcionará fondos por adelantado para mantener funcionando el negocio hasta que se haya recuperado. Por lo tanto, la capacidad para recuperarse venturosamente de los efectos de un desastre dentro de un período predeterminado debe ser un elemento crucial en un plan estratégico de trabajo para las organizaciones.

Debido a esta dependencia de las organizaciones en sistemas de tecnología que son vulnerables a diferentes tipos de contingencias tales como sistemas de inteligencia artificial, sistemas de información gerencial, sofisticadas redes de comunicaciones y sistemas computarizados para control de procesos, la planeación ante eventuales contingencias que pueden ser de índole natural, ambiental o incitados está tomando alta prioridad en la agenda de la gerencia de las organizaciones.

Un plan para recuperación de desastres puede definirse como cualquier proceso que es diseñado para maximizar el tiempo de operación (factor de servicio), la funcionalidad y acelerar el proceso de reanudación de los procesos de negocio. Basados en esta definición, un plan de recuperación de desastres es un conjunto de actividades diseñadas para contingencia y restauración de las funcionalidades de la organización.

Este proyecto de investigación está estructurado de forma que en el primer capitulo se plantea la importancia del desarrollo e implantación de un plan que permita la continuidad operativa con el menos impacto posible ante la ocurrencia de un desastre. En este sentido se esbozan los conceptos básicos de la recuperación de desastres a través del planteamiento de una estrategia que permite realizar la

planificación, el diseño y la implementación de una solución de recuperación de desastres que satisfaga los requerimientos de continuidad operativa del negocio.

En el segundo capitulo se describe en detalle el planteamiento del problema. En SINCOR la mayor parte de la infraestructura tecnológica se encuentra ubicada en la Sede Administrativa en Caracas, lo cual incluye al sistema SAP R/3. Debido a que en este sistema se ejecutan procesos medulares para la organización conllevó a tomar la decisión de que SAP R/3 se convirtiera, dentro del plan corporativo, en el sistema piloto para la ejecución de un plan de recuperación de desastres.

En consecuencia la organización tomó la decisión de llevar adelante la implantación de un ambiente tolerante a fallas a través de un centro de datos alternativo que permitir reanudar las funciones del negocio que pudieran afectarse como consecuencia de una falla o daño mayor en la plataforma tecnológica instalada en el *centro de datos primario* ubicado en Caracas.

De acuerdo al problema planteado referido a la implantación de un ambiente tolerante a fallas para el sistema SAP R/3 en un *centro de datos alternativo* , y en función de sus objetivos se incorpora el tipo de investigación denominado Proyecto Factible. En atención a esta modalidad de investigación, el estudio se desarrolla en tres grandes fases. En la primera de estas fases se elaborará el plan de trabajo y la estrategia para implantar el sistema de recuperación en caso de desastre mayor para el sistema SAP R/3, la segunda fase y atendiendo a los resultados de elaboración del plan se realizará la implantación de la solución propuesta y posteriormente la fase de puesta en producción.

En los siguientes capítulos se desarrolla el proceso de implantación, los aspectos técnicos de la solución propuesta para el plan de recuperación de desastres y los procedimientos de mantenimiento de la solución implantada.

CAPITULO 1: MARCO TEÓRICO

Parece razonable que cuanto más medidas preventivas se tengan, menos posibilidades habrá de que una situación termine como desastre para la organización. Sin embargo, no importa lo estricto y riguroso de estas medidas preventivas, siempre habrá riesgo de interrupción de servicios. Se puede reducir el riesgo de desastres, pero aumenta el costo de las implementaciones para mitigar las consecuencias de estas interrupciones.

Deben tomarse ciertas medidas para ayudar a prevenir desastres que afecten la organización o para minimizar su impacto cuando sean inevitables. La mejor manera de determinar cuáles medidas se deben adoptar es realizar un análisis de riesgo para determinar dónde se encuentran las áreas más vulnerables.

Por lo general, las medidas preventivas mínimas son los buenos procedimientos de recuperación en el sitio para ayudar a evitar que los problemas de rutina se conviertan en desastres. Esto requiere, por ejemplo, repuestos de hardware, respaldos periódicos y un personal de operaciones capacitado. Además, puede ser necesario considerar factores como el refuerzo de la protección física de las instalaciones, mejoras en la protección contra incendios, control riguroso de acceso y otros procedimientos de operación y políticas empresariales. El tiempo y el costo implicados en la implantación y acatamiento de esas medidas pueden justificarse a través de la comparación con el tiempo y el costo implicados en el enfrentamiento de la situación al momento del desastre.

1.1 Características, planeación e implantación de una solución de recuperación de desastres

El desarrollo de un Plan de Recuperación de Desastres y de Continuidad del Negocio, es básicamente un plan de contingencia contra desastres informáticos, cuyo objetivo es mantener operativas las actividades de la empresa, aunque no es su objetivo primordial el mantener operativa la infraestructura tecnológica.

Un plan de contingencia bien concebido debe contar con la aprobación de los protagonistas principales, ser flexible, tener procesos de mantenimiento, ser efectivo en costos, concentrarse en la continuidad del negocio, permitir una respuesta organizada, asignar responsabilidades específicas e incluir un programa de pruebas. Algunas características claves son las siguientes[1]:

[1] Myers, Kenneth N. (1996). *Total Contingency Planning for Disaster, pág. 41*

- **Aprobación**

El plan debe ser aceptado y entendido por auditores internos y externos, gerentes generales y usuarios claves. Se debe diseñar y elaborar de acuerdo con las necesidades del negocio.

- **Flexibilidad**

El plan debe consistir en una guía, más que entrar en detalles relacionados con situaciones específicas de situaciones de desastres.

- **Mantenimiento**

Es necesario evitar detalles innecesarios de manera que el Plan de Recuperación de Desastres pueda ser fácilmente actualizado.

- **Efectividad en Costos**

La planeación del proyecto debe enfatizarse en la necesidad de minimizar los costos de desarrollo, implantación, procesamiento de backups, mantenimiento y pruebas.

- **Continuidad del Negocio**

El plan debe asegurar la continuidad de las actividades vitales de la empresa durante el período de recuperación de desastre.

- **Respuesta Organizada**

El plan debe proveer un "*checklist*" con una serie de puntos que necesitan atención inmediata una vez ocurrido el desastre. Este debe incluir lista de teléfonos y direcciones de personas a ser contactadas.

- **Responsabilidades**

Las responsabilidades de cada actividad que requiera atención durante la respuesta a la emergencia y durante el ínterin estas deben ser asignadas a individuos específicos.

- **Pruebas**

El plan debe establecer la frecuencia de pruebas y documentar la metodología de de las mismas, debe incluir pruebas con los usuarios y revisión de procedimientos de backups.

Como en cualquier proyecto de diseño, un método estructurado ayuda a asegurarse de que se toman en cuenta todos estos factores y de que se les trata adecuadamente.

1.2 Tipos de desastres

Aunque todas las organizaciones están propensas a la ocurrencia de desastres tales como sabotaje, algunas adicionalmente están sujetas a desastres directamente

relacionados con el tipo de negocio y el ambiente en el cual se desarrollan sus actividades.

Los desastres locales son eventos limitados a un área, cuarto o lugar específicos de un edificio. Un desastre es un tipo de incidente causado por eventos naturales, relacionados con el ambiente o inducido,

Aunque es imposible proporcionar una lista completa de todos los tipos de desastres, pueden identificarse varias categorías A continuación se muestra una lista de los diferentes tipos de desastres, clasificados en primer lugar por evento[2] y luego por localidad de ocurrencia:

1.2.1 Clasificación de desastres en base a evento

1.2.1.1 Causado por eventos naturales

- Inundación
- Incendio
- Huracán y tornado
- Fuego

1.2.1.2 Causado por eventos relacionados con el medio ambiente

- Accidente aéreo
- Explosión
- Contaminación localizada
- Derrame de sustancias tóxicas
- Falla en el servicio de comunicación telefónico
- Falla en el suministro de energía eléctrica
- Huelga general
- Motín y saqueo
- Filtración de agua

1.2.1.3 Causado por eventos incitados

- Incendio provocado
- Sabotaje
- Vandalismo
- Ataque terrorista

[2] Myers, Kenneth N. (1996). *Total Contingency Planning for Disaster, pág. 27*

1.2.2 Clasificación de desastres por localidad de ocurrencia

1.2.2.1 Desastres locales

Son eventos limitados a un área, cuarto o lugar específicos de un edificio (por ejemplo, la sala de computación). Este tipo de desastre puede ser resultado de:

- Inundación
- Incendio
- Falla irreparable del equipo
- Sabotaje
- Falla en el suministro de energía eléctrica

1.2.2.2 Desastres en el sitio

Son aquellos que afectan a todo el edificio y pueden ser causados por eventos como:

- Inundación
- Bomba
- Explosión de gas
- Incendio
- Daño de trasformadores de electricidad

1.2.2.3 Desastres de área

Estos por lo general afectan la zona donde se localiza el edificio. Esta zona puede cubrir un radio de varios kilómetros y pueden ser causados por:

- Accidente aéreo
- Terremoto
- Erupción volcánica
- Huracán y tornado
- Bomba
- Ataque terrorista
- Huelga general
- Motín y saqueo
- Contaminación química o nuclear
- Epidemia

1.3 Áreas sensibles sujetas a la ocurrencia de desastres

Es importante reconocer las áreas sujetas a la ocurrencia de desastres que pudieran afectar a la empresa o ambiente de negocios. A continuación, se describe algunas de las áreas más sensibles en cualquier empresa o ambiente de negocios y que puede estar sujeta a la ocurrencia de un desastre.

1.3.1 Sistemas de computación

Dada la dependencia crítica de las organizaciones modernas en cuanto a los sistemas de información computarizados, es claro que la perdida de la capacidad de procesamiento por un largo periodo puede ser extremadamente crítico para la continuidad operativa de la empresa. Los sistemas informáticos juegan un papel clave para muchas organizaciones en términos de procesamiento, nómina y pagos a proveedores, control de procesos, manejo de inventarios, facturación, contabilidad, etc. En consecuencia deben existir en sitio procedimientos de seguridad física y de los datos que ayuden a prevenir o mitigar la ocurrencia de un desastre. Adicionalmente, puede ser necesario un plan más extenso que permita la continuidad del negocio, esto tomando como base la naturaleza y complejidad del negocio y de la dependencia de sus operaciones de los sistemas de computación.

1.3.2 Sistemas de comunicación de datos

El intercambio de datos electrónicos está en constante incremento y es usado por clientes para introducir órdenes de compra, verificar el status de cualquier orden, para pagar facturas, transmisión de órdenes de fabricación y muchos otros procesos.

Por ello es importante tener un escenario separado que permita la continuidad del negocio ante la ocurrencia de un desastre que por su naturaleza ocasione la pérdida de comunicación remota de data por un largo periodo de tiempo. Otra razón para mantener un plan que permita la continuidad de las operaciones sin la existencia de comunicación remota de datos es la utilidad que esto puede tener al momento de la ocurrencia de un desastre que involucre adicionalmente los sistemas informáticos ya que las operaciones de estos sistemas son generalmente restaurados en un periodo de 2 semanas y puede llevar mucho más tiempo la reconstrucción de toda la red de comunicaciones. Con esto las unidades remotas pueden tomar ventaja de la restauración de los sistemas aun cuando las líneas de comunicación no estén operativas.

1.3.3 Comunicaciones de voz

La mayor parte de las personas son más dependientes de lo que se imaginan de los sistemas de comunicación de voz, así como de sofisticados sistemas de telefonía computarizada que adicionalmente los hace más vulnerables. La comunicación telefónica es crítica para procesos de mercadeo, servicio a clientes, comunicaciones internas, y contacto con proveedores. En las grandes metrópolis se experimenta constantes fallas en los sistemas de telefonía y en estos ambientes se requiere algún tipo de plan para la continuidad operativa en caso de interrupción del servicio telefónico por largos periodos de tiempo.

1.3.4 Estructuras e instalaciones vitales

¿De qué manera pueden continuar las operaciones si importantes instalaciones son destruidas o no pueden ser accedidas por largo periodos de tiempo? En este caso la pérdida de las actividades primarias es la preocupación, ya que oficinas, almacenes, centros de distribución y producción constituyen las áreas donde se desarrollan las actividades vitales de las organizaciones. Por ejemplo el departamento de bomberos, agencia de salud, o cualquier otra pudiera ordenar la cuarentena de un edificio debido a problemas estructurales como resultado de derrame de sustancias peligrosas, contaminación, etc.

1.3.5 Operaciones de salvamento en el sitio de desastre - centro de datos primario

Los esfuerzos iniciales deben enfocarse en proteger y preservar los equipos de computación. En particular almacenamientos de datos magnéticos (Disco duro, cintas, disquetes, CD). Estos deben ser identificados y protegidos en sitio seguro, lejos del lugar de desastre.

Al mismo tiempo debe realizarse una evaluación de la escena del desastre a fin de estimar el monto de tiempo requerido para volver a restituir la operatividad del centro de datos primario. Sobre la base a este análisis debe tomarse la decisión de usar el sistema instalado en el centro de datos secundario y en éste pueden ser restauradas temporalmente las funcionalidades hasta tanto sean restituidas las operaciones en el centro de datos primario.

1.3.6 Adquisición y re-ensamblaje de nuevos equipos

Se requiere el reemplazo de aquellos equipos que no pudieron ser recuperados. Para ello es necesario activar un proceso de adquisición en condiciones de emergencia, siendo necesario contactar al proveedor de hardware y activar un proceso de procura de estos equipos.

Los componentes recuperados así como los nuevos adquiridos deben ser re-ensamblados en el centro de datos primario. Debido a que todos los planes de este tipo están sujetos a cambios que ocurren en la industria de la computación, puede ser necesario que el personal involucrado en el plan de recuperación se desvíe de éste, más si el plan no ha sido actualizado. Puede ser necesario realizar sustituciones de equipos a último minuto. Una vez que el proceso de re-ensamblaje haya sido completado, el trabajo debe concentrarse en los procedimientos de recuperación de datos.

1.3.7 Recuperación de los datos a partir de backups

El proceso de recuperación de los datos debe contar con backups almacenados en un lugar fuera de los predios de las oficinas administrativas. Los backups pueden provenir de medios de almacenamiento magnéticos tales como cintas, CDs o cualquier otro medio de almacenamiento. Los primeros esfuerzos deben basarse en la restauración del sistema operativo, luego la recuperación del sistema.

1.3.8 Regreso al centro de datos primario

Una vez restauradas la operatividad del *centro de datos primario*, es necesario iniciar el proceso de restauración de data desde el *centro de datos alternativo* en este caso se requiere un proceso de recuperación a partir de backups generados en el Centro de datos secundario y que deben ser movilizados al *centro de datos primario* para su aplicación.

1.4 Método estructurado para la planificación e implementación de un plan con capacidad de recuperación de desastres

1.4.1 Determinación de los requerimientos del negocio[3]

El primer paso en el desarrollo de una solución de recuperación de desastres para los recursos de *procesamiento de datos* es determinar exactamente lo que requiere el negocio. Para lograr esto, debe hacerse un análisis de riesgo y un análisis de impacto en el negocio para determinar cuáles son los requerimientos de éste. Muchos procesos del negocio son tan dependientes del *procesamiento de datos* que ya no se pueden realizar en caso de un desastre. Estos procesos deben evaluarse por su impacto negativo; es decir, pérdida del negocio y de los ingresos del mismo.

Este análisis indicará cuáles son sus prioridades de proceso del negocio y cuál es la escala de tiempo de recuperación que se requiere para cada proceso. Un desastre conlleva también riesgo de que la organización pierda la pista de algunas transacciones de negocios que hayan estado en proceso cuando ocurrió el desastre. El análisis de impacto en los negocios tendrá que determinar hasta qué grado puede tolerarse una pérdida así en cada proceso de la empresa. Los resultados pueden utilizarse en el siguiente paso para determinar los requerimientos de *procesamiento de datos*.

Los requerimientos de la empresa deben ser analizados para determinar cuál será su estrategia de recuperación de desastre. Deben considerarse dos áreas principales cuando se determinan los requerimientos:

[3] Gregor Neaga, Bruce Winters y Pat Laufman. (1997). *Prevención y Recuperación de Desastres*, pág. 5

- **Tipo de riesgo al que es vulnerable la organización**

No todas las organizaciones se enfrentan a los mismos riesgos en la misma medida. Por ejemplo, algunos edificios corren más riesgos de ser presa del fuego que otros. Algunas áreas son vulnerables a los terremotos, otras a las inundaciones. Un análisis de riesgo puede ayudar a determinar estas exposiciones.

- **Tiempo que puede soportar la organización**

¿Cuánto tiempo pueden soportar las funciones vitales de la empresa la ocurrencia de una interrupción del servicio?
Un sistema de facturación de una empresa de servicios públicos, como el que imprime el recibo de luz o de teléfono, tal vez pueda tolerar una interrupción de servicio de varios días sin poner en riesgo negocios actuales y futuros. Para un banco, una institución del mercado de valores o un sistema de registro de pedidos por correo, una interrupción de servicio de unas cuantas horas puede ser fatal.

Un análisis de impacto en los negocios ayudará a determinar el tiempo que la empresa puede permitir que deje de funcionar su sistema. Los resultados de ambos análisis mostrarán cuáles requerimientos del negocio debe afrontar la solución de recuperación.

1.4.1.1 Análisis de Riesgos

Se suele tener la tentación de clasificar todos los procesos del negocio como muy importantes y de exigir las mejores opciones de recuperación posibles para todos ellos. Cuando se definan sus requerimientos de recursos de recuperación, debe tenerse en cuenta que puede ser considerable la inversión necesaria para proporcionar una solución viable de recuperación de desastres. Si la solución implica una recuperación de desastres en otro sitio de la empresa o se logra por contrato con un proveedor externo, tal vez sea muy alto el costo del hardware y software y de la posible construcción de un edificio. Por esta razón, es prudente limitar los requerimientos de recursos sólo a aquellos que resulten esenciales para la supervivencia del negocio.

Un análisis de riesgo debe dar como resultado lo siguiente:

- La determinación de cuáles son las medidas preventivas necesarias.
- La determinación de cuál tipo de recuperación de desastres se requiere.
- Una aceptación consciente de los riesgos no cubiertos por las dos primeras medidas.

La implementación de medidas preventivas reduce el riesgo de sufrir un desastre y, si éste ocurre, puede minimizar su impacto, mientras que implementar una estrategia de recuperación de desastres provee protección contra riesgos no cubiertos por !as medidas preventivas.

Sin embargo, en algunos casos, puede haber riesgos que una organización decida, conscientemente, no cubrir en su estrategia de recuperación de desastres.

Por ejemplo, un laboratorio y su centro de procesamiento de datos podrían estar situados en las mismas instalaciones. Si ocurre un desastre y se limita al centro de datos, entonces se ejecutará el plan de recuperación y el procesamiento se restablecerá en un centro de datos alterno. Sin embargo, si todo el edificio (incluyendo el laboratorio) se destruye, no se ejecutará plan alguno. La organización ha elegido no proporcionar un edificio alterno, puesto que no se necesitaría procesamiento de datos sin el laboratorio.

Se puede hacer determinaciones de recuperación como éstas, relacionadas con la empresa, haciendo análisis de riesgo y análisis de impacto en el negocio.

1.4.1.2 Áreas de análisis de riesgos de un desastre

La realización de un análisis de riesgo muestra los puntos débiles de una organización que podrían llevar a la pérdida de activos y de funciones vitales de la empresa.

Para minimizar de manera congruente el impacto de un desastre, debe ser realizado un estudio a fondo, además de llevarse a cabo revisiones periódicas, para así determinar el riesgo de varías categorías de desastres que ocurren en el área (o en un tipo particular de empresas) y el grado en que esos desastres afectarán a la empresa. Esto determinará entonces el riesgo de cada categoría de desastre que afecte a su operación de procesamiento de datos.

El análisis de riesgo debe incluir (pero no estar limitado a) las siguientes áreas:

- **Seguridad física**

Los temas relacionados con el edificio o con las propias instalaciones, como prevención de intrusiones y especificaciones del edificio de prevención de incendios y de seguridad de la estructura.

- **Seguridad de los datos**

Los procedimientos aplicados para asegurar la integridad de los datos de los sistemas de información en toda la organización.

- **Empleados disgustados**

Prácticas y procedimientos diseñados para neutralizar posibles acciones negativas por parte de empleados que se encuentren a disgusto con la empresa. Entre esas prácticas debe incluirse la de acompañar a los empleados afuera del edificio inmediatamente después del despido.

- **Sistemas de respaldo y recuperación**

Un análisis de los procedimientos de respaldo y recuperación que se aplican actualmente para proteger los datos y los componentes de hardware vitales para la función de procesamiento de datos de !a empresa.

- **Vulnerabilidad de la infraestructura**

Este análisis cubre temas como fuentes redundantes de energía eléctrica, fuentes ininterrumpibles de poder (UPS), líneas telefónicas de entrada y suministros de agua.

- **Ubicación del centro de datos**

Se concentra en la ubicación física del centro de datos dentro del edificio, además de la ubicación del propio edificio, para determinar desastres a los que tal vez sea muy vulnerable el centro de datos, como inundaciones o terremotos. Si el propio edificio se encuentra en un área vulnerable a las inundaciones, entonces el centro de datos no debe estar ubicado en el sótano.

- **Habilidades claves**

Es necesario determinar si la organización depende de habilidades o de individuos clave específicos y si un desastre puede acarrear la pérdida de esos individuos. Debe tomarse en consideración la necesidad de crear duplicados de esas habilidades con capacitación, educación, y la implementación de procedimientos y documentación de gran amplitud.

El resultado del análisis puede expresarse como una tabla que muestra la probabilidad de cada amenaza y la duración de la interrupción potencial de servicio que puede provocarse. Con esa tabla, la administración puede tomar una decisión consciente sobre el alcance de falla que van a cubrirse y, lo más importante, sobre los que no se van a cubrir.

Con base en los resultados, podría tomarse una decisión de alto nivel para la protección contra "desastres locales", pero no contra desastres regionales o nacionales.

No hay una estrategia práctica o económicamente sustentable de recuperación de desastres que pueda proteger contra todas las amenazas posibles. Por ejemplo, la mayor parte de las organizaciones implementarán una estrategia que proteja contra desastres locales, pero pocas cubrirán desastres nacionales o incluso internacionales. Asimismo, las organizaciones que cuentan dos o más operaciones de procesamiento de datos pueden tener una estrategia de recuperación que funcione en caso de que un sitio sea destruido, pero no si varios sitios son destruidos al mismo tiempo.

Como consecuencia, siempre se tiene que tolerar algún riesgo residual. La decisión sobre el alcance del desastre para el que habrá de prepararse debe tomarse en los más altos niveles de la empresa. El riesgo residual específico debe documentarse de manera explícita y aceptarse conscientemente.

Si bien es económica y funcionalmente imposible proteger a una empresa contra todos los riesgos concebibles, es esencial tener un amplio plan de rescate que asegure la pronta recuperación de una interrupción inevitable del servicio.

Además del impacto para el negocio, hay varias razones más por las que se decida que no vale la pena arriesgarse. Éstas van desde presiones externas hasta políticas internas. Las presiones externas pueden venir de auditores externos, de la prensa y de organismos de regulación como instituciones gubernamentales. Entre las políticas internas se incluyen elementos como auditores internos, políticas empresariales y sindicatos.

1.4.1.3 Análisis de los procesos del negocio

La otra parte de la comprensión de los requerimientos del negocio para recuperarse de los efectos de un desastre, es determinar el impacto de una interrupción de servicio en los procesos de negocios. Antes de analizar las consideraciones que habrán de tomarse en cuenta al analizar los procesos de negocios, se debe hacer la distinción entre un proceso de negocios y una aplicación.

Un proceso de negocios se refiere a un grupo de actividades interrelacionadas que dan sostén a la operación exitosa de la empresa o de sus servicios. Una aplicación se refiere al conjunto de tareas interrelacionadas de *procesamiento de datos* o de sistemas en línea diseñados para dar soporte a los procesos de negocios. Por ejemplo, una línea aérea tal vez tenga una aplicación de procesamiento de datos llamada "reservaciones". Dentro de esta aplicación puede haber varios procesos como la expedición de boletos, las escalas de los viajes, el abordaje, etc.

En algunos casos, tal vez un proceso de negocios necesite el apoyo de más de una aplicación. Inicialmente, tal vez sólo se recuperen los procesos de negocios más vitales. ¿Pero cuáles son los procesos vitales? ¿Y qué tan vital es lo vital? ¿Son servicios que deben recuperarse en horas o la interrupción de servicio puede prolongarse a días? Además, aunque algunos servicios tal vez toleren interrupciones de servicio más largas, todos los servicios tienen que recuperarse en algún momento. Así que, ¿en qué orden deben hacerlo? Estas preguntas pueden responderse si se realiza un análisis de impacto en los negocios.

El análisis de los procesos del negocio debe definir:

- Cuáles procesos del negocio deben incluirse en el alcance de una recuperación.
- El costo (en dinero, pérdida de ingresos, de clientes, etc.) de una interrupción de servicio en cada proceso del negocio.
- La máxima interrupción de servicio permisible para cada proceso del negocio.
- La prioridad de recuperación para los procesos del negocio
- La dependencia entre los procesos del negocio.
- El nivel de las transacciones irrecuperables que será aceptable para cada unidad de negocios en el caso de un desastre.

Como en el caso del análisis de riesgo, el análisis de impacto en negocios puede hacerse mediante un estudio formal para determinar con exactitud los diferentes impactos en todas las funciones de la empresa. Sin embargo, en muchas organizaciones la alta gerencia está bien consciente de cuáles funciones o procesos del negocio son críticos para la supervivencia de la empresa. En el caso de un sistema de mediana capacidad que pueda recuperarse por completo en 24 horas, la dirección decidirá probablemente restablecer todo el sistema en lugar de tomarse el tiempo y la molestia de desarrollar un análisis a fondo de impacto en negocios.

1.4.2 Determinación de los requerimientos de procesamiento de datos

Cuando se han terminado el análisis de riesgo y el análisis de impacto en el negocio, se debe tener toda la información necesaria para determinar los requerimientos de recuperación para las funciones vitales de la organización. Ésta debe trasladarse ahora de un contexto de negocio a un contexto de procesamiento de datos, con el fin de determinar cuáles procedimientos y recursos son necesarios para dar soporte a la recuperación y al procesamiento normal en el sitio de la recuperación[4].

Necesitan tomarse en consideración dos tipos de procesos de *procesamiento de datos*.

- Las aplicaciones que actualmente conforman los procesos del negocio.
- Los procesos de infraestructura en la administración de sistemas de procesamiento de datos que se requieren para ejecutar y dar soporte a las aplicaciones de los procesos del negocio.

1.4.2.1 Asociación de los requerimientos del negocio con las aplicaciones

Aunque el propósito de la recuperación de desastres es restablecer los procesos del negocio, en la práctica la recuperación del *procesamiento de datos* se relaciona con la restauración de aplicaciones. Para diseñar una solución apropiada de recuperación de desastres, primero es necesario identificar los requerimientos de recuperación para las aplicaciones y los datos vitales.

El departamento de *procesamiento de datos* da soporte a los procesos del negocio - con su arquitectura, recursos (hardware, software y personal) y operación del procesamiento de datos. Una vez que se han determinado los requerimientos de recuperación del negocio, la administración debe identificar las relaciones entre los procesos del negocio, las aplicaciones y los datos para el ambiente de procesamiento de datos.

[4] Gregor Neaga, Bruce Winters y Pat Laufman. (1997). *Prevención y Recuperación de Desastres, pág. 11*

Los requerimientos para recuperar una aplicación y sus datos son los mismos requerimientos para la recuperación del proceso del negocio al que da soporte. Si un proceso del negocio tiene una máxima interrupción tolerable de servicio de 12 horas, entonces las aplicaciones y los datos que dan soporte a ese proceso del negocio deben restablecerse y recuperarse en 12 horas o menos. Si un proceso del negocio sólo puede aceptar una pérdida de transacciones de hasta una hora antes del desastre, entonces las aplicaciones asociadas deben recuperarse de manera que aseguren que la pérdida de datos sea de menos de una hora.

Una vez que se han determinado los requerimientos de recuperación de aplicaciones y que se ha evaluado la interdependencia entre las aplicaciones y sus datos, el resultado es un inventario de aplicaciónes, esto documenta los requerimientos de recuperación de las aplicaciones: con cuánta rapidez debe recuperarse cada una, los recursos requeridos para recuperar y ejecutar la aplicación (incluyendo los requerimientos de disco, procesador, red e impresión) y las interdependencias con otras aplicaciones y datos.

1.4.2.2 Procesos de administración de sistemas

Terminado el inventario de aplicaciones, deben identificarse también todos los procesos de infraestructura del *procesamiento de datos* que se necesiten para ejecutar y dar soporte a las aplicaciones del negocio. A menudo se hace referencia a estos procesos de infraestructura como *procesos de administración de sistemas* o *procesos de administración de instalación*, y se los utiliza para controlar y administrar todos los aspectos operacionales clave de una instalación de *procesamiento de datos*, como cambios, problemas, capacidad, rendimiento y seguridad.

Estos procesos y sus procedimientos y herramientas asociados deben analizarse para evaluar cuáles se requieren para ejecutar y dar soporte a las aplicaciones del negocio, a los niveles de servicio requeridos. Todos los componentes esenciales necesitan definirse y aprobarse como un requisito para la fase de diseño de la solución. La regla básica es que si un componente es necesario para ejecutar o dar soporte a una aplicación del negocio en el sitio principal, entonces debe duplicarse en el sitio de recuperación. En la práctica, la mayoría de estos componentes (si no es que todos) son datos, y por lo tanto realmente se trata de asegurar que se respalden y restablezcan junto con todos los demás datos vitales.

1.4.2.3 Acuerdos de nivel de servicio para recuperación de desastres

Como parte del proceso de analizar los requerimientos de recuperación y de decidir una estrategia de recuperación de desastres, es importante que los usuarios de procesos vitales del negocio estén de acuerdo con el nivel de servicio que habrá de prestarse como resultado de la estrategia seleccionada. Se recomienda que esto se documente en los acuerdos de nivel de servicio existentes, o que se creen nuevos acuerdos, si no los hay.

Los acuerdos de nivel de servicio describen el alcance del servicio, el rendimiento y la infraestructura que habrá de prestar el procesamiento de datos. En relación con la recuperación de desastres, los acuerdos de nivel de servicio deben contener declaraciones sobre:

- Aplicaciones disponibles en el procesamiento de respaldo de desastres.
- Aplicaciones no disponibles en el procesamiento de respaldo de desastres.
- Máxima duración de la interrupción de servicio de la aplicación.
- Máxima duración de la interrupción de servicio de la conectividad de red.
- Máxima pérdida de datos.
- Tiempos en línea y de respaldo de las aplicaciones disponibles.
- Rendimiento esperado y tiempos de respuesta.
- Divisiones y departamentos conectados en red, velocidad de línea y capacidad.
- Servicio de impresión: tiempos de envío de salida, capacidad, procedimientos
- Limitaciones y aclaraciones de responsabilidad.
- Contabilidad: cómo se les registra a los departamentos el cargo contable por respaldo de desastres.

Los acuerdos de nivel de servicio deben revisarse periódicamente. Los cambios en la estrategia de recuperación de desastres y en la solución técnica afectarán al servicio que habrá de prestarse.

1.4.3 Diseño de la solución de respaldo y recuperación

Una vez que sean aceptados los requerimientos de procesamiento de datos, todo se encuentra listo para desarrollar un boceto o diseño de la solución final, de la misma manera en que un arquitecto dibuja un boceto o construye la maqueta de un edificio.

El diseño del plan de recuperación de desastres describe, en términos amplios, las características generales y los elementos principales de la solución que se pretende. Estos elementos aparecen en la lista que se muestra a continuación y se analizan en las siguientes secciones[5]:

- Alcance de la recuperación
- Estrategia de pruebas
- Procesos de respaldo y recuperación de datos
- Administración y operación del sitio alterno
- Descripción de la configuración de recuperación

El nivel de detalle en el diseño dependerá de su propósito. Si el objetivo en este punto es estimar el costo de una o más soluciones potenciales, tal vez no se necesiten estos niveles de detalle. Si, por otra parte, ya se ha decidido por una

[5] Gregor Neaga, Bruce Winters y Pat Laufman. (1997). *Prevención y Recuperación de Desastres*, pág. 14

solución y se está elaborando un diseño final listo para la implementación, se necesitará mucho más detalle.

1.4.3.1 Alcance del plan de recuperación

El diseño del plan de recuperación de desastres debe definir claramente el alcance de la recuperación, es decir, qué es lo que se esta recuperando y dentro de qué periodo. Esto tiene el objetivo de asegurar desde el principio que no haya confusión entre lo que es y lo que no es parte del diseño de recuperación. La definición del alcance debe incluir:

- La suposición de cuáles tipos de desastre se incluyen y se excluyen
- La secuencia en que las aplicaciones se recuperarán
- El tiempo máximo de recuperación para cada aplicación
- Los datos que se recuperarán
- La actualidad de los datos una vez que se recuperen

Esta información se basará en el análisis de riesgos y en los requerimientos de aplicación.

1.4.3.2 Estrategia de pruebas

En esta etapa es útil determinar, de forma muy general, cómo se efectuará la prueba, porque esto puede influir en la complejidad y el costo de la solución propuesta. Es adecuado responder preguntas como las expuestas a continuación:

¿Dónde tendrá lugar la prueba?
¿Qué recursos se necesitarán?
¿Puede probarse la red de producción?
¿Es necesario eliminar otras cargas de trabajo o de datos durante la prueba?

Tal vez parecería que probar es más fácil cuando el sitio de recuperación es un segundo sitio propiedad de la compañía. La compañía es la propietaria y es quien administra ambos sitios y, por lo tanto, debería de ser más fácil planear y coordinar.

En la práctica, suele ser difícil probar en este ambiente, debido a las necesidades de deshacerse de cualquier carga de trabajo que ya se esté ejecutando en el procesador de recuperación y, posiblemente, de respaldar los datos. Así ocurre especialmente en los casos en que el procesador de recuperación normalmente ejecuta una parte vital de la carga de trabajo, pero es difícil incluso encontrar momentos adecuados para hacer a un lado cargas de trabajo menos vitales. Y aun cuando esto sea posible, a menudo el tiempo de prueba se alarga por la necesidad de respaldar los datos en el disco y restaurarlos después de la prueba. Realizar la prueba en un segundo sitio suele resultar en que se ejecuten pruebas con menos frecuencia o que no sean tan completas como sería lo ideal.

Cuando hay suficientes recursos de reserva en el sitio de recuperación o cuando la carga de trabajo puede desplazarse fácil y rápidamente, este problema se elimina. En este caso, la prueba en casa por lo general es muy efectiva.

Cuando se utiliza un sitio comercial con todos los recursos necesarios para las pruebas de recuperación, la prueba necesita programarse con el proveedor de servicio. La competencia con otros clientes tal vez signifique que las pruebas tengan que programarse con mucha anticipación. Por otra parte, una vez que se ha convenido el periodo de prueba, ésta tiene que ser muy eficiente porque todos los recursos estarán listos y a su disposición de principio a fin.

1.4.3.3 Procesos de respaldo y recuperación de datos

Para poder definir la configuración de recuperación requerida, es necesario determinar los procesos para respaldar y recuperar los datos vitales. Los métodos utilizados para respaldar los datos, la forma en que se transporten y almacenen fuera del sitio y las técnicas de recuperación de datos, influyen en los recursos físicos requeridos en el sitio alterno y en la interconexión entre sitios.

La complejidad y volatilidad de los datos los convierte en el recurso más difícil de manejar durante la recuperación. Mientras la naturaleza relativamente estática del hardware y de las instalaciones permite que los sitios estén listos antes de que la recuperación sea necesaria, la naturaleza volátil de los datos significa que deben manejarse como un proceso continuo. Los datos se mantienen al corriente en un sitio de recuperación o tienen que ser puestos al corriente como parte del proceso de recuperación. Por consiguiente, uno de los componentes clave del diseño del plan de recuperación de desastres es la estrategia de respaldo y recuperación de datos; es decir, cuáles datos se respaldarán, con qué frecuencia y de qué manera, y cómo habrán de recuperarse y en qué orden.

Aunque los procedimientos para el respaldo y la recuperación son piezas del diseño lógicamente separadas, no pueden diseñarse por separado porque están estrechamente vinculadas.

En la siguiente sección se analizan los factores que influirán en las decisiones sobre las técnicas y momentos oportunos del respaldo y la recuperación.

1.4.3.4 Categorías de datos

Cuando se analizan las técnicas para el respaldo y la recuperación de datos, es útil agruparlos en categorías con base en su uso y su volatilidad. Al menos hay tres categorías generales de datos asociadas con un sistema de computación: *datos de aplicación*, *datos de infraestructura* y *datos de sistema*. Es necesario comprender la naturaleza de los datos en cada una de esas categorías para elaborar un plan eficaz de recuperación de desastres.

- **Datos de la aplicación**

Aquí se incluyen todos los datos pertenecientes a las aplicaciones (bases de datos, archivos de trabajo, programas, etc.) que deben estar presentes para que las aplicaciones se ejecuten. En un desastre, todos estos datos necesitan recuperarse o volverse a crear para permitir la recuperación de la aplicación.

- **Datos de infraestructura**

En esta categoría, se incluyen los datos del subsistema que dan soporte a las aplicaciones, como los sistemas de administración de base de datos, los catálogos, y los datos de control de acceso y sistemas de seguridad. Por lo general estos datos están sujetos a cambios frecuentes.

A este tipo de datos se les ve con frecuencia como datos del sistema; sin embargo, normalmente son más volátiles que los datos del sistema y están relacionados de manera más cercana con los datos de la aplicación. Es útil tratarlos por separado desde el punto de vista del respaldo y la recuperación.

- **Datos de sistema**

Entre éstos se incluyen la plataforma del sistema y los archivos afines necesarios para la carga de un programa inicial, o el "inicio" de un sistema operativo. Consisten en el software del sistema elaborado para la configuración específica de una máquina. Estos datos por lo general están sujetos a pequeños cambios entre nuevas versiones o actualizaciones del sistema. Son el tipo de datos que se vuelve a crear con más facilidad.

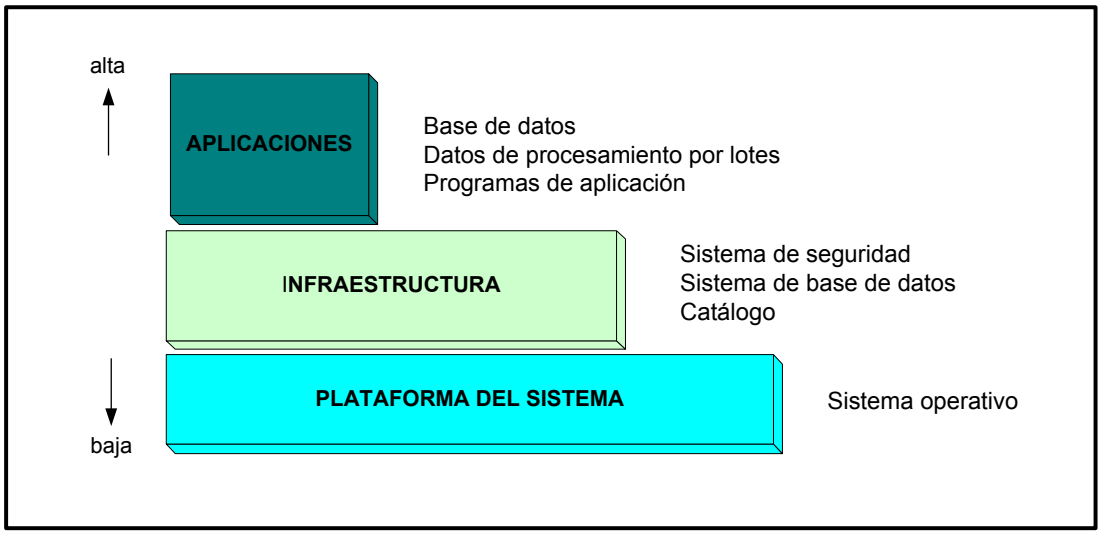

FIGURA - 1.1 CATEGORÍAS DE DATOS

1.4.3.5 Opciones de respaldo de datos

La recuperación de datos por lo general consiste en la restauración de una copia de los datos y en la aplicación de cualquier actualización necesaria. La mayoría de las instalaciones utilizan esos procedimientos de respaldo y recuperación hoy en día dentro de su sitio principal, para el propósito de una recuperación interna. Cuando los datos tienen que restaurarse en un centro de datos secundario se aplican consideraciones adicionales, tales como, que el hardware en ambos sitios tiene que ser compatible y los datos de respaldo deben sacarse del sitio rápidamente Los procedimientos de respaldo de datos no deben tener demasiado impacto en las operaciones normales.

- **Copias al momento**

Las copias al momento respaldan los datos tal como están en un momento específico. Tradicionalmente, esto ha significado detener la aplicación y el sistema de administración de base de datos (DBMS) para que no puedan realizarse actualizaciones, copiar los datos y reiniciar la aplicación y el DBMS. Las copias al momento por lo general se utilizan para respaldos periódicos.

- **Copias en línea**

El respaldo de datos debe realizarse con una interrupción mínima o sin interrupción de servicio en el centro de datos principal. Para lograr esto, ahora muchos DBMS proporcionan servicios que respaldan los datos estando la base de datos en uso. La copia producida por estos servicios no es consistente por sí misma. La recuperación implica restaurar esta copia y aplicarle todas las actualizaciones que se hayan hecho durante el proceso de respaldo. Este procedimiento crea una copia consistente. La limitación de este método es que, debido a que la base de datos recuperada está actualizada hasta cierto momento después del final de la operación de copia, es difícil sincronizarla con respaldos de otros archivos o bases de datos.

Algunos productos utilizan una combinación de técnicas de software y hardware para crear una copia consistente de los datos en un momento determinado como se veían al principio de la operación de copia, permitiendo que a la vez se hagan actualizaciones de los datos. Esta técnica es más adecuada cuando se necesitan sincronizar varios respaldos.

- **Copias incrementales**

Las copias incrementales son aquellas en que sólo se copian las partes de los datos que han cambiado. Estas copias sólo son útiles cuando se utilizan junto con una copia anterior completa de los datos. Las copias incrementales se utilizan para reducir el tiempo de copia. Sí sólo ha cambiado una pequeña porción de los datos, las copias incrementales pueden resultar útiles. Sin embargo, cuando han cambiado partes considerables de los datos, las copias incrementales tal vez tomen más tiempo que una copia completa.

- **Copias de datos de registro del sistema de administración de base de datos**

Los datos de registro son una recolección de todas las actualizaciones hechas a una base de datos. Estas actualizaciones las hace el sistema de administración de base de datos (DBMS) escribiéndolas en un archivo. Cuando este archivo está lleno, el DBMS empieza a escribir las actualizaciones en otro archivo de registro. A este proceso se le llama a menudo *cambio de registro*. Una vez que ocurre el cambio, el archivo de registro completo se copia a otro archivo llamado *registro de archivos*.

- **Transporte de datos y almacenamiento seguro**

El método más común de transferencia de datos para la recuperación de desastres del sitio principal a un sitio alterno, es copiar los datos a un cartucho de cinta o CD-ROM y transportarlo manualmente. Estos datos por lo general se llevan a un proveedor de almacenamiento fuera del sitio, no al sitio alterno.

Este procedimiento resulta apropiado en muchos casos. Sin embargo, como ha aumentado la presión para reducir los tiempos de recuperación, evitar la pérdida de datos y facilitar la administración de los datos, muchas empresas han empezado a transferir los datos electrónicamente.

La decisión de utilizar transporte manual de cintas, conexión procesador a procesador, dispositivos remotos o espejeo de discos depende de varios factores, entre los que se incluyen:

El tiempo de recuperación establecido: Mientras más corto sea el tiempo de recuperación requerido, más actualizados deberán mantenerse los datos. El concepto de actualización o preparación de datos se analiza en "Disposición del sitio alterno", más adelante.

La cantidad de los datos que habrá de transferirse: El ancho de banda de las comunicaciones entre los sitios puede ser de alto costo si necesitan transferirse grandes cantidades de datos.

La pérdida de datos permisible: La transferencia electrónica de datos permite que los datos se muevan fuera del sitio más rápidamente que un transporte manual de cinta. Si habrá de minimizarse la pérdida de datos, tal vez no sea adecuado el transporte manual de la cinta.

Cuando los datos se transfieren físicamente entre sitios o a un almacén fuera del sitio, debe tenerse cuidado para asegurar un manejo estricto. Esto es para salvaguardar la pérdida de datos vitales y mantener seguros los datos confidenciales. Los datos transmitidos electrónicamente, por lo general, son más fáciles de manejar y de salvaguardar. Si habrán de transferirse datos confidenciales a través de las líneas de comunicación, deben considerarse las técnicas de encriptación.

1.4.4 Selección de los productos adecuados para el diseño

Una vez elaborado un diseño de la solución de recuperación de desastres, se puede seleccionar los productos que se requieren para implementar la solución y es en este momento cuando se podrá estimar el costo de la recuperación para la organización.

El diseño de la recuperación de desastres que se ha desarrollado hasta este punto es un diseño lógico. Describe la forma en que funcionará la solución de recuperación, pero no incluye una especificación exacta sobre los componentes que la conforman. La selección de productos se excluye intencionalmente del diseño para permitir que el diseño inicial se determine por los requerimientos del usuario y no por las capacidades de los productos. Éste es un principio de diseño importante.

Sin embargo, a menudo resulta práctico desarrollar el diseño inicial con algún conocimiento de los productos disponibles, para evitar que sea requerida una función para la que no existe un producto o para la que el producto tiene restricciones operacionales. Cierto conocimiento de las capacidades de los productos disponibles asegura que el diseño resultante será práctico.

1.4.4.1 Selección de productos

La selección de productos es el proceso de elegir un conjunto de productos que pueden utilizarse en combinación para permitir la implementación del diseño de recuperación de desastres. Un producto en este contexto es cualquier componente de la solución que necesita comprarse o desarrollarse. El hardware y el software son productos, igual que el sitio alterno o el servicio de recuperación que se planea utilizar y el personal requerido para desarrollar y operar la solución[6].

En algunos casos, habrá una función requerida por el diseño que sólo un producto disponible la realice. En otros casos tal vez no haya productos que cumplan exactamente con los requerimientos. Cuando ocurre esto, será necesario evaluar los requerimientos para determinar si la función debe efectuarse internamente o eliminarse, o si el diseño necesita rehacerse. Como se mencionó anteriormente, debe evitarse esta situación en las funciones importantes del diseño, esforzándose por incluir únicamente funciones que se sabe que se encuentran disponibles.

1.4.4.2 Selección de hardware y software

Los productos de hardware y software que se seleccionen dependerán en gran medida de la plataforma de procesamiento del sitio principal. Aunque los requerimientos funcionales para el respaldo y la recuperación son muy similares entre plataformas, varían mucho las herramientas disponibles y su funcionalidad.

Cuando se desarrollen planes para un sitio de recuperación de desastres debe asegurarse de que cualquier acuerdo contractual con proveedores de software

[6] Gregor Neaga, Bruce Winters y Pat Laufman. (1997). *Prevención y Recuperación de Desastres*, pág. 31

prevea que esos productos se restauren o ejecuten de manera continua en el sitio alterno. Algunos productos tal vez requieran licencias adicionales de software para el sitio alterno.

1.4.5 Selección y disposición del sitio alterno

1.4.5.1 Selección del sitio alterno

Elegir un tipo de sitio alterno puede ser la decisión más importante a tomar. Este sitio no necesariamente debe ser propiedad de la organización. Puede utilizarse proveedores profesionales de servicios para recuperación de desastres, o puede establecer un acuerdo con otra empresa para utilizar su equipo de procesamiento de datos en el caso de un desastre. Entre los posibles métodos se incluyen:

- **Sitio alterno propiedad de la organización**

Muchas empresas utilizan instalaciones de procesamiento de datos localizadas en varios sitios. La razón original de tener varios sitios puede ser geográfica o histórica, pero en cualquier caso, la multiplicidad de sitios de procesamiento de datos ofrece una infraestructura conveniente para dar soporte a la recuperación de desastres.

- **Servicio de recuperación por parte de una empresa externa**

Este método es parecido a los seguros; es decir, por una cuota periódica y como se especifica en un contrato, un proveedor profesional de servicio de recuperación proporcionará recursos para recuperación de desastres si surge la necesidad. Estas instalaciones por lo general son compartidas por varios suscriptores.

Este método resulta mucho más barato y permite la utilización del soporte técnico y administrativo, además de las habilidades de coordinación del proveedor de servicios. Muchos proveedores de servicios de recuperación ofrecen servicios móviles, además de los tradicionales sitios "fijos". Estos servicios móviles de recuperación varían desde un acuerdo para llevar equipo PC hasta un ambiente de procesamiento de sistemas grandes completamente funcional, contenido en un camión, tráiler o remolque, y conducido a una ubicación convenida en caso de un desastre.

1.4.5.2 Opciones para la operación de un sitio alterno

La preparación del sitio de recuperación a menudo se clasifica como sigue[7]:

- **Sitio frío (Cold Site)**

Consiste típicamente de facilidades con un adecuado espacio e infraestructura (energía eléctrica, conexiones de telecomunicaciones y controles ambientales) para soportar los sistemas de IT. El sitio, por lo general, no contiene equipos de IT y

[7] Marianne Swanson, Amy Wohl, Lucinda Pope, Tim Grance, Joan Hash, Ray Thomas. (June 2002). *Contingency Planning Guide for Information Technology Systems,* págs. 28, 29.

usualmente equipos de automatización de oficina, tales como teléfonos, máquinas de fax o copiadoras. La organización que usará el *Cold Site* será responsable por proveer e instalar los equipos necesarios.

- **Sitio intermedio (Warm Site)**

Está parcialmente equipado y contiene poco o todo los sistemas de hardware, software y telecomunicaciones y suministro de energía. El *Warm site* se mantiene en un status operacional listo para recibir la reubicación de los sistemas. El sitio puede necesitar algunos acondicionamientos antes de recibir los sistemas y el personal. En muchos casos este tipo de sitios puede servir como facilidades de operaciones normales para otros sistemas y en el caso de una contingencia, las actividades normales son desplazadas temporalmente para alojar los sistemas que fueron declarados en contingencia.

- **Sitio caliente (Hot Site)**

Son oficinas apropiadamente dimensionadas para soportar todos los requerimientos de sistemas y están configurados con todos los dispositivos de hardware, infraestructura y personal de soporte. Los *Hot Sites* son sitios de operación 24x7, y el personal asignado comienza las preparaciones para el arribo de los sistemas tan pronto como se notifica la ocurrencia de la contingencia.

- **Sitio movil (Mobile Site)**

Este tipo de sitio está disponible a través de alquiler a proveedores comerciales. Las facilidades están frecuentemente en un trailer y deben ser conducidas y ajustadas a la ubicación alterna. Para obtener una solución de recuperación viable con este esquema, el sitio móvil debe ser diseñado con antelación con el proveedor y se debe establecer un Acuerdo de nivel de servicio (SLA), esto es necesario debido al tiempo que es para configurar el sitio móvil requerido.

- **Sitio espejo (Mirrored Site)**

Son completamente redundantes con data en tiempo real, estos sitios son idénticos al sitio primario en todos los aspectos de tecnología requeridos. Este tipo de sitio provee el más alto nivel de disponibilidad debidos a que los datos son procesados y almacenados simultáneamente en ambos sitios. Este tipo de sitio es construido, operados y mantenido por la organización misma.

Existen diferencias obvias en costo y disponibilidad de los sitios entre estas cinco opciones. El *Mirrored Site* o espejo es la opción más costosa pero asegura el 100% de disponibilidad. Los *Cold Sites* son menos costoso de mantener, pero requieren un considerable tiempo para adecuarlos a los requerimientos de sistemas. Los sitios parcialmente equipados como los *Warm Sites*, entran en el medio de espectro y constituyen una adecuada solución para muchas empresas. En muchas ocasiones los *Mobile Sites* son despachados al sitio requerido en lapsos que alcanzan las 24 horas, pero los tiempos se incrementan al considerar la instalación de equipos necesarios.

TABLA 1.1 - CRITERIOS DE SELECCIÓN DEL SITIO ALTERNO

SITIO	COSTO	HARDWARE	TELECOM	TIEMPO	UBICACIÓN
COLD SITE	Bajo	Ninguno	Ninguno	Alto	Fijo
WARM SITE	Medio	Parcial	Parcial/Full	Medio	Fijo
HOT SITE	Medio/Alto	Full	Full	Corto	Fijo
MOBILE SITE	Alto	Dependiente	Dependiente	Dependiente	No Fijo
MIRRORED SITE	Alto	Full	Full	Ninguno	Fijo

1.4.5.3 Opciones para la operación del sitio alterno

En la planeación de un sitio alterno para la recuperación de desastres, se debe decidir la forma en que se habrá de operar el sitio. Básicamente se puede elegir entre tres opciones[8]:

- **No hay operaciones en el sitio alterno**

Éste será el caso en el cual se decide no administrar una carga de trabajo en el sitio alterno. Esto podría deberse a que el sitio alterno es un *Cold Site*, un *Hot Site* comercial o un servicio móvil de recuperación. En este caso, las operaciones sólo se volverán importantes en el momento del desastre.

- **Sitio alterno operado remotamente**

Un sitio alterno que está manejando una carga de trabajo puede operarse desde el sitio principal. Si un desastre afecta al sitio principal, tendrá que transportarse al personal de operación y alojarlo en el sitio alterno o en algún otro centro de mando. El tiempo requerido para transportar a los operadores al centro de datos secundario debe incorporarse entonces al tiempo permitido para la recuperación.

Como alternativa, el centro de operaciones puede ser remoto tanto para el sitio principal como para el secundario. Si éste es el caso, y si el desastre no afecta al centro de operaciones, no se requiere transportar al personal de operaciones. Por supuesto, el centro de operaciones sería un solo punto de falla para ambos sitios y deben tomarse en consideración arreglos especiales de respaldo.

En algunos casos, los clientes de *Hot Sites* comerciales están ejecutando sistemas mínimos con el propósito de transferir datos electrónicamente a éste. Estos sistemas son operados por el proveedor de servicios o a distancia desde el sitio principal.

[8] Gregor Neaga, Bruce Winters y Pat Laufman. (1997). *Prevención y Recuperación de Desastres*, págs. 21, 22.

- **Personal de operaciones en ambos sitios**

Si el personal de operaciones está localizado en ambos sitios, la recuperación generalmente será más simple y rápida. Esta opción requerirá normalmente más operadores y será más cara que cuando están consolidados en un lugar.

Las primeras dos opciones requieren la implementación de una combinación de operaciones remotas y automatizadas. Si esas operaciones no se utilizan o si su uso es mínimo, entonces la tercera opción es realmente la única solución.

1.4.5.4 Consideraciones cuando se evalúan opciones

Al evaluar las opciones para operar un sitio alterno, se deben considerar su efecto sobre las actividades de las operaciones:

- **Actividades del procesador**

Se requiere un operador para desarrollar funciones básicas del procesador como encender, reiniciar y apagar. Cuando se planea la recuperación de desastres, estas funciones deben considerarse para sitios de recuperación que tengan poco personal o que no lo tengan en absoluto. Casi todas estas acciones se pueden automatizar o pueden llevarse a cabo desde un lugar remoto.

- **Interpretaciones e interacciones de consola**

El operador tiene que leer y entender los mensajes que aparezcan en la consola que tal vez requieran acciones. Estos mensajes pueden estar relacionados con información, advertencias, mensajes de error o acciones como el montaje de una cinta o de formularios especiales en las impresoras.

Los mensajes, los códigos y las respuestas deben automatizarse en el segundo sitio utilizando los productos de software disponibles. Esto da como resultado mayor control en la administración de operaciones. En un desastre, este control permitirá un cambio más eficiente de la carga de trabajo al sitio de recuperación.

- **Manejo de cinta**

Se dispone de tres opciones para permitir el procesamiento de cintas en un sitio de recuperación que sólo es atendido por unos cuantos operadores o incluso por ninguno.

La primera, es el uso de un *robot de cinta* que permite que se monten y desmonten las cintas automáticamente. Esta actividad requiere alguna operación manual, por ejemplo, para mover cintas vitales de respaldo entre la biblioteca de cinta y una bóveda fuera del sitio.

La segunda opción es colocar los dispositivos de cinta en un tercer sitio y conectarlos con el sitio principal y el sitio de recuperación. Esta configuración tiene la ventaja de que los datos de respaldo en las cintas se conservan en un lugar alejado de los sitios de procesamiento.

Una tercera opción consiste en colocar las cintas y unidades en un cuarto seguro y separado, en el sitio principal. Pueden conectarse remotamente con el sitio de recuperación. Existe el riesgo obvio de que el cuarto de cintas en el sitio principal pudiera ser víctima de un desastre que destruya el sitio principal por completo. En el peor de los casos, se deja a la organización sin ningún medio para recuperar. El cuarto de cintas seguro por lo general necesita estar especialmente bien protegido contra varios desastres potenciales.

- **Manejo de impresión**

Se deben considerar tres opciones principales, cuando se planea la recuperación de estaciones centrales de impresión.

a) Instalar equipo duplicado en el sitio de recuperación que manejaría los requerimientos diarios de impresión.
b) Mantener espacio disponible para el equipo que se arrendaría o compraría en caso de un desastre.
c) Asegurar un contrato de servicio de "sólo recuperación", que muchos proveedores de servicios de impresión externos están ofreciendo ahora.

La distribución de impresos desde un punto central también debe revisarse con la recuperación de desastres en mente, porque los documentos impresos deben transportarse desde varios sitios hasta un punto central para su distribución. La impresión remota no debe ser afectada por cambios de sitio, siempre y cuando las direcciones de las impresoras se mantengan iguales en los diferentes sitios.

- **Control ambiental**

Operaciones por lo general es responsable de controlar el ambiente del centro de computación, incluyendo el aire acondicionado, el flujo de agua fría, la humedad y las instalaciones eléctricas. Si se planea dirigir un centro de datos con poco o sin un equipo de operaciones, debe considerar algún control ambiental automatizado.

- **Reinicio de unidades de control de terminales**

Eventualmente se requiere de operaciones para restablecer unidades de control en terminales que han quedado inutilizadas por diferentes razones.

Cuando se planea un sitio secundario sin personal, esta opción debe tomarse en consideración con todo cuidado. Una posible solución sería mover las unidades de control de terminales a un área fácilmente accesible para el personal de servicio técnico, pero que al mismo tiempo esté segura contra intervenciones no autorizadas. Una segunda solución sería utilizar la tecnología de hardware disponible e instalar estas unidades de control en el sitio del operador remoto.

1.4.5.5 Distancia entre los sitios principal y alterno

Si un incendio es el único tipo de desastre del cual debe preocuparse, dos sitios pueden estar tan cerca entre sí como dos cuartos de máquinas en el mismo edificio, separados sólo por una pared a prueba de fuego. Sin embargo, los desastres pueden

afectar a más de un solo cuarto de máquinas o edificio. El alcance del desastre puede ser tal que se afecte a un área urbana completa o incluso varias ciudades. Por lo tanto, una mayor distancia entre los sitios de procesamiento de datos da como resultado una mayor seguridad contra cualquier desastre extendido.

Sin embargo, una gran distancia tiene su precio en otros términos, como costo de interconexión, esfuerzo y costo de reubicación del negocio, etc. Con la tecnología actual, no es fácil ni barato interconectar dos sitios que se encuentran a cientos o miles de kilómetros de distancia, a alto ancho de banda, para mantener completamente sincronizadas grandes cantidades de datos en ambos sitios.

Con la moderna tecnología de interconexión es posible interconectar de manera efectiva dos sitios a una distancia moderada entre ambos. Entre las ventajas se incluyen:

- **Alto ancho de banda de interconexión**

En este contexto, alto ancho de banda significa más de un solo vínculo en el rango de los megabits o gigabits por segundo. Significa docenas o cientos de vínculos de ese tipo, sobre todo cuando se considera la conexión remota entre unidades de disco y cinta.

- **Bajo costo de interconexión**

En general, el costo de las interconexiones depende de la distancia cubierta. El costo de las conexiones de la magnitud que se acaba de describir puede ser prohibitivo en caso de larga distancia.

- **Fácil reubicación del negocio en caso de un desastre**

Si todo lo que los usuarios necesitan es una conexión de red, entonces el sitio de procesamiento de datos puede volverse a ubicar en cualquier lugar. Sin embargo, si hay una gran cantidad de interacción física con el sitio de procesamiento de datos central, como intercambio de disquetes o de cinta magnética, impresión central o procesamiento de lectura electrónica de texto, este negocio tal vez no funcione si el sitio de procesamiento de datos se encuentra a cientos de kilómetros de distancia. Además, una reubicación a largo plazo del personal de procesamiento de datos puede representar un problema mayor. En estos casos, una distancia corta al sitio de recuperación podría ser un requisito importante.

- **Actualización remota en tiempo real a través de interconexiones de alto ancho de banda**

Las estrategias avanzadas de respaldo, sobre todo en actualización remota en tiempo real o de copia de sombra en disco, pueden prolongar el tiempo de respuesta de las transacciones. Por lo tanto, requieren interconexiones de alto ancho de banda y alto rendimiento. Con algunas de estas tecnologías, la distancia de la interconexión también afecta al rendimiento. Para mantener al mínimo el impacto en el tiempo de respuesta de tales tecnologías, a menudo es necesario elegir un sitio de recuperación a una distancia moderada.

1.4.6 Capacidad de recuperación

Al diseñar el sitio alterno, es vital que los recursos cumplan con los requerimientos de capacidad y desempeño de la carga de trabajo vital para la organización.

Cuando se planea para la recuperación de desastres, tal vez se decida permitir que toda la carga de trabajo crítica de la aplicación, o un subconjunto de la carga de trabajo, opere en modo degradado; es decir, dispone de menos recursos de computación para la recuperación de desastres con el fin de reducir el costo de las instalaciones y los recursos que se requerirían en la operación de la carga de trabajo a los máximos niveles de rendimiento. Sin embargo, algunas organizaciones no están dispuestas a tolerar una degradación en el rendimiento de cualquiera de sus cargas de trabajo críticas en el modo de recuperación de desastres. Ambas opciones resaltan la necesidad de que se establezcan acuerdos en el nivel de servicio para la operación de recuperación de desastres. Los diseñadores del sitio alterno deben asegurarse que se proporcionan recursos suficientes de computación para cumplir con estos acuerdos en el nivel de servicio[9].
También debe tomar en cuenta el crecimiento convencional de la aplicación cuando planee el sitio para recuperación de desastres. Quienes planean la capacidad por lo general proporcionan en el sitio principal capacidad adicional para que las aplicaciones puedan crecer a la tasa programada. Tal vez también se requieran provisiones de capacidad similares en el sitio de recuperación.

1.4.6.1 Dependencia de componentes específicos

El recurso planeado para el sitio de recuperación debe incluir una configuración de hardware y software que cumpla con los requerimientos específicos de cada aplicación definida en la carga de trabajo crítica. Si una aplicación del sitio principal requiere una característica específica para su cooperación, entonces esa característica debe existir también en el sitio de respaldo. Si las aplicaciones son dependientes del dispositivo, entonces deben configurarse dispositivos compatibles en el sitio de recuperación.

En algunos casos, las aplicaciones tal vez dependan de la disponibilidad de equipo especial o crearlo a la medida. En este caso, debe tomarse la decisión de duplicar el equipo en el sitio de recuperación, adquirirlo o reconstruirlo en el momento del desastre. En el caso de cierto equipo, la reconstrucción significará una demora inaceptable y, por lo tanto, la única opción será mantener el hardware duplicado.

1.4.6.2 Opciones de interconexión

Tanto el sitio principal como el secundario no necesitan estar interconectados para la recuperación de desastres. Por ejemplo, tal vez los datos en cinta se lleven regularmente al sitio de recuperación. Es más, para proporcionar la mejor protección

[9] Gregor Neaga, Bruce Winters y Pat Laufman. (1997). *Prevención y Recuperación de Desastres*, pag. 25

posible de los datos, además de la reanudación más rápida posible en el caso de un desastre, los datos deben transmitirse fuera del sitio con la mayor rapidez y frecuencia. Esto se logra utilizando tecnología de interconexión de alto ancho de banda para conectar dispositivos de disco o cinta remotos a través de canales extendidos. Aparte del costo, la distancia puede ser aquí un factor de limitación. Aunque alguna tecnología emergente puede ampliar esta capacidad en el futuro, es probable que la interconexión de ancho de banda más alto implique siempre una cierta limitación de distancia.

1.4.6.3 Diseño de una red de comunicaciones

Hay dos componentes en el diseño de una red para la recuperación de desastres. El primero es la posibilidad de conectar la red a un sitio alterno en caso de un desastre o una prueba. El segundo es la posible conexión de red entre los sitios para permitir la transferencia de datos. Aunque estos componentes están separados lógicamente, tal vez compartan la misma infraestructura de red.

- **Conexión de red en el caso de desastre**

En el caso de un desastre, la red tiene que conectarse al sitio alterno. Esto puede lograrse mediante varios métodos diferentes, incluyendo el cambio de líneas en el momento del desastre o la disposición de líneas permanentemente instaladas en el sitio alterno.

La capacidad de la línea requerida después del desastre debe analizarse cuidadosamente. El movimiento de la carga de trabajo al sitio alterno puede provocar cambios importantes en el tráfico de la red. Los usuarios pueden cambiar de un vínculo local a uno remoto, y los usuarios remotos tal vez requieran rutas de transmisión significativamente diferentes a través de la red.

En muchos casos, los costos prohibirán la duplicación de toda la red de producción, y en realidad tal vez sea necesario recuperar únicamente una parte de la red de producción con base en la carga de trabajo crítica y las ubicaciones incluidas en el alcance de un plan de recuperación.

También se requiere algún nivel de conectividad de red para probar la recuperación en el sitio alterno. Para gran parte de la prueba esto será un subconjunto de la red requerida en previsión de un desastre; sin embargo, periódicamente necesitan probarse las necesidades de activación de toda la red, para tener la certeza de que funcionará en caso de un desastre.

- **Conexión entre sitios para transferencia de datos**

La configuración para la recuperación de desastres puede incluir la transferencia electrónica de los datos por medio de una conexión de red entre los sitios principal y alterno. Esto puede incluir:

a) Operación *remota:* La operación de uno o ambos sitios puede controlarse remotamente, lo que puede causar un flujo sustancial de mensajes adicionales en la red.

b) *Cambios de sistema y aplicación:* Es deseable que se mantengan sincronizados todos los sistemas y el software de aplicación, en ambos sitios. Una manera razonable de enviar datos de los cambios a un sitio remoto es utilizar la red.

c) *Administración de sistemas:* La mayor parte de las tareas de administración de sistemas necesitan la red. Por ejemplo, además de los datos de los cambios descritos, tienen que intercambiarse datos apropiados de la administración de cambios.

d) *Copias de respaldo de la base de datos:* Si se van a enviar por la red copias de respaldo de la base de datos, se requerirán enlaces de transmisión de capacidad extremadamente alta.

e) *Registros de transacciones de la base de datos:* Para facilitar un proceso de actualización en el sitio de recuperación, deben enviarse periódicamente los registros de transacciones de la base de datos, al sitio de recuperación. Si se elige la red como medio de transmisión, esto provocará una carga adicional en la red.

f) *Cintas o discos remotos:* Los dispositivos de cinta o disco pueden ser colocados en el sitio alterno, conectados con el sitio principal a través de canales remotos o extensiones de canales. Además de la red de área amplia, esas extensiones de canales deben ser parte del diseño de la red para la recuperación de desastres.

- **Propiedades del diseño de red**

Un diseño de red con capacidad de recuperación de desastres debe tener las siguientes propiedades:

a) *Acceso a red para ambos sitios:* Esto es requerido tanto para tomar el control de la carga de trabajo como para las pruebas periódicas.

b) *Ambos sitios deben tener capacidad para controlar la red:* Las grandes redes, aunque pueden conectar varios sitios, por lo general son controladas desde un solo lugar. Deben existir disposición para mover la función de control de la red a otro sitio, en el caso de un desastre en el lugar de control.

c) *Rutas externas aisladas:* Si existen dos sitios, cada uno con su propio gateway, un solo punto de falla puede existir en la conexión externa entre los gateways y una estación telefónica pública de intercambio. Idealmente,

ambos gateways deben estar conectados a estaciones telefónicas públicas diferentes.

d) *Rutas alternas para todas las ubicaciones:* La topología de la red debe proporcionar rutas alternas entre las ubicaciones del host y todas las ubicaciones remotas de usuario. Por lo general, éste es un requisito para alta disponibilidad y, como tal, a menudo se cumple cuando no existe estrategia explícita de recuperación de desastres.

e) *Cambio automático de ruta:* Cada vez que se requiere un cambio de ruta en el caso de recuperación de desastres, debe tener lugar automáticamente o bajo control central. Los usuarios remotos por lo general no están capacitados ni tienen la experiencia suficiente para desarrollar esta tarea de manera confiable.

1.4.6.4 División de la carga de trabajo

La opción más simple es ejecutar toda la carga de trabajo en el sitio principal y asegurarse de que hay recursos suficientes en el sitio de recuperación. Esta solución tiene el beneficio de que la recuperación es relativamente directa. Además, el sitio de recuperación también podría ejecutar una copia del software del sitio principal, listo para tomar el control de inmediato en el caso de un desastre. En algunos casos, tal vez se requiera este tipo de estrategia debido a los requerimientos de recuperación del negocio. Sin embargo, en la mayor parte de los casos, una empresa no puede justificar un sitio de recuperación sin uso.

Una estrategia más viable consiste en separar la carga de trabajo no crítica y ejecutarla en el sitio de recuperación. En algunos casos, esto puede significar una separación entre el desarrollo y la producción; en otros casos, algunas funciones de negocios pueden ser más vitales que otras, permitiendo una división por aplicación.

En este escenario, si el sitio de recuperación sufre un desastre, la carga de trabajo crítica permanecerá intacta. Sólo si ocurre un desastre en el sitio principal es necesaria la recuperación de desastres. Ésta es una solución más aceptable, porque reduce la capacidad inactiva. Por lo general, la carga de trabajo no crítica es mayor que la carga de trabajo crítica y, por lo tanto, parte de la capacidad inactiva estará disponible en el sitio de recuperación. Suponiendo que no se requiere una carga de trabajo no crítica en el caso de un desastre, no se requiere una capacidad de reserva en el sitio principal. Sin embargo, generalmente, todas las cargas de trabajo se vuelven críticas mientras continúa la interrupción de servicio y por lo tanto deben preverse algunas medidas para recuperación.

Cuando sea necesaria la división de la carga de trabajo, ésta debe diseñarse para que ambos sitios sean independientes. Una falla de un sitio no debe afectar inmediatamente la operación del otro.

1.4.6.5 División de la carga de trabajo crítica

Dividir la carga de trabajo crítica de una manera práctica y útil a menudo es una actividad compleja y depende mucho de la naturaleza de cada instalación. A continuación se analizan algunos puntos que deben de considerarse.

- **Más adecuada**

Un método aparentemente simple es el de la división más adecuada de la carga de trabajo por aplicación. En este caso, las aplicaciones críticas estarían separadas en dos grupos que requieren similares capacidades para ejecutarse. En una situación estática, esto sería muy simple. Sin embargo, la carga de trabajo en la mayor parte de las organizaciones crece de manera irregular, lo que requiere ajustes constantes de la división de la carga de trabajo.

Esto significa un incremento en el monitoreo para asegurar que sea adecuada la capacidad disponible para aplicaciones críticas en ambos centros de datos. Además, a menudo las aplicaciones se relacionan entre sí a través de los datos y el procesamiento, dificultando en muchos casos la separación. Un buen conocimiento de estas aplicaciones es vital para permitir esa separación.

- **Interrelaciones con cargas de trabajo no críticas**

Si el propósito de la separación es proporcionar respaldo mutuo, tiene sentido dividir la carga de trabajo crítica entre los dos centros de datos y luego colocar la carga de trabajo restante donde pueda asignarse.

A veces, parte de la carga de trabajo menos crítica depende de bases de datos o aplicaciones críticas. En esos casos, la ubicación de las aplicaciones menos críticas está determinada por la aplicación crítica. Por lo tanto, debe realizarse un análisis de las dependencias entre las aplicaciones para determinar cuáles aplicaciones críticas van a cuál centro de datos.

- **División de la red**

En algunos casos, una aplicación se ejecuta en ambos centros de datos para diferentes subconjuntos de usuarios. Por lo general, esto implica una división de la red, la cual puede estar dividida de varias maneras:

a) *División 50/50:* Los usuarios están divididos, más o menos al azar, entre los dos centros de datos.
b) *Geográficamente:* Cada centro de datos sirve a los usuarios de una o más ubicaciones geográficas en particular.
c) *Alternancia geográfica:* Usuarios geográficamente adyacentes se asignan a centros de datos alternos. Esto significa que, en el caso de la falla de uno de los centros de datos, toda el área seguirá cubierta, pero el número de usuarios y servicios cubiertos será la mitad.
d) *Al azar geográficamente:* Los usuarios son seleccionados al azar para asignarlos a uno de los centros de datos. Parecido a la alternancia

geográfica, en el caso de falla en un centro de datos, el área de servicio seguirá cubierta y aun se le dará servicio a un 50% de los usuarios.

e) *Funcionalidad:* Los usuarios se asignan a los centros de datos de acuerdo con sus funciones. Por lo tanto, todos los usuarios de una función serían atendidos por un centro de datos y todos los usuarios de otra función por el otro centro de datos.

1.4.6.6 Consideraciones de la programación de aplicación

La implementación de la recuperación de desastres en algunos casos requiere algunos cambios a la programación de aplicaciones. Sin embargo, deben considerarse cierta programación y ciertos estándares del diseño de base de datos, cuando se desarrollan nuevas aplicaciones, para hacer más fácil y transparente la recuperación de desastres.

En el diseño de aplicaciones, la capacidad de transporte es una consideración importante, por lo tanto deben evitarse las interfaces complejas y los enlaces con otras aplicaciones. Debe tratar de que cada aplicación sea lo más autónoma o independiente posible, teniendo en cuenta que estos objetivos de diseño se encuentran en conflicto con los métodos de diseño de base de datos y de aplicación tradicional, pues recomiendan bases de datos no redundantes, y una integración de sistemas y aplicaciones. Para cada aplicación, hay un compromiso que habrá de establecerse entre estos métodos de diseño conflictivos, con base en los requerimientos del negocio que subyacen en la aplicación particular.

Deben comunicarse los cambios hechos a las aplicaciones y que afectarán a la recuperación, la capacidad y el desempeño a través de los canales de la administración del cambio.

1.4.7 Implementación de la solución de respaldo y recuperación

Una vez alcanzada la etapa de implementación, se habrán tomado todas las decisiones importantes relacionadas con la solución de recuperación y se deberá haber definido ya el alcance del proyecto de implementación[10]. El proyecto de implementación general también podría dividirse en varios subproyectos, que luego podrían asignarse a los individuos o los equipos de trabajo que habrán de implementarlos.

El proyecto para implementar la solución de recuperación cubre tres áreas principales:

[10] Gregor Neaga, Bruce Winters y Pat Laufman. (1997). *Prevención y Recuperación de Desastres*, págs. 33 - 39

1.4.7.1 Configuración de la instalación alterna de recuperación

Deberá haberse decidido ya el tipo de sitio de recuperación, también necesitan definirse las especificaciones detalladas para el sitio de recuperación y las instalaciones que albergará. Las tareas de implementación que necesitan completarse varían, dependiendo del tipo de solución de sitio alterno que se haya elegido. Tal vez sea necesario construir y equipar una nueva instalación de recuperación, adquirir o reacondicionar un sitio existente o negociar y firmar un contrato con un proveedor de servicios externo.

Configurar un segundo sitio que sea propiedad de la empresa constituye un proyecto importante en sí mismo y no se analiza de manera detallada en este proyecto. Si la solución de recuperación incluye contratar un sitio Hot comercial, deben tomarse en consideración los siguientes elementos:

- Magnitud o duración del contrato en comparación con los costos
- Distancia del sitio principal
- Facilidad de actualización cuando se requiera
- Tiempo para prueba incluido en el contrato
- Tamaño y tecnología utilizada en el sitio
- Capacidad para admitir el crecimiento de la empresa
- Cláusulas de cancelación en el contrato
- Número de suscriptores permitido dentro de un área o un edificio determinado
- Servicios de soporte
- Si se incluye en el contrato un sitio Cold
- Prestaciones de la red
- Seguridad física

1.4.7.2 Desarrollo de procedimientos de recuperación

Tienen que crearse nuevos procedimientos y enmendarse los existentes para tener la seguridad de que pueden recuperarse los procesos vitales de negocios y ejecutarse en el sitio de recuperación. Algunos ejemplos de los tipos de procedimientos que es preciso desarrollar o modificar son:

- **Procedimientos de respaldo de datos**

Aunque la mayoría de las organizaciones respaldan datos actualmente, muchas no han hecho un estudio a fondo para determinar cuándo deben respaldarse ciertos datos, cómo deben respaldarse y cuántas generaciones deben conservarse fuera del sitio. Por lo tanto, una vez que se haya realizado el análisis de impacto en el negocio, los cambios necesitan reflejarse en los procedimientos de respaldo de datos existentes (o nuevos) para cada aplicación.

Tal vez sea necesario tener un conjunto de respaldos para recuperación de desastres separados de los respaldos de producción, debido a las reglas del ciclo.

Para este propósito tal vez valga la pena establecer una convención de asignación de nombres a los archivos de respaldo para recuperación de desastres.

- **Procedimientos de almacenamiento fuera del sitio**

Una vez que se hayan determinado los requerimientos de respaldo de los datos, deben crearse los procedimientos para implementar las reglas del ciclo en el sistema de manejo de cintas y asegurarse que todos los nuevos respaldos de recuperación de desastres entren al ciclo fuera del sitio. Algunos de los datos que necesitan mantenerse fuera del sitio, pero no necesariamente incluirse en el ciclo, estarán en formato impreso. Puede tratarse de formas especiales, documentación o guías de referencia que serán necesarias para la recuperación o para realizar una función de trabajo, una vez que el sistema esté funcionando en la instalación alterna. Los procedimientos fuera del sitio deben ser verificables, para asegurar que los datos y la documentación vitales se mantienen o se incluyen en el ciclo fuera de sitio de manera regular.

Si la solución incluye transferencia electrónica de datos para la instalación alterna, se deben proporcionar procedimientos para el manejo y la seguridad de estos datos.

- **Procedimientos de recuperación de datos**

También es necesario crear o enmendar procedimientos de recuperación para restaurar todos los datos vitales en el centro de recuperación. Estos procedimientos de recuperación de datos necesitan reflejar el nuevo respaldo de datos y los procedimientos de almacenamiento fuera del sitio.

- **Procedimientos de administración del cambio**

La administración del cambio por lo general corresponde a los cambios en el ambiente de procesamiento de datos de producción actual. Habitualmente se realiza por medio de formularios de solicitud de cambios en línea y revisiones semanales para la aprobación de los cambios solicitados. Una sección sobre el impacto de la recuperación de desastres debe agregarse a todas las solicitudes actuales de los diferentes departamentos que piden administración del cambio. Esto evitará cambios de implementación que pudieran tener un fuerte impacto sobre la capacidad de recuperación sin que nadie se dé cuenta. Una vez que se conozca el impacto, pueden darse los pasos apropiados para asegurar que no se encuentra comprometida la viabilidad de la recuperación.

- **Reglas de diseño de la aplicación**

El mejor momento para evaluar la importancia vital de una aplicación y el impacto en la recuperación de desastres es cuando se encuentra en las etapas de diseño y elaboración. Esto permite crear aplicaciones fáciles de recuperar y reaccionar a los cambios necesarios, como contratar o adquirir un disco adicional o capacidad de procesador en la instalación alterna. Por lo tanto, se debe establecer reglas para asegurar que se determinen los requerimientos de recuperación durante el diseño y la elaboración y que se implementen, antes de llevar la nueva aplicación de la elaboración a la producción.

- **Procedimientos de recursos humanos**

En este momento deben darse los pasos para establecer políticas o procedimientos de la empresa encaminados a los temas de recursos humanos que surgen en una situación de desastre. Esas políticas y procedimientos pueden definir la forma en que se notificará de un desastre a los empleados, se determinará quién trabaja y quién no, las compensaciones, el asesoramiento y el progreso de la recuperación.

1.4.7.3 Elaboración del plan de recuperación

Un plan de recuperación de desastres es un documento extenso y detallado que establece todas las acciones que se tomarán antes, durante y después de que ocurra una catástrofe. Una vez que se ha implementado la solución de recuperación y se ha elaborado el plan, los pasos "antes" se refieren al mantenimiento del plan, los pasos "durante" se refieren a la ejecución del plan en el momento del desastre y los pasos "después" se refieren a la preparación para el retorno al sitio original.

Un plan de recuperación de desastres amplio y viable para un sistema grande sólo puede desarrollarse como parte de un proyecto importante de implementación. Aunque es posible cierta automatización, la recuperación es básicamente una tarea manual. La preparación y habilidad del personal involucrado pueden tener un efecto significativo en la velocidad y el éxito de la recuperación.

- **Contenido del plan**

El plan de recuperación debe incluir algunos elementos como:

a) Alcance y supuestos de la recuperación
b) El proceso para reconocer un desastre y ejecutar el plan
c) Identificación de los equipos de trabajo de recuperación y de sus miembros
d) Tareas y responsabilidades principales de los equipos de trabajo de recuperación
e) El (los) responsable(s) del plan
f) La forma en que se mantendrá el plan
g) La forma en que se probará el plan

Como en el caso de cualquier proyecto grande, es extremadamente importante que todos los implicados comprendan el alcance del trabajo que habrá de realizarse. El alcance, los supuestos y las directrices generales debieron haberse definido y documentado claramente en el plan de recuperación.

1.4.8 Reconocer el desastre

Un desastre no necesariamente causa una falla inmediata en todo el centro de datos. Más bien, podría iniciarse como una serie de fallas graduales o como un daño aparentemente limitado. No siempre queda claro que ha ocurrido un desastre. Además, el problema podría suceder en el peor momento, durante el fin de semana o en el cambio de turno de la noche, cuando los expertos ya no están disponibles para evaluar la dimensión del problema. Esa situación se caracteriza por la incertidumbre

y, a menudo, por la confusión. Debido a esto deben implementarse procedimientos que definan claramente la acción que habrá de tomarse.

La mayor parte de los departamentos de procesamiento de datos utilizan alguna forma de procedimiento de operación para documentar escenarios problemáticos. Como parte de la estrategia de recuperación de desastres, esta documentación debe ampliarse para que incluya directrices sobre cuándo debe declararse como desastre un problema específico y qué pasos se deben seguir para atacar la situación. Esa documentación tal vez no cubra toda situación posible de manera detallada, pero en la mayor parte de los casos permitirá una evaluación más objetiva y exacta de la misma.

El alcance de estos escenarios quizá vaya de problemas posibles de controlar (como una falla de comunicación en una conexión de red importante o la validación de datos en una base de datos) hasta situaciones realmente extremas como incendio en salas de máquinas o destrucción total a causa de un sismo. La recuperación después de los daños causados por los primeros problemas por lo general puede hacerse internamente, mientras que la reparación en el caso de los últimos pertenece obviamente al campo de la recuperación de desastres.

1.4.9 Regreso al sitio principal

El plan de recuperación de desastres debe incluir una sección que cubra el regreso al sitio principal, el cual pudo haber sido seriamente afectado por la ocurrencia de un evento.

Muchas de las tareas son parecidas al traslado al sitio alterno, aunque en este caso la mudanza se planeará y será más controlada. El nivel de esfuerzo y el detalle aplicados a la planeación de esta actividad antes de un desastre dependerá de cuánto tiempo se puede permanecer en el sitio alterno. Si hay tiempo suficiente en el sitio alterno, el plan para regresar al sitio principal puede desarrollarse después del desastre.

Si el sitio alterno resulta un sitio Hot comercial, tal vez pueda permanecer allí sólo un máximo de seis semanas. En este caso, quizás necesitará planear un movimiento intermedio a una instalación de sitio Cold además del regreso final a su sitio principal.

1.4.10 Mantenimiento actualizado de la solución de recuperación de desastres

Una vez que se ha elaborado el plan de recuperación de desastres y que se ha implementado la solución de recuperación, deben ponerse en práctica los procedimientos para mantenerla viable, antes de cerrar el proyecto. Los cambios en el ambiente de procesamiento de datos son constantes, y cualquier cambio podría

inutilizar el plan de recuperación. Estos procedimientos deben incorporar estos tres elementos distintos:

1.4.10.1 Procedimiento de mantenimiento

El propósito de los procedimientos de mantenimiento es proporcionar un mecanismo para actualizar la solución de recuperación cuando se hagan cambios en el ambiente que puedan tener impacto en la viabilidad del plan, así como proveer la prueba continua del plan y llevar a cabo la capacitación constante del personal.

Los cambios que pueden afectar a la solución de recuperación pueden provenir de muchas fuentes, tales como, desarrollo de nuevas aplicaciones, cambios a la configuración actual de hardware, cambios a la red, cambios organizacionales, cambios del sistema y cambios al sitio alterno.

Debe haber un sistema de administración del cambio integrado para toda la organización, con el fin de proporcionar un solo punto de control. Debe revisarse el impacto de todos los cambios sobre el plan de recuperación de desastres, porque cualquiera puede afectar a la viabilidad del plan. Por ejemplo, un simple cambio en la configuración tal vez tenga un impacto significativo en el sitio alterno.

Tal vez necesite reconsiderarse la decisión de hacer un cambio si el impacto es demasiado grande. Esto resulta especialmente cierto si el sitio alterno es un segundo sitio propiedad de la compañía. Por supuesto, si se hace un cambio en el sitio principal, tal vez no sea necesario o apropiado hacer un cambio idéntico en el segundo sitio. Todos estos factores deben ser valorados por la función de administración del cambio. En las siguientes secciones se tratan algunos de los tipos principales de cambio que pueden tener un efecto sobre el plan de recuperación de desastres.

- **Cambios en la configuración del hardware**

Cuando se hacen cambios al ambiente de hardware en el sitio principal, se debe determinar el impacto que tendrán estos cambios en el plan de recuperación de desastres. Los cambios en esta área pueden tener impacto en los objetivos de rendimiento.

- **Cambios en la aplicación**

Es esencial que, si las aplicaciones o los programas de aplicación se desarrollan o modifican de cualquier manera en el sitio principal, esos cambios se apliquen también a la solución de recuperación. El equipo de trabajo de administración del cambio debe determinar la manera más apropiada de asegurar que se ha evaluado el "impacto en el momento del desastre" y se han tomado medidas preventivas para antes de la aceptación de la aplicación o programa en el ambiente de producción.

- **Cambios en el ambiente de software**

Si el sitio alterno es propiedad de la compañía, es importante tomar en consideración el impacto de que el ambiente del sistema operativo en ambos sitios no sean idénticos. Idealmente, debe ser así, aunque en la realidad esto no siempre es posible. Cuando se realiza el plan del sitio de recuperación de desastres, debe asegúrese de que se consideren ventajas y desventajas de sistemas idénticos.

1.4.10.2 Auditoria del plan de recuperación de desastres

La única manera segura de determinar si se han aplicado las actualizaciones o los cambios al documento del plan de recuperación de desastres es auditarlos. El contenido del plan debe auditarse de manera semestral o anual tomando en cuenta lo siguiente:

- No deben tomarse todos los datos para auditoria al mismo tiempo.
- Todos los documentos auditados deben devolverse en un plazo no mayor de 24 horas a quien los tenía.
- Las deficiencias deben anotarse y corregirse antes de devolver el documento a su depositario original.
- Debe entregarse un informe a la administración que documente el estado de cada documento de quien conserva el plan, es decir, completo o incompleto.

Además de auditar el contenido de los planes de recuperación de desastres, deben auditarse mensual o bimestralmente todos los componentes importantes del proceso de recuperación. Entre los ejemplos de tales componentes se encuentran:

- La lista de cintas de archivos vitales para asegurarse de que todos los respaldos requeridos se encuentran fuera del sitio.
- El sistema de "paquete único" o de "emergencia" para asegurarse de que está actualizado. Este sistema también debe probarse de vez en cuando en el sitio principal, para asegurarse de que puede ser iniciado.

1.4.10.3 Pruebas al plan de recuperación desastres

Una parte esencial de la planeación de la recuperación de desastres es la prueba o ensayo. Con gran frecuencia, la simple creación de un plan de recuperación de desastres produce una falsa sensación de seguridad. Sin antes probarlo, es casi inevitable que el plan sencillamente no funcione cuando ocurra el desastre. La prueba es la única manera de saber si están funcionando sus procedimientos de mantenimiento. Una vez que se ha desarrollado y probado el plan, la única manera en que puede fallar es la de que no se haya llevado a cabo correctamente el mantenimiento.

Siempre que sea posible, se debe elegir una estrategia de recuperación de sitio remoto que le permita hacer pruebas con frecuencia. La prueba de sus tareas y procedimientos de recuperación de desastres ofrece los siguientes beneficios:

- Saber que el plan de recuperación funciona.
- Descubrir problemas, fallas y errores que pueden resolverse o corregirse.
- Capacitar empleados en las pruebas de ejecución y manejo de situaciones de recuperación de desastres.
- Hacer del plan de recuperación un documento "vivo".
- Despertar la conciencia de todas las partes de la organización de procesamiento de datos (PD) sobre la necesidad de planear la recuperación de desastres.

Hay dos tipos de prueba que deben efectuarse. En las pruebas "activas" se va a un sitio alterno y se restauran los sistemas y aplicaciones como se estableció en el plan de recuperación de desastres. La otra prueba, "pasiva", es una prueba logística del plan. Generalmente se realiza reuniendo a los equipos de trabajo de recuperación (incluyendo la administración) en una sala de conferencias y revisando los pasos que cada quien daría en caso de un desastre.

- **Frecuencia de las pruebas**

Casi invariablemente, las instalaciones afrontan un mini desastre cuando prueban por primera vez el plan de recuperación; en el mejor de los casos, esto se dará durante la etapa de desarrollo. Los defectos del plan sólo saltarán a la vista en el curso de varios intentos de recuperación.

Por lo tanto es recomendable planear varias pruebas durante el desarrollo del plan. Una vez que se ha llevado a cabo la elaboración del mismo, las pruebas deben efectuarse dos o cuatro veces al año.

En condiciones normales, es recomendable que el plan de recuperación se pruebe por lo menos dos veces al año. En las pruebas, las personas involucradas saben lo que va a suceder. Esto es esencialmente una revisión de que los procedimientos para la recuperación de la plataforma, los datos y los procesos de negocios estén completos y sean exactos.

- **Niveles de prueba**

Ninguna de las pruebas realizadas en el sitio alterno será una prueba completa del plan de recuperación de desastres. Hay varios niveles de prueba que deben tomarse en consideración, de acuerdo con lo siguiente:

a) Pruebas de las plataformas de sistema

Siempre que haya un cambio importante en el sistema operativo debe planearse una mini prueba en el sitio alterno, para asegurarse de que el sistema operativo puede recuperarse e iniciarse con el nuevo software. En este momento puede ser conveniente realizar hacer pruebas limitadas de red.

b) Pruebas de la red

Los cambios importantes al ambiente de red tal vez requieran pruebas independientes para verificar que pueden establecerse conexiones y que los datos pueden transmitirse antes de ejecutar una prueba completa. El sistema operativo necesitará restaurarse como parte del proceso, junto con algunos datos y ubicaciones de prueba.

c) Pruebas de plataformas, red y aplicaciones seleccionadas y procesos del negocio

A menudo se le llama a este conjunto la prueba completa, porque incluye la prueba de todos los componentes importantes de la recuperación, aunque tal vez no se incluyan en la prueba todas las aplicaciones o procesos del negocio.

Por el trastorno en el trabajo del personal en el sitio principal, es raro que se prueben todos los procesos del negocio en una sola verificación. Por lo general, en cada prueba se revisan diferentes procesos para que todos se hayan probado alguna vez en el curso del año. En una empresa pequeña, tal vez sea posible probar todas las aplicaciones críticas y los procesos de negocios al mismo tiempo.

d) Transferencia total de servicios al centro de recuperación de desastres

Mientras no se haya experimentado esta opción, no se puede tener plena seguridad de que el plan de recuperación de desastres funcionará eficazmente en un desastre real. Es un ejercicio muy costoso, porque presenta el riesgo real de que, si el plan no funciona, las fallas durante el ensayo pudieran tener impacto a la hora del retorno al centro de datos normal.

Sería poco práctico intentar la recuperación de todas las aplicaciones y procesos del negocio durante la primera prueba de aplicación. Cada aplicación o grupo de aplicaciones debe probarse por separado; luego, cuando todas se hayan recuperado por separado y con éxito, se puede probar la recuperación de todas las aplicaciones juntas.

- **Actividades antes de la prueba**

La planeación para una prueba importante debe empezar uno o dos meses antes de la fecha programada de la prueba en el sitio alterno. Si éste es un sitio Hot comercial, las pruebas deben programarse por lo menos con seis semanas de anticipación. Para pruebas largas (de 3 a 4 días), tal vez se tenga que programar las pruebas con un año de anticipación. Si el sitio alterno es un segundo sitio propiedad de la empresa, entonces debe notificarse debidamente a quien corresponda para que haya recursos suficientes para la prueba.

A continuación se presentan algunos de los pasos que deben incluirse como parte de las actividades previas a la prueba:

- Activar el enlace o interfaz con el sitio alterno, para asegurarse de que se ha programado la fecha de la prueba v de que los recursos están disponibles.
- Cada prueba debe ser precedida por un repaso con todos los participantes.
- En general, la prueba programada debe incluir los componentes de sistema, aplicación, red y procesos del negocio del plan pudieran tener impacto a la hora del retorno al centro de datos normal.
- Debe prepararse y distribuirse previamente el programa de la prueba a todos los miembros del equipo de trabajo.
- Los auditores deben participar en todas las pruebas.
- Los objetivos, criterios, enfoques y actividades de la prueba deben documentarse y distribuirse a los miembros del equipo de trabajo.
- Debe determinarse la asignación de personal, incluyendo la ubicación de cada persona.

Debe convenirse de antemano las metas y los resultados esperados de cada función y proceso para permitir la medición del éxito que se obtenga.

1.4.10.4 Criterios de aceptación

Para cada prueba, el criterio de aceptación variará dependiendo de los objetivos de la prueba. En general, debe lograrse lo siguiente en cada prueba:

- El software de los sistemas debe proporcionar una versión actual de los sistemas de software operativo y de aplicación, con todos los componentes importantes activos y en buen funcionamiento.
- Por lo menos debe recuperarse y probarse una aplicación, incluyendo el procesamiento de la misma, el procesamiento por lotes y la conciliación de datos. La excepción a esto sería una prueba del sistema operativo solo para probar cambios como los de una nueva configuración de hardware.
- Todos los datos vitales tienen que venir de una instalación de almacenamiento fuera del sitio.
- Deben ponerse a prueba todas las causas de deficiencias de la última prueba para asegurar que se han corregido.

Dependiendo de la gravedad de los problemas, la prueba puede repetirse de inmediato o el problema puede dejarse para resolverlo antes de la siguiente prueba. Los problemas encontrados durante la prueba motivo del informe deben agregarse a los objetivos de la siguiente prueba. Cualquier cambio requerido a la documentación como resultado de la prueba debe incorporarse en el presente instante al plan de recuperación. Después de que se hayan realizado los cambios, deben distribuirse los documentos revisados y corregidos a todos los que tengan el plan.

CAPÍTULO 2: PLAN DE RECUPERACIÓN DE DESASTRES PARA SAP R/3 EN SINCOR

2.1 Planteamiento del problema

Antecedentes

Sincrudos de Oriente, SINCOR C.A. posee una amplia infraestructura tecnológica compartida entre las diferentes localidades, Caracas y Anzoátegui: Jose, Pariaguán y la Estación Principal. La mayor parte de la infraestructura tecnológica, lo que incluye servidores, sistemas y telecomunicaciones, se encuentran ubicada en la sede administrativa en Caracas, lo cual implica que gran cantidad de usuarios se conecta remotamente desde las diferentes dependencia para hacer uso de los sistemas administrativos y aplicaciones operativas instaladas en Caracas.

Sincrudos de Oriente, SINCOR C.A. decidió dar inicio a la implantación de un plan corporativo de recuperación de desastres. Dentro de este plan maestro el proyecto piloto consistió en la implantación de un ambiente tolerante a fallas para el sistema SAP R/3.

La decisión que el sistema SAP R/3 se erigiera como proyecto piloto radica en que la mayor parte de las actividades administrativas de SINCOR en procesos relacionados con finanzas, mantenimiento de planta (PM), manejo de materiales (MM), costos (CO), comercialización (SD) son ejecutados a través del sistema SAP R/3. Esto lo convierte en uno de los sistemas vitales para la organización, lo cual hace necesario garantizar la continuidad operativa de este sistema ante cualquier tipo de falla.

Como consecuencia, en el departamento de IS*/IT & Telecom* de SINCOR se planteó la necesidad de implantar un ambiente tolerante a fallas en el cual exista una replica del sistema SAP R/3 mediante la instalación en un *centro de datos alternativo* en un sitio remoto.

2.2 Objetivo general

Implantación de un ambiente tolerante a fallas a través de un centro de datos alternativo que permitir reanudar las funciones del negocio que pudieran afectarse como consecuencia de una falla o daño mayor en la plataforma tecnológica instalada en el *centro de datos primario* ubicado en Caracas.

2.3 Objetivos específicos

1. Evaluación de requerimientos de hardware, software y telecomunicaciones.

2. Analizar de posibles riesgos para la plataforma tecnológica actualmente instalada en el centro de datos primario.

3. Diseñar e implantar una infraestructura de sistemas tolerante a fallas que permita lograr alta disponibilidad y acceso continúo a los datos del sistema SAP R/3.

4. Definición e implantación de estrategias de respaldo para recuperación de desastres, planeación de una metodología avanzada de respaldo para la protección en caso de fallas y para una rápida recuperación de los servidores de bases de datos en caso de desastre.

5. Generación de procedimientos que permitan la activación del ambiente replica en caso de falla y posterior restauración, una vez solucionada la falla al centro de datos primario.

2.4 Metodología y alcance de la implantación

2.4.1 Consideraciones generales

El alcance contempla el diseño e implantación de un plan que permita mantener las operaciones del sistema SAP R/3 en condiciones de desastre mayor de la infraestructura que soporta el sistema de producción, tales como daño a los servidores del ambiente SAP R/3, daño total o parcial de los respaldos en cinta, problemas eléctricos.

Esto se realizará mediante la implantación de un ambiente tolerante a fallos en el cual exista una replica del sistema SAP R/3 en un *centro de datos alternativo* , el cual por su ubicación y seguridad estará ubicado en el Complejo Refinador de Jose en el Estado Anzoátegui.

Esta infraestructura de sistemas tolerante a fallas permitirá lograr un factor de servicio manteniendo las actividades clave para la empresa que se ejecutan a través del sistema SAP R/3 y el acceso continuo a los datos de este sistema critico. A través de la instalación del centro de datos se reanudarán las funciones del negocio que pudieran afectarse como consecuencia de una falla o daño mayor en la plataforma tecnológica instalada en el *centro de datos primario* ubicado en Caracas.

La replicación o actualización de datos se realizará a través de la WAN de SINCOR. La frecuencia debe ser establecida en función del volumen de datos que viajarán a través del enlace. No está considerado inicialmente la ampliación del enlace de

telecomunicaciones y la propuesta debe tomar en consideración las limitaciones en el ancho de banda de la infraestructura de telecomunicaciones de SINCOR.

El establecimiento del alcance de este proyecto se basa en la descomposición de los requerimientos para la implantación del plan (*WBS - Work Breakdown Structure*), el cual se muestra en el *Apéndice C: Descomposición de actividades.*

2.4.2 Tipo de estudio

De acuerdo al problema planteado referido a la implantación de un ambiente tolerante a fallos para un sistema SAP R/3 en un *centro de datos alternativo*, y en función de sus objetivos se incorpora el tipo de investigación denominado Proyecto Factible. En atención a esta modalidad de investigación, el estudio se desarrolla en tres grandes fases. En la primera de estas fases se elaborará el plan de trabajo y la estrategia para implantar el sistema de recuperación en caso de desastre mayor para el sistema SAP R/3. La segunda fase y atendiendo a los resultados de elaboración del plan se realizará la implantación de la solución propuesta y posteriormente la fase de puesta en producción.

2.4.3 Premisas

1. La configuración y pruebas se realizarán inicialmente en Caracas y luego de completada esta fase se trasladará al centro de datos alternativo .
2. Se realizará el reemplazo del servidor central actualmente en operación para el sistema SAP R/3.
3. La actualización de la información se realizará a través de la WAN de SINCOR.
4. La propuesta se basará tomando en consideración los recursos actuales relacionados con el medio de comunicación satélite / fibra óptica) así como las limitaciones en el ancho de banda.
5. El sistema réplica en el *Centro de Datos Alterno*, deberá estar actualizado al sistema original SAP R/3 de Producción y esto va a depender de las limitaciones físicas que presenta el enlace de telecomunicaciones instalado entre Caracas y Jose en el estado Anzoátegui.

2.4.4 Enfoque primario del plan

El enfoque primario de este proyecto es proveer un plan que responda a un eventual desastre que pueda afectar severamente la operatividad del sistema SAP R/3. El objetivo es restaurar la operatividad del sistema con los datos más recientes disponible y esto en el menor tiempo posible.

Todo plan de recuperación de desastres asume un cierto nivel de riesgo y existen compromisos entre cantidad de tiempo, esfuerzo, y dinero invertido en la planeación y preparación de un plan de recuperación de desastres y cantidad de datos perdidos que pueden tolerarse y aun continuar las operaciones de la empresa una vez

ocurrido el desastre. Muchas organizaciones simplemente no pueden funcionar sin sistemas de computación y en estos casos los esfuerzos de recuperación deben concentrarse en una rápida recuperación o quizás cero tiempo de perdida por medio del mantenimiento de ambientes de cómputo en localidades separadas.

Las técnicas de backup y recuperación usadas en este plan no garantizan la recuperación total de los datos. SINCOR está dispuesta a asumir el riesgo de una cierta perdida de datos en caso de una eventual situación de desastre. Los esfuerzos de recuperación de este plan están enfocados en tener el sistema SAP R/3 operativo a partir de los archivos de transacciones generados por la base de datos Oracle.

2.4.5 Visión global del plan

El plan de recuperación de desastres para el sistema SAP R/3 está basado en la preparación de un ambiente tolerante a fallas en el cual se realice la replicación de archivos de transacciones desde el centro de datos primario ubicado en el Centro Empresarial Sabana Grande en las oficinas principales de SINCOR hacia el centro de datos secundario ubicado en el Complejo Mejorador de crudo en Jose. Estado Anzoátegui. Esta replicación se realiza a través de la WAN de SINCOR.

Inmediatamente ocurrida la situación de desastre se da inicio a una secuencia de eventos en los cuales personal clave debe ser notificado y una serie de actividades deben iniciarse como consecuencia de la situación de desastre generada.

2.5 Diseño de la estrategia de implantación

El plan general de trabajo para la implantación del ambiente tolerante a fallas o de recuperación de desastres para el sistema SAP R/3 se dividió en cuatro fases:

2.5.1 Primera Fase – Planificación

Elaboración del plan de trabajo y la estrategia para implantar el sistema de recuperación en caso de desastre mayor para el sistema SAP R/3. Esta fase contempla las siguientes actividades:

- Análisis de riesgos en el centro de datos primario.
- Definición de la Infraestructura requerida para la implantación del sistema redundante (hardware, software y telecomunicaciones)
- Evaluación de estrategia de replicación para base de datos
- Medición del volumen de datos a replicar, sobre la base de la cantidad de datos que se actualizan en un periodo de tiempo determinado. Esto con la finalidad de evaluar el impacto sobre la plataforma de telecomunicaciones.
- Evaluación de la frecuencia de replicación una vez establecido el impacto en la WAN.
- Elaboración de planes de pruebas.

2.5.2 Segunda Fase - Procura e instalación de hardware

Esta fase deberá estar concluida para el inicio de la tercera fase y contempla las siguientes actividades:

- Procura de hardware.
- Instalación, configuración del servidor e instalación del sistema operativo.

2.5.3 Tercera Fase - Implantación de la solución

Esta fase contempla las siguientes actividades:

- Instalación y configuración del sistema SAP R/3 en el equipo que va a soportar la aplicación en el periodo de contingencia.
- Copia del sistema SAP R/3 original al sistema de contingencia.
- Pruebas locales de la replicación de datos para evaluar el impacto real en la infraestructura de telecomunicaciones.
- Definición de usuarios, reportes y transacciones criticas que se mantendrán operativos en caso de activación de la contingencia. Estas se utilizaran además para certificar la implantación del ambiente tolerante a fallas.
- Generación de manuales y procedimientos:
  - Procedimiento para replicación de datos al c*entro de datos alternativo*.
  - Procedimiento de activación de la contingencia.
  - Procedimiento de simulación de recuperación en caso de desastres.
  - Procedimiento para recuperación de la condición normal de operaciones en el *centro de datos primario*.
  - Estrategia de respaldo para todo el ambiente SAP R/3.

2.5.4 Cuarta Fase - Puesta en Producción

Ejecución de pruebas integrales entre los equipos instalados en el *centro de datos primario y Alternativo*.

- Instalación definitiva del servidor en el centro de datos alternativo.
- Pruebas y entonación de la replicación de datos vía WAN entre Caracas y Jose en el Estado Anzoátegui.
- Pruebas de reportes y transacciones críticas por parte de los usuarios del sistema en el servidor alterno.
- Certificación de las pruebas.
- Simulación de recuperación en caso de desastre.

2.6 Planeación y Estimación de riesgos

2.6.1 Eventuales desastres y prevención

La importancia de mantener un plan de recuperación en caso de desastre es el de tomar medidas para prevenir o mitigar sus efectos. Esta sección del plan plantea algunas de las amenazas que pueden conducir a una eventual situación de desastre.

Las amenazas consideradas pueden ser naturales o creadas por medios humanos. SINCOR desarrollo una matriz de evaluación de riesgo en la cual se clasificaron los probables riesgos a los cuales está sometida las oficinas principales. En esta evaluación se consideraron los diversos factores de riesgo en función de la probabilidad de ocurrencia y en función de ello se establecieron las medidas a tomar en cada uno de los casos.

2.6.2 Aproximación a la estimación de riesgos

Para la medición de riesgos se realizó una aproximación cualitativa, clasificando la naturaleza y la frecuencia del riesgo, se utilizó las escalas mostradas en las tablas 2.2 y 2.2 para realizar una clasificación cualitativa en cuanto a probabilidad de ocurrencia y su impacto.

TABLA 2.1 - CLASIFICACIÓN CUALITATIVA: IMPACTO DEL EVENTO

CÓDIGO	IMPACTO DEL EVENTO
5	Catastrófico
4	Crítico
3	Mayor
2	Menor
1	Insignificante / fácil recuperación

TABLA 2.2 – CLASIFICACIÓN CUALITATIVA: PROBABILIDAD DE OCURRENCIA

CÓDIGO	PROBABILIDAD
0.1	Poco probable
0.3	Remoto
0.5	Ocasional
0.7	Probable
0.9	Frecuente

2.6.3 Índice de riesgos

En el presente plan se plantean los riesgos de mayor probabilidad de ocurrencia que pueden afectar la operatividad del centro de datos y como consecuencia el sistema SAP R/3.

A continuación se presenta los diferentes eventos que pudieran ocasionar un desastre. En la tabla 2.3 se muestran los diferentes eventos que pudieran ocasionar un desastre. Se analiza el impacto, la probabilidad de ocurrencia. En base a la multiplicación de estos dos índices se genera un factor de ocurrencia. Este factor proporciona una aproximación acerca de las prioridades en las cuales deben ser afrontadas las causas y las consecuencias de la ocurrencia de estos eventos.

La escala utilizada consiste en multiplicar el índice de impacto y la probabilidad de ocurrencia de este evento. La escala para el impacto va desde 1 para el evento que puede ser catastrófico hasta el 5 para un evento insignificante y de fácil recuperación. La probabilidad de ocurrencia va del valor 0.1 para un evento poco probable hasta 0.9 para un evento de frecuente ocurrencia. Al multiplicar ambos índices se obtiene el factor de ocurrencia.

Los eventos considerados son los siguientes:

- Accidente Aéreo, Fuego generalizado, terremoto
- Fuego / inundación en el cuarto de datos (*Telecom Room*)
- Crímenes informáticos
- Daño en los canales de comunicación
- Daño de link T-Data
- Daño en la conexión de CANTV
- Daño en canales de comunicación satelital
- Daño en la conexión de última milla en Caracas
- Daño al cableado interno
- Daño en los servidores
- Daño en las cintas de respaldo
- Huelga general
- Falla eléctrica
- Falla en hardware
- Falla en el aire acondicionado del cuarto de datos (*Telecom Room*)

TABLA 2.3 - ANÁLISIS DE EVENTOS E IMPACTO

ID	EVENTO	CAUSA DEL EVENTO	IMPACTO Y CONSECUENCIAS	SEVERIDAD (1)	PROBAB. (2) (x100)	FACTOR (1 x 2)	INTERRUPCIÓN DE SERVICIOS
01	Problemas eléctricos	Error humano Sabotaje	Pérdida de comunicación interna y externa	4	70	280	Variable
02	Falla en el aire acondicionado del cuarto de datos (Telecom Room)	Problemas eléctricos Falla en Hardware	Daño a servidores y equipos de telecomunicaciones Interrupción de todos los sistemas	3	90	270	Tiempo indeterminado
03	Daño al cableado interno	Error humano Sabotaje	Pérdida de comunicación interna y externa	4	50	200	2 días
04	Daño en Servidores	Error humano Hacking Sabotaje	Pérdida de data en línea, e-mail y acceso SAP R/3	4	50	200	2 días
05	Falla en hardware	Error humano Sabotaje accidentes	Pérdida de data en línea, e-mail y acceso SAP R/3 Pérdida en conectividad de red	3	70	210	Variable
06	Daño en los canales de comunicación	Error humano Sabotaje	Pérdida de comunicación con las áreas a través de red interna de comunicación	3	50	150	Variable
07	Daño de link T-Data	Tormenta eléctrica Error humano Sabotaje Conflicto con proveedor.	Pérdida de conectividad con las áreas	3	40	120	0 días
08	Daño en la conexión de CANTV	Tormenta eléctrica Error humano Sabotaje Conflicto con proveedor.	Perdida de conexión a CANTV (no acceso a teléfono, red, perdida del link primario Caracas-Jose)	3	40	120	Variable
09	Daño en canales de comunicación satelital	Tormenta eléctrica Error humano Sabotaje Conflicto con proveedor.	Perdida en canales secundarios de comunicación (backup links) Pérdida de comunicación a los pozos (Rigs)	3	40	120	Variable
10	Daño en la conexión de última milla en Caracas			3	40	120	
11	Crimen informático	Conexión Internet Conexión OSS (SAP R/3). Conexiones con otras empresas/contratistas Dial-Up / Conexiones VPN	Daño a servidores y/o modificación o daño a la data y/o sustracción de información	2	50	100	1 semana
12	Fuego / inundación en el cuarto de datos (Telecom Room)	Problemas eléctricos Sabotaje Filtración de fluidos	Pérdida de una semana de data Daño permanente en hardware	4	20	80	2 semanas
13	Daño en las cintas de respaldo	Error humano Falla en los dispositivos Sabotaje	Máximo: Pérdida de una semana de data respaldada	2	40	80	2 días
14	Huelga general	Situación Política /Económica	No acceso a las oficinas para proveer soporte	2	40	80	Tiempo indeterminado
15	Accidente aéreo, fuego generalizado, terremoto	Falla en aeronaves Ataque terrorista Desastre natural	Perdida en sistemas, data y personas	5	10	50	3 semanas

2.6.4 Ejemplo de análisis de algunos eventos de riesgo

A continuación se ejemplifica algunos eventos de riesgo así como las medidas preventivas y las recomendaciones de cada caso.

2.6.4.1 Riesgo de Fuego

La amenaza de fuego en el centro de datos primarios y posee un alto factor de riesgo, ya que dicho centro de datos esta completamente lleno de dispositivos eléctricos y conexiones que pueden sobrecalentarse o generar un corto circuito que pudiera causar el inicio de fuego.

- **Medidas preventivas**

A continuación se describen en términos generales cuales son los sistemas y medidas preventivas tomadas en consideración en el centro de datos primario.

a) Alarmas indicadoras de fuego

El centro de datos primarios está equipado con sistemas de alarma, con detectores de humo colocados en los techos.

b) Extinguidotes de fuego

Los estinguidores de mano están ubicados en sitio visible. El equipo que tiene acceso al centro de datos está entrenado en el uso de este tipo de dispositivos.

c) Sistemas de gas Inergén

El Centro de datos está protegido por un sistema de extensión de fuego por gas *Inergén*.

d) Construcción del Centro de datos

El centro de datos primarios está construido principalmente de materiales no combustibles lo cual reduce el riesgo de propagación o generación de fuego.

- **Recomendaciones**

Revisión periódica de los procedimientos a fin de asegurar que están actualizados. Estas revisiones deben ser conducidas por un administrador imparcial y debe generarse una evaluación escrita.

Inspecciones periódicas del equipo de prevención de incendios (SSAP). Los estinguidores de fuego y los detectores de humo deben ser periódicamente revisados así como el sistema de gas *Inergén*, en este caso deben hacerse pruebas no intrusitas.

2.6.4.2 Riesgo por crímenes informáticos

Los crímenes informáticos se han transformado en una causa de desastres de alto riesgo, con las nuevas tecnologías de *networking* se ha incrementado el potencial riesgo de accesos no autorizados a los sistemas informáticos.

Los crímenes informáticos usualmente no afectan el hardware de una manera destructiva. Este tipo de riesgo puede provenir inclusive desde adentro, es decir un empleado disgustado que pueda introducir un virus o una bomba de tiempo en alguna aplicación informática, o inclusive un empleado bien intencionado que pueda generar código erróneo que afecte la integridad de la data.

- **Medidas preventivas**

a) Todos los sistemas deben tener productos de seguridad instalados con la finalidad de protegerlos contra accesos no autorizados.
b) Todos los sistemas deben estar protegidos por claves de acceso.
c) Todos los usuarios de sistemas deben cambiar sus claves de acceso como una tarea regular.
d) Todos los sistemas de seguridad deben registrar los intentos de acceso inválidos a los sistemas, y estos registros deben ser revisados por los administradores como una tarea regular.
e) Todos los sistemas deben ser respaldados con frecuencia y estos respaldos deben ser almacenados en un área separada de la data original. Deben establecerse estándares en el número de respaldos, ciclos de retención y tiempo de retención.

Especialmente para SAP R/3 se han tomado medidas relacionadas con restricción en el acceso a las instalaciones del centro de datos así como la creación de rutinas de respaldo, las cuales serán detalladas posteriormente.

- **Recomendaciones**

Debido a que en SINCOR existen políticas de seguridad estrictas en cuanto a accesos a cuentas de sistema operativo, e-mail, acceso externo a través de firewalls. A los fines del presente plan no se realiza recomendación alguna relacionada con políticas de seguridad.

La seguridad informática es una tarea continua que debe ser actualizada de acuerdo a las nuevas tendencias informáticas.

2.6.4.3 Riesgo por Sabotaje y acciones terroristas

- **Medidas preventivas**

La seguridad física es extremadamente importante y en todo caso acciones de sabotaje o terroristas pueden ocurrir a pesar de la seguridad interna de las oficinas.

- **Recomendaciones**

Actualmente la seguridad física de las oficinas es adecuada y el acceso al Centro de datos está restringido y solo accede a esta sala el equipo de personas que por la naturaleza de sus actividades así lo requiere.

CAPITULO 3: ESTRATEGIA Y PROCEDIMIENTOS DE IMPLANTACIÓN

3.1 Aspectos técnicos y funcionales

A continuación se establecen los aspectos técnicos y funcionales en la implantación de una solución de *Recuperación de Desastres* basada en la instalación de una Base de Datos StandBy Oracle.

Además, del estudio de las herramientas de respaldo de SAP R/3 (brarchive) que ofrecen una solución a la aplicación y transporte de *Archive Redo Logs*.

El presente capítulo trata los siguientes temas:

1. Esquema actual de configuración
2. Esquema propuesto
3. Creación de la base de datos StandBy en el servidor de Recuperación de Desastre (Contingencia).
4. Activación de la base de datos StandBy.
5. Solución de recuperación de Oracle 8 y Oracle 8i.
6. Solución BRARCHIVE de SAP R/3.
7. Colocación en línea del sistema.
8. La Base de datos StandBy se activa y pasa a producción.
9. Puesta en marcha del ambiente tolerante a falla.

3.1.1 Esquema de configuración actual

Sistema SAP R/3

El sistema SAP R/3 está conformado por un sistema productivo, un ambiente de desarrollo y un ambiente de consolidación. Este es el esquema Standard usado en una implantación completa para SAP R/3.

Todo el ambiente SAP R/3 está centralizado en el centro de datos ubicado en Caracas y existen usuarios para el sistema en todas las localidades en las cuales SINCOR tiene operaciones, como lo son Jose, Pariaguán y Zuata. Todas estas ubicadas en el Estado Anzoátegui. A continuación un diagrama en el cual se muestra la distribución de localidades y configuración del ambiente SAP R/3.

Las opciones para recuperación en caso de cualquier contingencia se basa en el intercambio de las cintas de respaldo entre las oficinas de Caracas (sede administrativa) y las oficinas de ubicadas en Jose. En el caso del sistema SAP R/3 los respaldos son diarios y fuera de línea, por lo que se tiene una alta garantía de recuperación de los datos del sistema productivo en caso de falla, pero en caso de

perdida parcial o total del centro de datos o de la plataforma instalada para SAP R/3, los tiempos de recuperación son altos ya que no existe plataforma tecnológica alterna que soporte este tipo de falla. Ver figura 3.1.

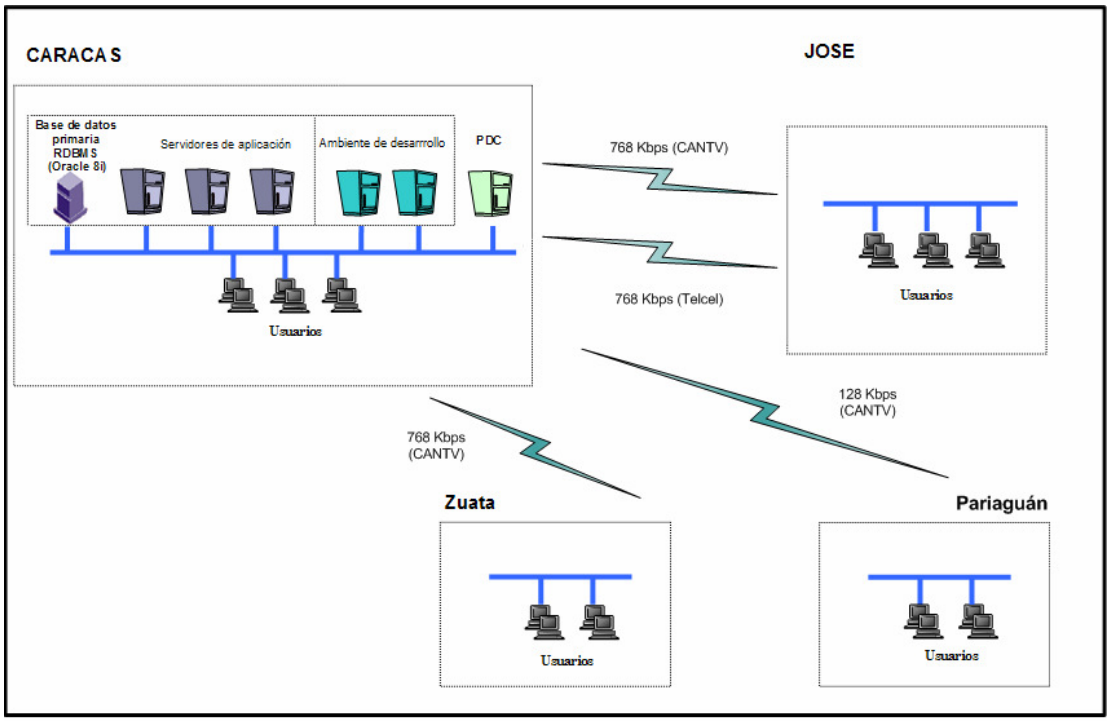

FIGURA 3.1 - LOCALIDADES SINCOR Y VISTA ACTUAL DEL AMBIENTE SAP R/3

Red WAN

Como se muestra en la figura 3.2, existen dos enlaces TDM[11] (Clear Channel) de 768 Kbps. Estos enlaces son contratados a través de CANTV y Telcel y son operados por la empresa Schlumberger- OMNES.

Estos enlaces son dedicados, es decir el ancho de banda está completamente disponible, aun cuando no se estén usando. Estos dos canales ofrecen conexión Frame Relay para servicios de video conferencia, voz y data. El CIR es de 768 Kbps para cada canal, y para la video conferencia está garantizado 512 Kbps, la voz tiene garantizado 96 Kbps (8 canales de voz a 8Kbps cada uno + 2 Kbps de header) y los datos tiene garantizado 512 Kbps, pero en caso de no haber video conferencia esta puede tomar todo el ancho de banda disponible en el canal.

[11] TechWeb - The Bussiness Technology Group. Time Divition Multiplexing. [On-line]. Disponible en: http://www.techweb.com/encyclopedia/defineterm?term=tdm&x=25&y=11

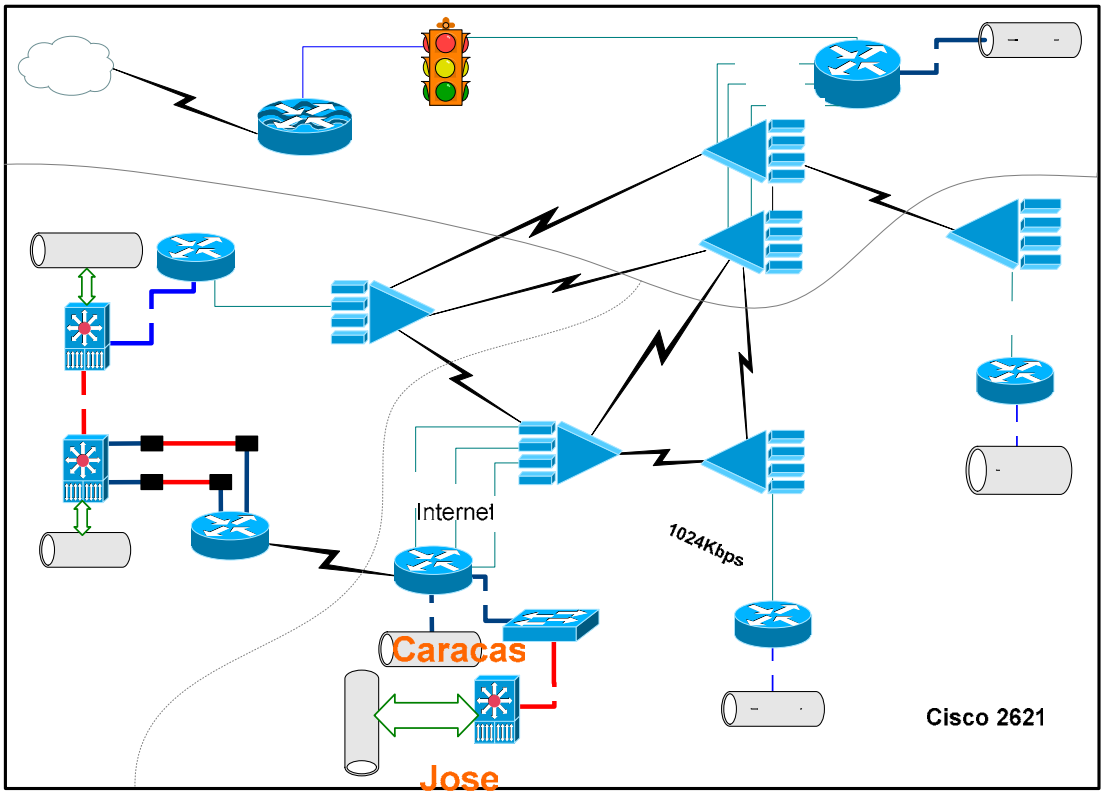

FIGURA 3.2 - DIAGRAMA DE RED SINCOR

Upgrader VLANs

3.1.2 Esquema de configuración propuesta

Las soluciones tradicionales de *recuperación de desastres* se basan en una estrategia de respaldos, donde todas o una parte de las cintas de respaldo son acumuladas en lugares diferentes a las oficinas donde se encuentran los servidores productivos. Estos lugares pueden ser: otras oficinas de la misma empresa (ubicadas en direcciones o lugares geográficos diferentes a la oficina central), bancos, otras empresas del grupo e inclusive empresas contratadas especializadas en la labor de resguardar cintas de respaldo para otras empresas.

En SINCOR, como se muestra en la figura 3.3 y 3.4, se ha implementado una solución más dinámica y en línea, para que en caso de una eventual situación de contingencia en la cual sea necesario activar el *Plan de Recuperación de Desastres*, esto se haga en el mínimo tiempo posible y con una mínima pérdida de información. Para esto se implementó una Base de Datos Oracle StandBy en combinación con las herramientas de respaldo de SAP R/3 que facilitan la aplicación de dicha técnica.

PMT VLANs

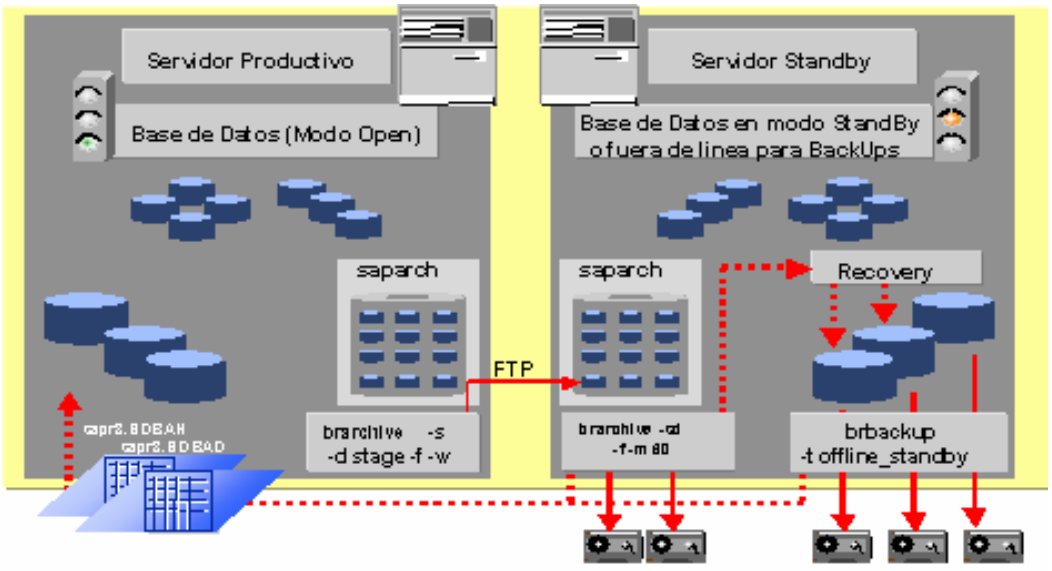

FIGURA 3.3 - ESQUEMA DEL SISTEMA DE RECUPERACIÓN DE DESASTRES DE SINCOR

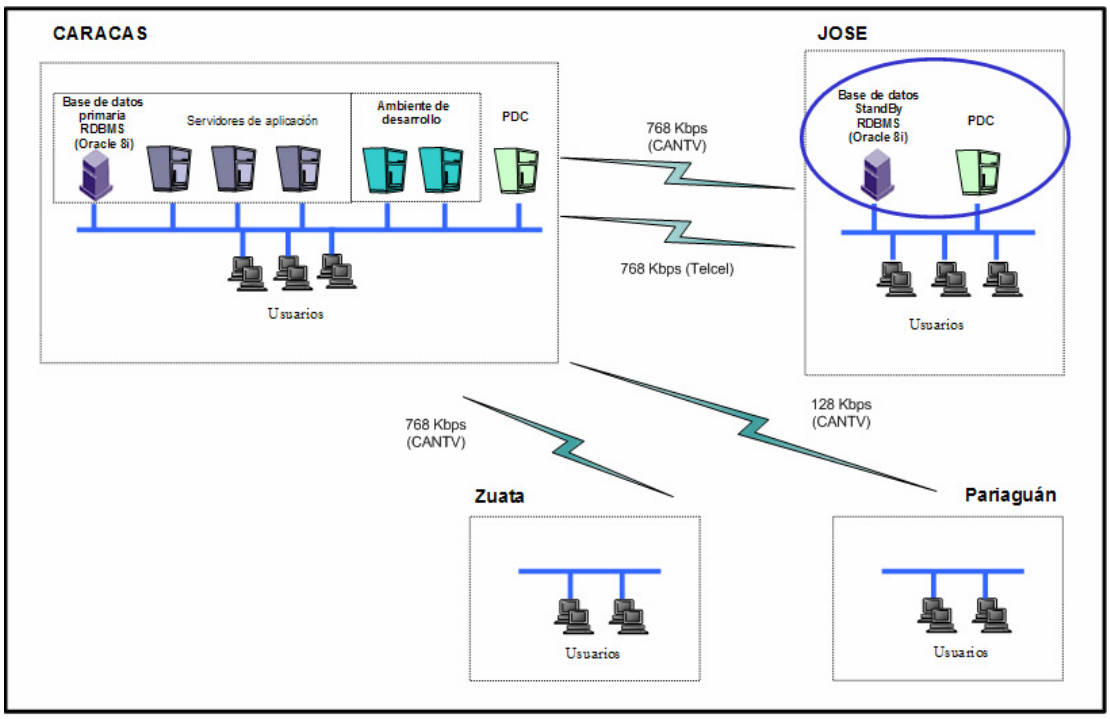

FIGURA 3.4 - LOCALIDADES SINCOR Y ESQUEMA IMPLANTADO DEL AMBIENTE SAP R/3

3.1.3 Configuración e implementación de la base de datos StandBy

Como se muestra en la figura 3.5, la base de datos primaria es aquella que contiene datos de sistema en producción. Una base de datos StandBy es una copia de la base de datos primaria utilizada esencialmente para recuperación en caso de desastre. La base de datos está normalmente en estado de *Recovery*. Esto se consigue aplicando los *Archive Redo Logs* generados en la base de datos de producción. Cuando la base de datos StandBy es activada, esta se transforma en la base de datos de producción y ya no es compatible con la base de datos primaria.[12]

La base de datos primaria y StandBy deben residir en hardware similar y sistema operativo idéntico. Las versiones de base de datos también deben ser idénticas y nunca deben cruzar versiones, es decir mantener versiones como 8.0 y 8i o 8i y 9i.

Los parámetros en los archivos de inicialización deben ser idénticos. La creación de la base de datos puede resumirse brevemente de la siguiente manera:

- En la base de datos primaria:

    a) Establecer monitoreo y rutinas para transferencia de archivos.
    b) Realizar respaldo de archivos de inicialización y archivos de datos.
    c) Crear *Controlfile* StandBy.

- Transferir archivos a la ubicación de la base de datos StandBy

- En la base de datos StandBy

    a) Crear archivos y rutinas de monitoreo.
    b) Colocar la base de datos StandBy en modo mount usando los controlfile creados.
    c) Iniciar la base de datos StandBy en modo recovery.

[12] Oracle Support Services (1999). Oracle8i Standby Database. [On-line] Disponible en: http://otn.oracle.com/deploy/availability/pdf/stby8i_twp.pdf

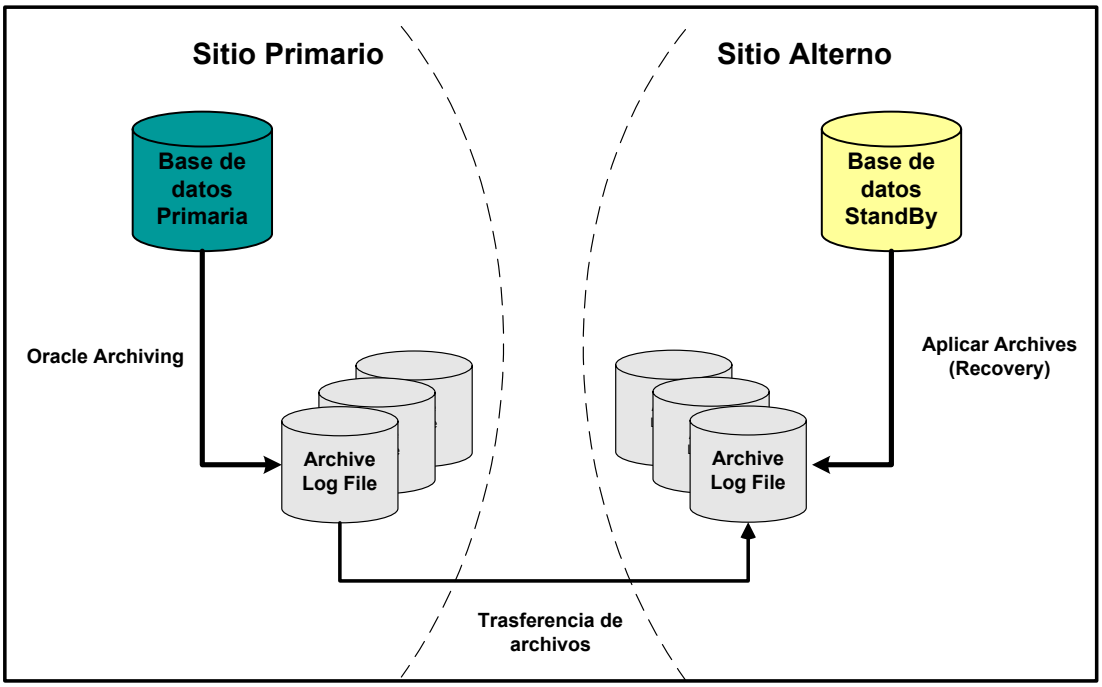

FIGURA 3.5 - DIAGRAMA GENERAL DE CONFIGURACIÓN DE LA BASE DE DATOS STANDBY

Luego de la creación de la base de datos StandBy, ésta debe permanecer en *modo recovery* y continuar la aplicación de los *Archive Redo Logs* generados en la base de datos primaria de manera de asegurar que los cambios en la base de datos primaria sean propagados a la StandBy. Estas actividades deben automatizarse de manera que la propagación ocurra rápidamente y consistentemente asegurado que la base de datos StandBy está actualizada con la base de datos primaria.

La frecuencia de transferencia y aplicación de los archives logs en la base de datos StandBy depende del *nivel de acuerdo de servicio* (S*ervice Level Agreement*). El MTTR en caso de contingencia es de 60 minutos (MTTR = 60 minutos), en consecuencia la propagación de archivos hacia la base de datos StandBy, *log switch* en la base de datos primaria y posibilidad de aplicar estos archivos en la StandBy debe ser menos a 60 minutos.

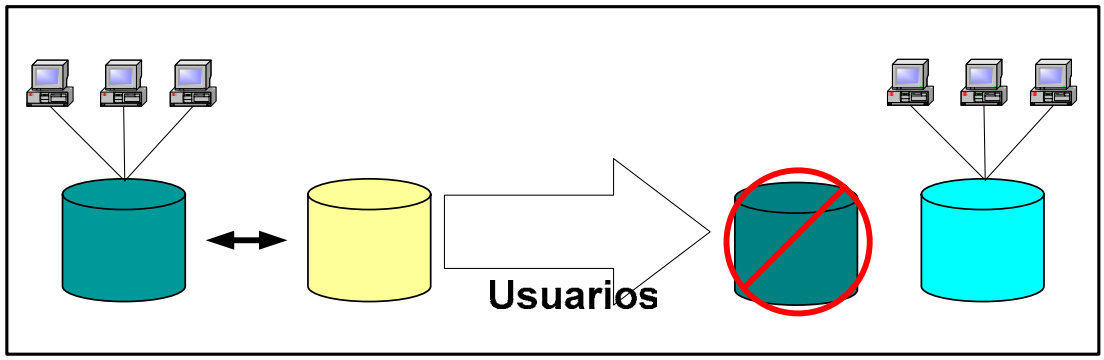

FIGURA 3.6 - LA BASE DE DATOS STANDBY SE CONVIERTE EN PRIMARIA LUEGO DE UNA FALLA

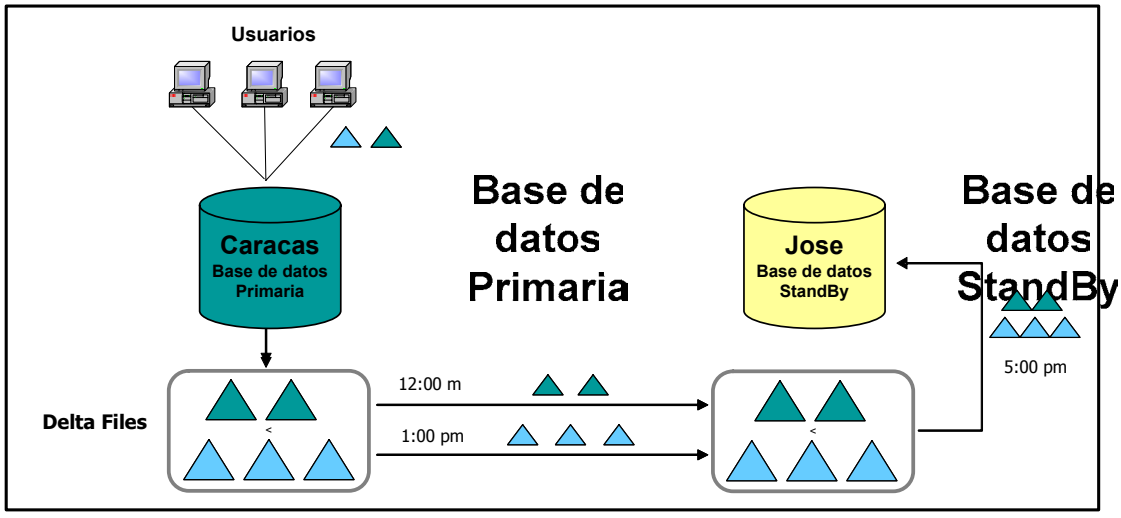

FIGURA 3.7 - PROCESO DE ACTUALIZACIÓN BASE DE DATOS STANDBY

3.1.3.1 Creación y activación de la base de datos StandBy

Debido a la concepción de la base de datos StandBy, la cual es dependiente de la base de datos primaria de la cual recibe las actualizaciones en data a través de los Archive Redo Logs, la base de datos StandBy no está disponible para operaciones tradicionales (acceso de usuarios al sistema).

Para la creación, bajo el ambiente de Windows NT 4.0 y versión 4.6C de SAP R/3, se implementó una base de datos StandBy Oracle y se diseño y evaluó un procedimiento de creación e implantación de un ambiente tolerante a falla en base a los requerimientos de SINCOR.

Procedimiento general de creación

Para creación de la Base de Datos StandBy se deben de ejecutar los siguientes pasos:

1. Se verifica el modo Archive log de la base de datos productiva (servidor productivo). Este es un paso que puede obviarse para el caso de SAP R/3, ya que los sistemas productivos SAP R/3 siempre están con el modo archive log activado.

2. Se ejecuta un respaldo total de la base de datos productiva (SAPPRDDB). En este respaldo se incluyen todos los archivos de datos (datafiles), Archive Redo Logs y online redo logs; debe ser un respaldo en frío, es decir con la base de datos cerrada (*shutdown en modo normal o immediate*).

3. Se crea el control file para la base de datos StandBy. El control file se genera desde el sistema productivo original, con el programa **svrmgrl** ó **sqlplus** de Oracle ingresando con el usuario **sys** de la base de datos.

4. Se verifica la estructura de directorios del servidor de Recuperación de Desastre. En el caso de SINCOR se utiliza un servidor con una configuración de discos similar a la del sistema en producción. Se debe verificar que el servidor presente la misma configuración de discos, y que el tipo de partición sea NTFS. Adicionalmente es recomendable verificar:

- Versión de Windows NT y nivel de Service Pack (Service Pack 6 en SINCOR).
- Memoria swap de acuerdo a los estándares SAP (4 veces memoria RAM).
- Tamaño de cache "Maximize the throughput for Network Aplications".

5. Se instala el manejador de Base de Datos Oracle8i en el servidor para Recuperación de Desastre. La versión de Oracle del servidor Recuperación de Desastre es el mismo que el del servidor productivo.

6. Se instala la instancia SAP R/3 4.6C en el servidor de Recuperación de Desastre. Para instalar la instancia central de SAP R/3 utilizar el programa R3SETUP de la manera tradicional seleccionando el Archivo CENTRAL.R3S ó CENTRDB.R3S como script de instalación.

7. Se verifica la existencia de los archivos en el servidor de Recuperación de Desastre:

<Drv>:|orant|database|init<SID>.ora
<Drv>:|orant|database|init<SID>.dba
<Drv>:|orant|database|init<SID>.sap
<Drv>:|usr|sap|<SID|sys|exe|run|strdbs.cmd

En caso contrario es necesario copiarlos desde el sistema en productivo.

8. Se restauran los archivos de datos de la Base de Datos productiva original en el servidor de Recuperación de Desastre:

- Todos los Datafiles.
- Todos los Archives Redo Logs
- Todos los On-Line RedoLogs
- Archivos de inicialización: init<SID>.ora, init<SID>.dba y init<SID>.sap (opcional).

9. Se copia el StandBy Controlfile generado en el sistema productivo al servidor de Recuperación de Desastre. Se copió el StandBy Control file en el servidor de Recuperación de Desastre en el lugar correspondiente al directorio de los control files de la base de datos StandBy. La base de datos para SAP R/3 abre tres diferentes copias del control file de la base de datos Oracle en tres diferentes directorios. Se debe de copiar el control file StandBy a todos estos directorios.

Debe de adaptarse en el archivo init<SID>.ora del directorio <drive>:\orant\database el parámetro **control_files** con los nuevos nombres de los archivos Controlfile.

Puede modificarse los nombres de los control files a los indicados en el archivo **init<SID>.ora**.

10. Se configura Oracle Network en la instancia Productiva. Esto con la finalidad que el sistema productivo se conecte y reconozca de alguna manera a la instancia StandBy de Base de Datos instalada en el servidor de Recuperación de Desastre. Se puede emplear también las herramientas *Net8 Assistant* ó *Net8 Administrator*, para configurar este archivo.

11. Se configura Oracle Network para la instancia **StandBy**. Para que la base de datos StandBy se conecte y reconozca a la instancia productiva de la base de datos instalada en el servidor productivo y para que las herramientas de respaldo SAP R/3 (brarchive) se conecten al sistema productivo.

12. Se ajustan los parámetros del archivo init<SID>.ora en la base de datos StandBy del servidor de Recuperación de Desastre. Editar y/ó copiar el archivo init<SID>.ora de la base de datos Productiva al servidor de Recuperación de Desastre y se hacen los siguientes cambios:

- El parámetro COMPATIBLE debe de ser igual al de la base de Productiva.
- DB_NAME, el mismo nombre que el de la Base de Datos Productiva.
- CONTROL_FILES debe ajustarse para que reconozcan los archivos Controlfile de la StandBy Database.
- Fijar el Parámetro LOG_ARCHIVE_DEST y STANDBY_ARCH_DEST al mismo valor. El parámetro STANDBY_ARCH_DEST solo aplica a partir de Oracle 8i.
- Incluir los siguientes parámetros:
  - LOG_ARCHIVE_DEST_STATE=enable (Oracle 8i)

- LOG_ARCHIVE_FORMAT=(mismo formato productivo, por defecto SAP ARC%s.%t)
- LOG_ARCHIVE_START=trae

13. Se crea un servicio de Windows para la de la base de datos StandBy en el servidor de Recuperación de Desastre. Se crea un servicio de Windows para la instancia de Base de Datos con la siguiente instrucción:

oradim -new -sid <SID> -startmode a

Se debe ajustar la ubicación de archivos de data (datafiles). Esto no aplica para SINCOR ya que ambos servidores tienen la misma estructura de discos.

Activación de la base de datos StandBy

Una vez instalada la Base de Datos StandBy en el servidor en el *Centro de Datos Alterno*, solo debe de arrancarse la base de datos StandBy en *Modo Mount*. No puede arrancarse en *Modo Open*, ya que de ser así se pierde la base de datos StandBy, por lo que se debe de volver a construir.

Una vez arrancada, deben de aplicarse los *Archive Redo Logs* generados desde el sistema en producción en el *centro de datos primario y* para esto existen varios métodos, unos de Oracle y otros de SAP, que se verán en el siguiente capítulo.

3.1.4 Procedimientos de respaldo y recuperación

Las opciones para recuperación en caso de cualquier contingencia se basa en el intercambio de las cintas de respaldo entre las oficinas de Caracas (sede administrativa) y las oficinas de ubicadas en Jose. En el caso del sistema SAP R/3 los respaldos son diarios y fuera de línea.

3.1.4.1 Esquema general de configuración de SAP R/3

La versión 45B de SAP R/3 basada en ORACLE ha sido configurada con los siguientes módulos funcionales:

- General Ledger (GL)
- Accounts Payable (AP)
- Account Receivable (AR)
- Treasury (TR)
- Asset Management (AM)
- Cost Controlling (CO)
- Joint Venture Accounting (JVA)
- Material Management (MM)
- Plant Maintenance (PM)

3.1.4.2 Esquema para respaldo del sistema SAP R/3

1. Sistema de Producción – Base de datos

Frecuencia de respaldo: Backup full diario

Base de datos: Fuera de línea (Offline)

Tiempo de ejecución de respaldo: 01:10 horas.

Esquema de rotación: Backup full diario durante 2 semanas, Backup full semanal durante 4 semanas y Backup full mensual durante 6 meses.

Preservación de cintas: Las cintas son resguardadas fuera del centro de datos en una caja fuerte blindada y contra fuego.

Contingencia: Semanalmente un juego de cintas de respaldo es enviado al Centro de datos alterno en Jose, Estado Anzoátegui.

2. Servidores de Aplicación

Frecuencia de respaldo: Backup full diario de Martes a sábado

Base de datos: Fuera de línea (Offline)

Tiempo de ejecución de respaldo: 02:00 horas.

Esquema de rotación: Backup full diario durante 2 semanas, Backup full semanal durante 4 semanas y Backup full mensual durante 6 meses.

Preservación de cintas: Las cintas son resguardadas fuera del centro de datos en una caja fuerte blindada y contra fuego.

Contingencia: Semanalmente un juego de cintas de respaldo es enviado al Centro de datos alterno en Jose, Estado Anzoátegui.

3. Sistema de Desarrollo/Integración y Consolidación

Frecuencia de respaldo: Backup full diario de lunes a viernes

Base de datos: Fuera de línea (Offline)

Tiempo de ejecución de respaldo: 02:00 horas.

Esquema de rotación: Rotación semanal el juego de cintas de respaldo es reutilizado.

Preservación de cintas: Las cintas son resguardadas fuera del centro de datos en una caja fuerte blindada y contra fuego.

Contingencia: Semanalmente un juego de cintas de respaldo es enviado al Centro de datos alterno en Jose, Estado Anzoátegui.

3.1.4.3 Restauración de archivos

La recomendación en relación a relacionada a que la manera más segura de respaldar un sistema bajo sistema operativo Windows NT/2000 es realizar un respaldo a nivel de sistema operativo incluyendo el archive de registro (*registry)*. Esto implica cerrar la base de datos Oracle durante al menos una hora, dos a tres horas al incluir verificación de la integridad de los datos respaldados a cinta, es este caso los archivos de la base de datos son tratados como archivos regulares.

En caso de contingencia de cualquier tipo que amerite la recuperación total o parcial del sistema, este tipo de respaldo asegura una perdida máxima de 12 horas de datos, esto en el caso de que inclusive se hayan perdido los *Archive Redo Logs* generados por la base de datos posterior a la culminación del respaldo.

La recuperación completa de todos los datos contenidos en cinta toma cerca de tres horas y esta actividad puede ser realizada por personal de operaciones con conocimientos de sistema operativo Windows NT/2000.

Posteriormente el especialista en base de datos o Administrador del sistema completará las actividades de recuperación aplicando los *Archive Redo Logs* generados por la base de datos y esto permite recuperar el sistema inclusive minutos antes de la ocurrencia de la contingencia.

3.1.4.4 Crecimiento de la data

El constante crecimiento de la cantidad de datos que es generada por un sistema ERP, como SAP R/3, ocasiona un incremento constante en el tiempo empleado para respaldar el volumen de datos, por lo tanto se recomienda en corto plazo realizar respaldos en línea de la base de datos y mantener el mismo esquema de rotación de cintas considerado previamente.

EL software utilizado actualmente para respaldo permite la configuración de agentes adicionales espaciales para la realización de respaldo *online* de la base de datos, así como mantener el respaldo de todos los restantes archivos de sistema.

3.2 Pruebas del plan de recuperación de desastres para SAP R/3

Esta sección tiene el objetivo de enumerar y presentar una la información general de las pruebas ejecutadas para la solución de Recuperación de Desastre con la utilización de Base de Datos StandBy de Oracle.

Este capítulo trata los siguientes temas:

1. Pruebas de creación de la base de datos StandBy.
2. Pruebas de copia/transferencia de logs.
3. Pruebas de aplicación de Archive Redo Logs.
4. Pruebas de activación de ambiente tolerante a falla.
5. Pruebas operativas (transaccionales) del sistema SAP R/3 en el ambiente tolerante a falla.

Para los aspectos técnicos de la solución consultar los manuales: *Disaster Recovery SINCOR Instalación y Disaster Recovery SINCOR Mantenimiento.*

3.2.1 Pruebas de creación de la base de datos StandBy

El objetivo de esta pruebas consistió en realizar la instalación y activación de la base de datos StandBy en el servidor alterno, así como realizar pruebas locales de transferencia de Archive Redo Logs.

Primera creación: Pruebas locales

Luego de realizar el reemplazo de servidores, se llevó a cabo en el centro de datos en Caracas la primera creación de la base de datos StandBy. Estas actividades se realizaron en el anterior servidor de producción, ahora renombrado a SAPPRDDR (***D****isaster* ***R****ecovery*). Las actividades desarrolladas en esta fase son:

1. Se realizó el montaje de la base de datos StandBy, lo cual se realizó a partir de la restauración del más reciente respaldo del sistema productivo. Se restauraron todos los datafiles, los Archive Redo Logs y los online redo logs. También se restauraron algunos archivos de configuración de la base de datos.

2. Se siguió el procedimiento sugerido por Oracle en la nota *70233.1: How to Create a Oracle 8i StandBy Database*[13].

3. Se hicieron pruebas de copia de Archive Redo Logs, aplicación de Archive Redo Logs, y finalmente se realizó el arranque (takeover) de la base de datos StandBy y se levantó exitosamente el sistema SAP R/3.

4. Se efectuaron pruebas de operatividad en el sistema SAP R/3 en el servidor de Recuperación de Desastre y se hicieron varias pruebas de generación de reporte, así como consulta y actualización de datos en los diferentes módulos: MM, SD, PM, FI y CO.

Segunda creación: Pruebas locales complementarias

[13] Oracle Support Services (1999). How to Create an Oracle 8i StandBy Database. [On-line]. Disponible en: http://metalink.oracle.com/metalink

Durante la fase de primera creación de la base de datos y con la finalidad de realizar pruebas con el sistema SAP R/3 ya operativo en el ambiente de recuperación de desastres, fue necesario poner en operación la base de datos StandBy. Por esta razón la primera actividad durante esta segunda creación consistió en crear nuevamente la base de datos StandBy. Las actividades desarrolladas en esta fase fueron:

1. se realizó el montaje de la base de datos StandBy, lo cual se hizo a partir de la restauración del más reciente respaldo del sistema productivo. Se restauraron todos los datafiles, los Archive Redo Logs y los online redo logs. También se restauraron algunos archivos de configuración de la base de datos.

2. Se instaló el manejador de base de datos Oracle aplicándole los mismos patches aplicados a la base de datos productiva.

3. Se instaló la instancia central productiva de acuerdo a los manuales de instalación tradicionales de SAP R/3.

4. Se configuró y montó la base de datos StandBy.

5. Se realizaron pruebas locales de transferencia de Archive Redo Logs entre los servidores. Estas pruebas se realizaron en Caracas, para lo cual se simuló un ancho de banda similar al de la WAN que conecta a las oficinas de Caracas con Jose.

Este procedimiento se realizó colocando en el centro de datos en Caracas, dos routers Cisco modelos 2600 y 1600. Para más información acerca de estas pruebas referirse al punto 3.2.2 y 3.2.3.

5. Se ejecutaron las primeras pruebas de transferencia y aplicación de Archive Redo Logs que esta vez se ejecutaron mediante el uso de rutinas automáticas creadas en el ambiente productivo de SAP R/3.

6. Se realizó el envío del servidor a la planta en Jose, Edo. Anzoátegui

7. Se realizaron pruebas de copia de Archive Redo Logs sobre la WAN que conecta a Caracas y Jose. Se hicieron mediciones y estimaciones del consumo de ancho de banda durante la copia sobre la red en tiempo real.

8. Se puso en marcha el proceso de copia de Archive Redo Logs mediante el uso de rutinas automáticas periódicos en SAP R/3, ejecutados desde el ambiente productivo. Este proceso se evaluó como una solución definitiva para la copia o transmisión de Archive Redo Logs.

9. Se hizo con éxito una segunda recuperación y arranque de la base de datos StandBy así como del sistema SAP R/3.

10. Para hacer esta instalación se utilizó la documentación desarrollada hasta el momento - *Procedimiento de Creación de la Base de Datos*. Con esta prueba el procedimiento definitivo fue mejorado sustancialmente.

3.2.2 Pruebas de copia y transferencia de Archive Redo Logs

Esta es una de las pruebas más importantes ya que de ello depende que las más recientes modificaciones sean transmitidas a la base de datos StandBy. Para ello también debe de tomarse en cuenta el ancho de banda de la WAN y como afecta esta copia de archivos globalmente sobre las comunicaciones en SINCOR entre la planta ubicada en Jose, Edo. Anzoategui y las oficinas principales ubicadas en Caracas.

Pruebas iniciales: Transferencia local

Las primeras pruebas realizadas fueron en la LAN de Caracas, simplemente copiando los Archive Redo Logs desde el servidor en producción hasta el servidor de Recuperación de Desastre. Las actividades desarrolladas en esta fase fueron:

Nota: Cada archivo ocupa aproximadamente 20 MB de memoria. Se evaluó la rapidez de la copia, tanto en la red LAN como en una emulación inicial de la WAN.

1. Se estudiaron varias posibilidades de hacer la transmisión de los Archive Redo Logs, entre ellas el uso del parámetro LOG_ARCHIVE_DUPLEX_DEST (el parámetro envía un segundo archive log a un directorio remoto) del archivo de configuración de base de datos *initMIS.ora*. Sin embargo, no se activó está opción ya que, según varias notas revisadas, el *performance* de la base de datos se vería severamente afectado en el momento de crear el segundo Archive Redo Log en un directorio remoto, el cual estaría ubicado en Jose.

2. Las pruebas se concentraron a ejecutar copias de Archive Redo Logs por medio del comando **brarchive** de SAP R/3, por varias razones:

- El comando brarchive es independiente de los procesos de base de datos.
- El comando brarchive es independiente de SAP R/3.
- Es fácil de configurar y de ejecutar.
- Presenta varias alternativas de solución para la transmisión de Archive Redo Logs.

3. La primera prueba de transmisión se ejecutó a nivel comando con las opciones:
brarchive –s –d disk –f –c [-w] [-k yes]
Este comando copia a un directorio remoto (especificado en la variable archive_copy_dir del archivo initMIS.sap) los Archive Redo Logs. El comando ejecuta de manera adecuada la copia, sin embargo, el ancho de banda se ve en algo afectado por dicha copia. Además SAP recomienda que se haga la copia con la opción **–w**, para verificación de la copia, por lo que el tiempo de copia se incrementó.

También se probó la opción **–k yes**, para compresión de los archivos. La transferencia de archivos tomó menos tiempo, pero debe igualmente utilizarse la opción **–w**. Además el log debe de aplicarse posteriormente por lo que debe de ser descomprimido en la base de datos StandBy, lo cual debe hacerse manualmente, por lo que tendía a complicar la solución. Finalmente, esta opción fue descartada.

4. Para la segunda prueba de transmisión se ejecutó a nivel comando con las opciones: **brarchive –s –d stage –f –c**

Adicionalmente, se fijaron las variables:
stage_copy_cmd=rcp, **remote_host**
remote_user y **archive_stage_dir**.

Para poder ejecutar este comando debe instalarse el servicio *Remote Shell Service* en el servidor de Recuperación de desastre. Para más detalles referirse al apéndice II del manual *Disaster Recovery SINCOR Instalación.*

Este comando copia a un servidor remoto, con Remote Shell Service activado, los Archive Redo Logs. El comando ejecuta de manera adecuada la copia con un mejor rendimiento y no es necesaria la utilización del parámetro **-w**.

El único problema de este comando es que solo puede ejecutarse en una sesión abierta de usuario. Se probaron varias maneras de ejecutarlo utilizando el comando **at** y los Jobs de SAP R/3 sin éxito alguno.

5. La tercera prueba de transmisión, y la más interesante, se ejecutó a nivel comando con las opciones: **brarchive –s –d stage –f –c**

Adicionalmente fueron incluidas en el archivo initMIS.sap las variables:
stage_copy_cmd=ftp
remote_host, **remote_user** y **archive_stage_dir**.

Para poder ejecutar este comando debe instalarse el servicio FTP de Microsoft Internet Service Manager en el servidor destino (servidor de Recuperación de desastre). Para más detalles referirse al apéndice III del manual *Disaster Recovery SINCOR Instalación.*

Este comando copia a un servidor remoto con el servicio FTP activado los Archive Redo Logs con la utilización de la utilidad **sapftp**. El comando ejecuta de manera adecuada la copia con un mejor rendimiento ante el ancho de banda y no es necesaria la utilización del parámetro **-w**.

Fue el comando más interesante ya que presentó la posibilidad de ser ejecutado desde una sesión de usuario, desde el comando **at** e inclusive desde un Job de SAP R/3, sin ningún problema.

Pruebas finales: Locales simulando una WAN

La pruebas finales tenían el objetivo de realizar las mediciones del consumo de ancho de banda por parte de los Archive Redo Logs que son enviados a la base de datos StandBy, así como ejecutar la copia de los Archive Redo Logs mediante la programación de una tarea periódica en SAP R/3 a nivel de producción y mediante la utilización de la herramienta **brarchive**. Las actividades desarrolladas en esta fase son:

1. Para utilizar el protocolo FTP para la transmisión del archivo, se utilizó la herramienta **brarchive** con la opción **–d stage** y las variables **stage_copy_cmd=ftp** y **archive_stage_dir** en el archivo initMIS.sap.

2. No se activó la opción **–f** (modo en espera), ya que se quiere tener un control y monitoreo desde el sistema SAP R/3 sin necesidad de entrar al sistema operativo.

3. Se añadió posteriormente la opción **–n 3**, al comando **brarchive** para limitar a tres el número de Archive Redo Logs a ser transmitido por cada ejecución.

4. Con la finalidad de automatizar el proceso de copia de Archive Redo Logs, se creo en la transacción SM37 una tarea periódica, que se ejecuta cada hora. Esta tarea es la encargada de transmitir los Archive Redo Logs pendientes desde el servidor de producción al servidor de Recuperación de Desastre en el cual se encuentra la base de datos StandBy (SAPPRDDR).

5. La simulación del ancho de banda se realizó colocando en el centro de datos en Caracas dos routers Cisco modelos 2600 y 1600 a los cuales se conectaron los servidores de SAP R/3 Primario y de Recuperación de Desastre. Se simuló una conexión a 512 Kbps con la finalidad de evaluar el consumo de ancho de banda en el envío de Archive Redo Logs entre las localidades de Caracas y Jose. El esquema utilizado para realizar las pruebas de transferencia de archivos es el mostrado en la figura 3.8.

El objetivo de esta prueba era medir la utilización de ancho de banda y la duración de los picos de utilización.

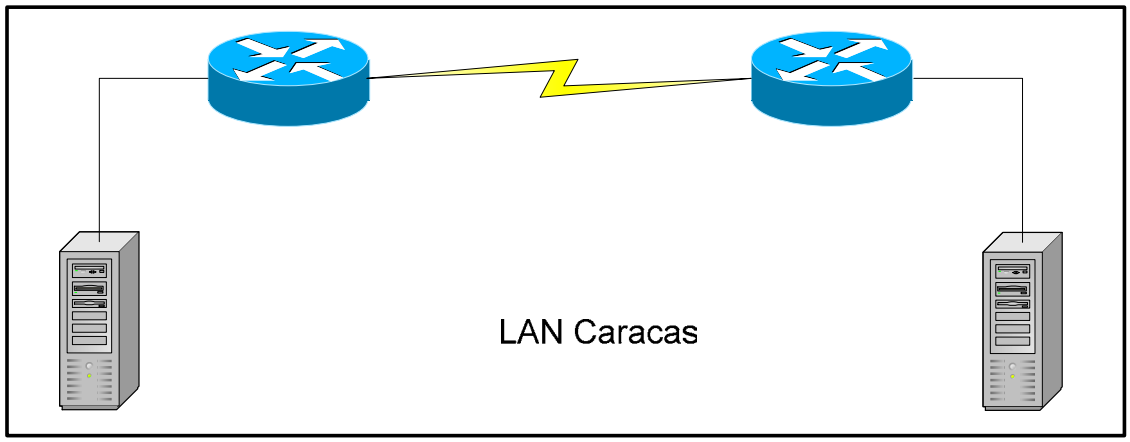

FIGURA 3.8 - CONEXIÓN PARA SIMULACIÓN DE TRANSFERENCIA DE ARCHIVE REDO LOGS

3.2.3 Resultados de las pruebas de monitoreo de la red WAN

Durante la ejecución de la copia de Archive Redo Logs desde el servidor de Producción (SAPPRDDB) al Servidor de Recuperación de Desastre (SAPPRDDR), el equipo de tecnología de SINCOR efectuó mediciones de la carga de la red WAN que conecta las oficinas de Caracas con la planta de Jose en Puerto la Cruz.

Las pruebas se realizaron mediante la transferencia de paquetes de datos del mismo tamaño de los que genera la base de datos y que deben ser transferidos al centro de datos alterno en Jose para luego aplicarlos y actualizar la base de datos StandBy. En la tabla 3.1 y en la figura 3.9 se muestran los resultados de las pruebas de transferencia de Archive Redo Logs.

3.2.3.1 Resultados de las pruebas de transferencia ftp Caracas-Jose

A continuación se presentan los resultados de las pruebas de transferencia de archivos desde Caracas hacia Jose a través de la WAN. Estas pruebas se realizaron durante la jornada laboral habitual. La transferencia se hizo a través de ftp y enviado un archivo (Archive Redo Log) generado por Oracle y con el cual se realiza la actualización de la base de datos del sistema de contingencia.

Premisas:

- El envió se realizó durante la jornada laboral de 8 horas en la cual hay mayor tráfico en la WAN.
- El envío se realizó utilizando ftp
- El tipo de archivo enviado corresponde a un Archive Redol Log generado por Oracle versión 8i cuyo tamaño, está fijado en 20 MB.

TABLA 3.1 - PRUEBAS DE TRANSFERENCIA FTP CARACAS-JOSE

FECHA	HORA	BYTES ENVIADOS (MB)	ELAPSED TIME (S)	TASA DE ENVÍO (KBYTES/S)	COMENTARIOS
DÍA 01	8:15 AM	20	285.75	73.38	
	8:45 AM	20	285.75	73.38	
	9:45 AM	20	273.40	76.67	
	10:25 AM	20	277.51	75.56	
	11:25 AM	20	273.41	76.68	
	11:55 AM	20	267.97	78.25	
	1:20 PM	20	285.72	73.36	
	1:50 PM	20	311.30	67.36	
	2:10 PM	20	810.45	25.87	
	2:45 PM	20	750.34	27.95	
	3:10 PM	20	630.19	33.27	
	3:30 PM	20	277.66	75.52	
	3:45 PM	20	271.06	77.36	
	4:15 PM	20	277.66	75.51	
DÍA 02	8:00 AM	20	547.69	38.29	En curso replicación diaria
	8:30 AM	20	480.41	43.65	En curso replicación diaria
	9:05 AM	20	361.55	58.00	En curso replicación diaria
	9:30 AM	20	285.75	73.38	
	10:00 AM	20	302.05	69.42	
	10:30 AM	20	285.72	73.39	
	11:00 AM	20	284.86	73.61	
	11:30 AM	20	855.13	24.52	Videoconferencia piso 28
	11:45 PM	20	487.55	43.01	Videoconferencia piso 28
	12:00 PM	20	292.22	71.76	
	1:10 PM	20	272.98	76.81	
	1:30 PM	20	269.92	77.68	
	2:00 PM	20	291.59	71.91	
	2:30 PM	20	269.50	77.81	
	3:00 PM	20	257.50	81.43	
	3:30 PM	20	255.44	82.09	
	4:00 PM	20	277.36	75.60	
	4:30 PM	20	274.00	76.53	
	5:00 PM	20	257.17	81.53	
DÍA 03	8:10 AM	20	796.00	23.64	Enlace ocupado por procesos
	8:30 AM	20	735.74	28.50	Enlace ocupado por procesos
	9:05 AM	20	722.30	29.03	Enlace ocupado por procesos
	9:30 AM	20	612.42	34.24	Enlace ocupado por procesos
	10:00 AM	20	644.50	32.53	Enlace ocupado por procesos
	10:30 AM	20	664.08	31.58	Enlace ocupado por procesos
	11:00 AM	20	645.09	32.50	Enlace ocupado por procesos
	11:30 AM	20	633.77	33.09	Enlace ocupado por procesos
	11:45 PM	20	657.73	31.88	Enlace ocupado por procesos
	12:00 PM	20	681.00	30.75	Enlace ocupado por procesos
	1:10 PM	20	664.08	31.58	Enlace ocupado por procesos
	1:30 PM	20	645.09	32.50	Enlace ocupado por procesos
	2:00 PM	20	657.73	31.88	Enlace ocupado por procesos
DÍA 04	8:10 AM	20	540.42	38.80	
	8:30 AM	20	293.64	71.41	
	9:05 AM	20	359.89	58.26	
	9:30 AM	20	334.17	62.75	
	10:00 AM	20	331.19	63.31	
	10:30 AM	20	277.51	75.56	
	11:00 AM	20	273.41	76.68	
	11:30 AM	20	267.97	78.25	
	11:45 PM	20	285.72	73.36	
	12:00 PM	20	272.98	76.81	
	1:10 PM	20	269.92	77.68	
	1:30 PM	20	291.59	71.91	
	2:00 PM	20	277.36	75.60	
	2:30 PM	20	285.72	73.36	
	3:00 PM	20	296.47	70.73	

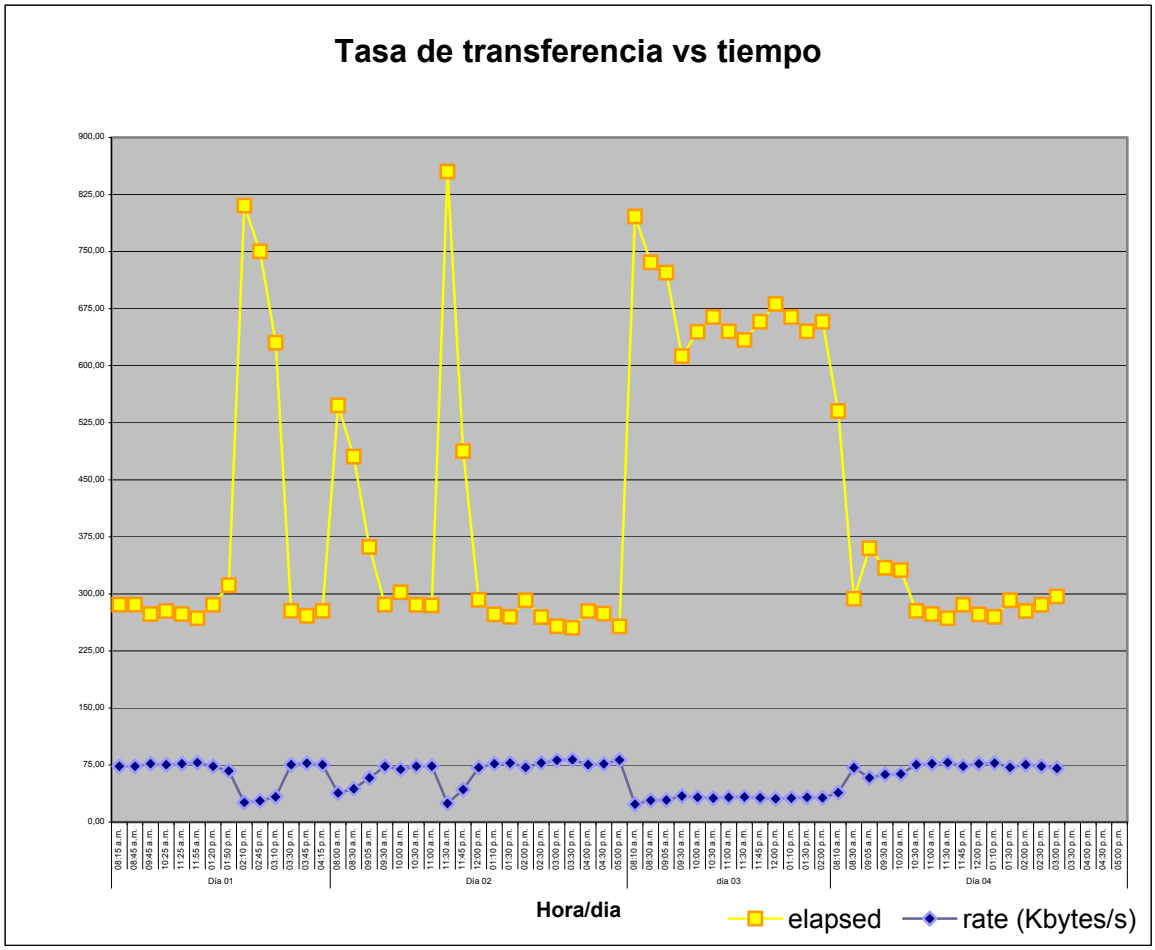

FIGURA 3.9 - RESULTADO GRÁFICO DE PRUEBAS DE TRANSFERENCIA FTP CARACAS-JOSE

3.2.4 Pruebas de operación del sistema SAP R/3 en el servidor de Recuperación de Desastre

Una vez realizados las pruebas de arranque de la base de datos StandBy, así como del sistema SAP R/3, se ejecutaron varias transacciones de prueba sobre el sistema SAP R/3 en el ambiente de Recuperación de Desastre.

Primera Prueba: centro de datos primario

Se realizó una primera prueba de arranque de la base de datos StandBy del servidor Recuperación de Desastre. Se arrancó también la instancia SAP R/3 en el mismo servidor. Todas estas tareas se hicieron con éxito.

Durante la primera activación del sistema SAP R/3 y de la base de datos StandBy realizado en las pruebas locales en Caracas, se ejecutaron varias transacciones

funcionales las cuales fueron exitosas pero no fueron documentadas. Las pruebas incluyeron:

- Realización de pagos en finanzas, las cuales implican actualizaciones en costos y la generación de documentos contables.

- Pruebas en órdenes de mantenimiento de planta. Se realizaron varias operaciones con órdenes de mantenimiento, como cambios de status, distribución de costos, etc.

- Se realizaron pruebas de entradas de mercancía y facturación sobre pedidos abiertos.

3.2.4.1 Segunda Prueba: Centro de datos alterno

Debido a que no fueron documentadas las primeras pruebas operacionales del sistema SAP R/3, se decidió realizar un segundo conjunto de pruebas con el sistema ya instalado en el centro de datos alterno. Estas pruebas se realizaron luego de transcurridas dos semanas en las cuales se habían realizado la transferencia y aplicación de Archive Redo Logs en el servidor de Recuperación de Desastre.

3.3 Puesta en operación del ambiente de recuperación de desastres para SAP R/3

La puesta en operación del plan de recuperación de desastres para SAP R/3 se realizó luego de haber completado un exhaustivo conjunto de pruebas. las cuales fueron detalladas en los puntos anteriores y pueden resumirse de la siguiente forma:

1. Pruebas de creación de la base de datos StandBy, pruebas preliminares y pruebas complementarias en las cual se activó la base de datos StandBy.

2. Pruebas operacionales de los diferentes módulos del sistema SAP R/3, para lo cual se activó la base de datos StandBy convirtiéndose en base de datos en producción.

3. Pruebas de transferencia a través de la WAN de los Archive Redo Logs. En esta fase se realizaron simulaciones del ancho de banda para evaluar dicho consumo de ancho de banda.

Como resultado de esta instalación se obtuvo el ambiente de Recuperación de Desastre ya instalado en el centro de datos alterno ubicado en Jose, con la correspondiente base de datos StandBy activa y la activación de rutinas automáticas y periódicas para el envío y aplicación de Archive Redo Logs desde la base de datos primaria hacia la base de datos StandBy.
Al igual que en la fase de segunda creación, fue necesario crear nuevamente la base de datos StandBy debido a que esta fue puesta en operación para realizar pruebas de operatividad del sistema SAP R/3.

La última creación de la base de datos StandBy se realizó en el centro de datos alterno ubicado en Jose. Se realizó a través de una conexión remota desde caracas hacia el servidor de Recuperación de Desastre SAPPRDDR.

Las actividades desarrolladas en esta última etapa fueron:

1. Creación de la base de datos StandBy a partir de la restauración del más reciente respaldo del sistema en producción. Se restauraron todos los datafiles, los Archive Redo Logs y los Online Redo Logs. También se restauraron algunos archivos de configuración de la base de datos.

2. Se aprovechó la instalación ya existente de la segunda prueba, instalación de SAP R/3, instalación de Oracle y toda la configuración la cual no fue necesario modificarla.

3. Se puso en operación en *modo mount* de la base de datos StandBy.

4. Inicio de la aplicación de los Archive Redo Logs y la puesta en operación, desde el sistema productivo SAP R/3, de las rutinas automáticas periódicas de copia y aplicación de Archive Redo Logs.

3.4 Protocolos de mantenimiento

El presente documento tiene el objetivo de establecer los aspectos técnicos y funcionales relacionados con el mantenimiento de una solución de recuperación de desastre basada en la instalación de una base de datos StandBy ORACLE.

Se añade también el estudio de las herramientas de Respaldo de SAP (brarchive) que ofrecen una solución a la aplicación y transporte de Archive Redo Logs.

El presente punto trata los siguientes temas:
1. Mantenimiento periódico de la base de datos StandBy.
2. Mantenimiento eventual de la base de datos StandBy.
3. Puesta en marcha: La base de datos StandBy pasa a ser productiva.

Para obtener más detalles de los aspectos relacionados con la instalación de la solución de recuperación de desastre, se puede consultar el manual **Disaster Recovery SINCOR Instalación**.

3.4.1 Mantenimiento de la base de datos StandBy

A continuación se enumeran los diferentes tipos de chequeos que deben ejecutarse en los sistemas para, ya sea, comprobar la ejecución de los procesos que mantienen actualizada a la base de datos StandBy ó para ejecutar chequeos eventuales y/o modificaciones a la estructura de la base de datos, entre otras.

3.4.1.1 Chequeos periódicos obligatorios

Los chequeos diarios a efectuar para comprobar la copia y aplicación de los Archive Redo Logs son los siguientes:

1. Verificar rutina automática de copia de Archive Redo Logs.

Verificar que la rutina *DISASTER_RECOVERY_COPIAR_LOGS* para copiado ha sido ejecutado con éxito en la transacción SM37. Verificar la secuencia de archives, el status de retorno del comando **brarchive** y verificar la existencia de los archives en el servidor de Recuperación de Desastre.

2. Verificar rutina automática de aplicación de Archive Redo Logs en la base de datos StandBy.

Verificar que la rutina *DISASTER_RECOVERY_APLICAR_LOGS* para aplicar los Archive redolog en la base de datos StandBy ha sido ejecutado con éxito en la transacción SM37. Verificar la secuencia de archives aplicados y el borrado, compactado y copia a disco. Verificar el status de retorno del comando **brarchive**.

Verificar rutina automática de archivos adicionales.
En caso de estar activo el Job para copia de otros archivos mediante XCOPY; Verificar que la rutina *DISASTER_RECOVERY_COP_DIRECTORIO* ha sido ejecutado con éxito en la transacción SM37. La rutina debe borrar del directorio **sapbackup** los viejos archivos de respaldo compactados.

3. Verificar transacción DB14.

Si se aplica la herramienta brarchive, con jobs, con comando ***at*** o manualmente, se puede verificar la transacción DB14 en el sistema SAP R/3, presionando el botón "BRARCHIVE" y visualizando los diferentes redo logs generados, fechas de ejecución y Archive Redo Logs copiados y respaldados

4. Verificar transacción DB12.

Adicionalmente en la transacción DB12 botón "Status *of most recent redo logs*", se visualizan la secuencia de logs generada, y el log que se está trabajando en el momento (log en línea). Si se utiliza el comando **brarchive** se visualiza si el archive log fue respaldado (copiado a la base de datos StandBy).
Adicionalmente se verifica con el botón "*Log directory status*" el espacio libre del directorio de archive redo log de producción.

5. Borrar Archive Redo Logs de respaldo.

Los archivos de logs de respaldo existentes en el directorio <Drive>:\oracle\MIS\saparch (D:\oracle\MIS\saparch) pueden ser borrados tanto

manualmente ó con el comando **sapdba –cleanup**. Las variables que se pueden ajustar son las siguientes:

expir_period_sapdba_normal (por defecto 11 días)
ffexpir_period_daily_check (por defecto 5 días)
expir_period_brbackup (por defecto 30 días)
expir_period_brarchive (por defecto 30 días)
expir_period_oracle_trace (por defecto 1 día)

En el servidor de Producción el comando se puede programar en la transacción DB13, para el servidor StandBy se puede incluir la rutina de copia de archivos.

6. Verificar el servicio Remote shell Service en el servidor de Recuperación de Desastre.

Verificar que el servicio *Remote Shell Service*, en el servidor de Recuperación de Desastre (SAPPRDDR), arranque con el usuario administrador del sistema SAP R/3, <sid>adm (ADMINSAP\sidadm). Ajustar el password, en caso de ser necesario.

3.4.1.2 Chequeos periódicos adicionales

Dentro de los chequeos diarios se puede incluir algunas tareas adicionales para el caso de implementar la solución con las herramientas de Oracle8 u Oracle8i:

1. Consulta de la vista V$ARCHIVED_LOG (No ejecutar con brarchive activo)
Se pueden verificar los archive los recibidos en la vista V$ARCHIVED_LOG de la base de datos StandBy.

2. Script para verificación de archivos faltantes (No ejecutar con brarchive activo)
Se puede tener este script para verificar, los archivos faltantes en la base de datos StandBy: Ver el Script en el APENDICE II del Manual de **Disaster Recovery SINCOR Mantenimiento**.

3. Consulta de la vista V$LOG_HISTORY (No ejecutar con brarchive activo)
En la base de datos StandBy se puede verificar en la vista V$LOG_HISTORY. Ejecutar el siguiente query para consultar los archives aplicados:
SRVMGR> select thread#, max(sequence#) AS "Last Applied Log"
SRVMGR > from v$log_history
SRVMGR > GROUP BY thread#;
Esta vista se puede verificar y comparar en ambos servidores.

3.4.1.3 Tareas eventuales y recomendaciones de mantenimiento

1. Parada de procesos BRARCHIVE

Parada de procesos **brarchive** en espera (opción –f). Para detener un proceso brarchive con la opción de espera activada se ejecuta el comando: **brarchive –f**

stop. El comando que este ejecutándose con esta opción (-f), ya sea en una sesión de usuario activa, o como residente en memoria, será detenido de inmediato.

Puede detenerse con el "Task Manager" de Windows NT (Tab "Processes"), siempre borrar el archivo <Drive>:\oracle\<SID>\saparch\.lock.bra. Casi siempre debe de volverse a hacer reset de los comandos **brarchive**.

Parada de procesos SAP R/3 de copia y aplicación de Archive Redo Logs. Para detener una tarea programada, se debe ejecutar la transacción SM37 seleccionar y desplegar los Jobs. Posteriormente seleccionar cada uno de ellos y ejecutar el menú **Job → Scheduled Job → Cancel**. Para volverlos a programar posteriormente seleccionar el Job y ejecutar el menú: **Job → Scheduled Job → Release**.

2. Terminación irregular de Jobs de copia o aplicación de Archivelog

En estos casos se debe chequear si el comando **brarchive** todavía se está ejecutando a nivel de sistema operativo donde se programó su ejecución. Esto se puede verificar en el "Task Manager" de Windows NT. Se puede chequear el directorio **saparch** correspondiente al servidor que presenta el problema, y verificar el log de respaldo de más reciente modificación (archivo de tipo [cadena de letras].svd ó [cadena de letras].sve). Revisar en este log si se dio algún error ó por el contrario sigue ejecutándose el comando brarchive (el log va cambiando).

En caso de seguir ejecutándose el comando brarchive, esperar a que este se complete ó detener el comando en el "Task Manager" de Windows NT y borrar el archivo de bloqueo generado en **saparch** llamado **.lock.bra**.

Esto también se puede verificar en la transacción DB14 de SAP R/3, ya que el comando sigue generando líneas en los logs de respaldo de archive log. Se recomienda siempre esperar a que se complete el comando **brarchive**.

3. Terminación irregular de BRARCHIVE

Es posible que después de que el programa brarchive termine de manera irregular, este no pueda volver a ejecutarse.

Borrar el archivo <Drive>:\oracle\<SID>\saparch\.lock.bra, ya que éste bloquea la utilización del comando brarchive.

4. Verificación de la secuencia de Archivelogs a ser aplicados en la base de datos StandBy

Para verificar la secuencia de Archive redo log a ser aplicado en la base de datos StandBy del servidor Disaster Recovery, se recomienda hacer lo siguiente:

- Entrar al Windows NT y ejecutar el modo comando (run CMD).
- Ejecutar el comando de Oracle SVRMGRL con **connect internal**.
- Ejecutar el comando "**RECOVER STANDBY DATABASE UNTIL CANCEL;**"
- Verificar el número de archive que la base de datos StandBy requiere.
- Ejecutar el comando **CANCEL** y salir del programa.

Esta opción puede ser necesaria para verificar el próximo archive redo log, copiarlo, y poner en marcha la recuperación, ya sea con el comando SQL RECOVER STANDBY DATABASE ó con el comando **brarchive** a nivel de sistema operativo.

5. Reinicio/borrado de Logs de comando BRARCHIVE

Puede darse el caso en que se pierda la secuencia de logs a ser copiados o aplicados en cualquiera de los dos servidores. Para arreglar esto quedan dos soluciones, la más sencilla es copiar los Archive Redo Logs faltantes al directorio **saparch**, pero, dependiendo del problema, no siempre es la mejor solución. En estos casos debe de hacerse reset a los logs de brarchive y volver a arrancar el proceso. Para hacer esto seguir los siguientes pasos:

1. Borrar todos los logs de la forma **[cadena de letras].svd** ó **[cadena de letras].sve** del directorio **saparch** (D:\oracle\MIS\saparch).
2. Eliminar el archivo arch<SID>.log (archMIS.log).
3. Eliminar ó mover del directorio **saparch** los Archive Redo Logs que no se requieren para el respaldo a ser ejecutado. Mantener los Archive Redo Logs a partir de la secuencia de la que se quiere hacer copia ó aplicación y respaldo.
4. Ejecutar nuevamente el comando **brarchive**, se vuelven a generar nuevos archivos de logs para dicho comando. A partir de aquí el brarchive verifica la secuencia de las próximas ejecuciones en el archivo arch<SID>.log (archMIS.log).

3.5 Resultados

Luego de realizar el desarrollo del plan para la implantación de un ambiente tolerante a fallas para el sistema SAP R/3 en SINCOR y de haber realizado las investigaciones pertinentes para ajustarse a los requerimientos y recursos disponibles, se obtuvo un sistema tolerante a fallas para el sistema SAP R/3.

3.5.1 Resultados obtenidos en base a los objetivos planteados

1. Se realizó la evaluación de requerimientos de hardware, software y telecomunicaciones.

2. Se realizó el análisis de posibles riesgos para la plataforma tecnológica actualmente instalada en el centro de datos primario ubicado en las oficinas principales de SINCOR en Caracas. Los detalles de este análisis se encuentra en el documento Risk Assesment, el cual por razones de confidencialidad y seguridad no se detallan en este documento. En el punto 2.6 de este documento se trata lo

relacionado con la planeación y estimación de riesgos así como los eventuales desastres y prevención.

3. Se realizó en base a las premisas establecidas el diseño y la implantación una infraestructura de sistemas tolerante a fallas que permita lograr alta disponibilidad y acceso continúo a los datos del sistema SAP R/3.

4. Se definieron e implantaron las estrategias de respaldo para recuperación de desastres, planeación de una metodología avanzada de respaldo para la protección en caso de fallas y para una rápida recuperación de los servidores de bases de datos en caso de desastre.

5. se generaron los procedimientos que permiten la activación del ambiente replica en caso de falla y posterior restauración, una vez solucionada la falla al centro de datos primario.

3.5.2 Procedimientos en caso de una eventual situación de desastre

A continuación se describen los procedimientos generados como parte de la implantación del plan d recuperación de desastres para el sistema SAP R/3.

Adicionalmente se mencionan algunos de los procedimientos a fin de garantizar la continuidad de las operaciones de la empresa, que fueron desarrollados como parte de la implantación en el ámbito de toda la empresa de un plan de recuperación que tiene como alcance todos los sistemas de redes y sistemas de información de SINCOR.

1. Disaster Recovery SINCOR Instalación: Tiene el objetivo de tratar en detalle lo relacionado con la creación de la base de datos StandBy Oracle 8i, procedimiento de montaje y puesta en línea de la base de datos StandBy de Oracle para la Solución de Recuperación de Desastre de SINCOR. así como el estudio de las herramientas de Respaldo de SAP (brarchive) que ofrecen una solución a la aplicación y transporte de Archive Redo Logs.

2. Disaster Recovery SINCOR Mantenimiento: Tiene el objetivo de tratar en detalle todos los aspectos técnicos y funcionales relacionados con el mantenimiento de una solución de Recuperación de Desastre basada en la instalación de una Base de Datos StandBy ORACLE. Se añade también el estudio de las herramientas de Respaldo de SAP (brarchive) que ofrecen una solución a la aplicación y transporte de Archive Redo Logs.

3. Disaster Recovery SINCOR Pruebas: Tiene el objetivo de enumerar y presentar una documentación general de las pruebas ejecutadas para la solución de Recuperación de Desastre con la utilización de Base de Datos StandBy de Oracle.

A continuación se mencionan algunos de los procedimientos existentes en la organización, los cuales fueron desarrollados a fin de garantizar la continuidad de las operaciones de la empresa:

1. Restaurando un Servidor NT de un desastre: El propósito de esta guía es servir de apoyo en el proceso de restauración de un servidor NT de un desastre, el cual consiste en aplicar herramientas al servidor afectado que permitan la pronta operatividad del mismo.

2.

3. Procedimientos para Backup Diferencial: El propósito de esta guía es servir de apoyo en el proceso backup diferencial a través de la WAN, el cual consiste en un backup diferencial de los drive F y G de Caracas en Jose y viceversa.

4. Procedimiento de Backup para SAP R/3 y base de datos Oracle: El propósito de éste procedimiento es de servir de apoyo en el proceso de respaldo de los ambientes SAP R/3 y de las bases de datos Oracle.

5. Password List Procedure: El propósito de éste es de marcar las directrices y políticas en relación a seguridad de claves de acceso.

6. Guía de Instalación de Netscape Messaging Server: El propósito de esta guía es servir de apoyo en el proceso de instalación de el servicio de mensajeria de netscape.

CAPITULO 4: ASPECTOS ADMINISTRATIVOS

4.1 Recursos empleados en la implantación

El equipo de trabajo que participó en la implantación del plan de recuperación de desastres para SAP R/3 estuvo conformado por especialistas del área SAP, administración de bases de datos Oracle, telecomunicaciones y redes.

Mi participación en este proyecto estuvo presente desde la fase de concepción del mismo, definición del alcance, objetivos y evaluación de alternativas. Posteriormente en la fase de implantación como gerente de proyecto y en la parte técnica desempeñando actividades de administración de bases de datos.

A continuación se detalla la cantidad de especialistas participantes así como la dedicación aproximada en horas a cada actividad principal requerida para llevar a cabo la implantación:

TABLA 4.1 - RECURSOS DE PERSONAL Y ASIGNACIÓN A LAS ACTIVIDADES DEL PLAN

RECURSO	CANT.	PLANIFICACIÓN (HORAS)	IMPLANTACIÓN (HORAS)	PUESTA EN PRODUCCIÓN Y CERTIFICACIÓN (HORAS)	TOTAL (HORAS)
Consultor SAP R/3 - Basis (*)	01	50	120	80	250
Especialista Oracle	01	10	30	20	60
Coordinador de Proyecto	01	24	20	20	64
Espec. Telecom	01	8	-	16	24
Espec. Redes	01	8	16	8	32
Funcional de SAP	01	8	8	16	32
Total (horas)		*108*	*194*	*160*	**462**

(*) Consultoría externa

4.1.1 Perfil del personal requerido

4.1.1.1 Recursos profesionales externos

Consultor SAP R/3 – Basis:

- Mínimo dos años de experiencia en SAP – Basis
- Experiencia en mantenimiento de sistemas bajo plataforma Windows NT
- Experiencia en implantación de sistemas SAP R/3

- Experiencia en implantación de procedimientos de respaldo y recuperación
- Experiencia en RDBMS Oracle versión 8i

4.1.1.2 Recursos profesionales SINCOR

Los recurso fueron asignados por la Gerencia de IS/IT & Telecom. No se detalla la descripción del perfil requerido.

Coordinador de proyecto:
- Experiencia en proyectos técnico del área de IS/IT

Administrador de base de datos:
- Experiencia en instalación, configuración y puesta en marcha de bases de datos Oracle8i.
- Experiencia en respaldo y recuperación.

Especialista en Telecom:
- Experiencia en medición de tráfico en redes WAN/LAN

Especialista en redes:
- Experiencia en sistemas operativos Windows NT
- Instalación y configuración de servidores

Funcional SAP R/3:
- Experiencia en los diferentes módulos SAP R/3 configurados en SINCOR

4.1.2 Recursos de personal asignados a cada actividad

La distribución de los recursos se realizó en base al plan general de trabajo para la implantación del plan de recuperación de desastres para el sistema SAP R/3, el cual fue dividido en cuatro fases. A continuación la distribución:

TABLA 4.2 - NOMENCLATURA UTILIZADA PARA RECURSOS UTILIZADOS

ESPECIALIDAD	NOMENCLATURA
Redes	R
Telecomunicaciones	T
Consultor SAP R/3	C
Coordinación del proyecto	G
Procura	P
Funcional SAP R/3	F
Oracle	O

Primera Fase - Planificación:

- Análisis de riesgos en el centro de datos primario. **(R, T, G, O)**

- Definición de la infraestructura requerida para la implantación del sistema redundante (hardware, software y telecomunicaciones) **(R, T, C, G, O)**
- Evaluación de estrategia de replicación para base de datos **(R, T, C, G, O)**
- Medición del volumen de datos a replicar, sobre la base de la cantidad de datos que se actualizan en un periodo de tiempo determinado, esto con la finalidad de evaluar el impacto sobre la plataforma de telecomunicaciones. **(R, T, C, O)**
- Evaluación de la frecuencia de replicación una vez establecido el impacto en la WAN. **(R, T, C)**
- Elaboración de planes de pruebas. **(R, T, C, G, O)**

Segunda Fase - Procura e Instalación de hardware:

- Procura de Hardware. **(P)**
- Instalación, configuración del servidor y del sistema operativo **(R, C)**

Tercera Fase - Implantación de la Solución:

- Instalación y configuración del sistema SAP R/3 en el equipo que va a soportar la aplicación en el periodo de contingencia **(C)**
- Copia del sistema SAP R/3 original al sistema de contingencia. **(C, G)**
- Pruebas locales de la replicación de datos para evaluar el impacto real en la infraestructura de telecomunicaciones. **(R, T, C, O)**
- Definición de usuarios, reportes y transacciones criticas que se mantendrán operativos en caso de activación de la contingencia. Se utilizaran además para certificar la implantación del ambiente tolerante a fallas. **(C, G, F)**
- Generación de manuales y procedimientos. **(C, G, F, O)**

Cuarta Fase - Puesta en Producción:

- Instalación definitiva del servidor en el *centro de datos alternativo* . **(R, T, C)**
- Pruebas y entonación de la replicación de datos vía WAN entre Caracas y Jose en el Estado Anzoategui. **(R, T, C, F, O)**
- Pruebas de reportes y transacciones críticas por parte de los usuarios del sistema en el servidor alterno. **(C, F)**
- Certificación de las pruebas. **(C, F, G, O)**
- Simulación de recuperación en caso de desastre. **(R, T, C, F, G, O)**

4.1.3 Requerimientos de hardware

Debido a los requerimientos propios del Sistema SAP R/3 se requiere de un servidor de alta capacidad de procesamiento, memoria y almacenamiento.

Características requeridas: HP Proliant DL 580, 4 procesadores Pentium Xeon @ 1.2 GHz, 4 GB Memoria RAM, 120 GB de espacio en disco, Fuente de poder redundante, tarjetas de red duales.

4.1.4 Costos de implantación

Los costos de hardware y software son estimados (+/- 5%) basándose en precios referenciales suministrados por Hewlett Packard Venezuela, Oracle, SAP y Microsoft.

La información en relación a costos de horas de consultoría proviene de la empresa escogida para llevar a cabo esta tarea.

TABLA 4.3 - COSTOS DE LA IMPLANTACIÓN

ITEM	COSTOS (USD)
Consultoría SAP R/3	28.000,00
Hardware	40.000,00
Licencias	10.000,00
Costos totales del proyecto	**78.000,00**

4.2 Cronograma de actividades

A continuación se muestra las actividades principales llevadas a cabo para la ejecución del proyecto de implantación de un ambiente tolerante a fallas para el sistema SAP R/3.

TABLA 4.4 - CRONOGRAMA DE ACTIVIDADES

	Mayo ' 03	Junio ' 03	Julio ' 03	Ago ' 03
PROYECTO IMPLANTACIÓN PLAN DE RECUPERACIÓN DE DESASTRE PARA SAP R/3				
Definición de Estrategia a seguir para la Implantación				
Procura de Hardware				
Implantación				
Desarrollo de procedimientos				
Puesta en Producción				
Pruebas y certificación de la implantación				
Cierre del proyecto				

CONCLUSIONES

Debido a la dependencia de las organizaciones en sistemas de tecnología que son vulnerables a diferentes tipos de contingencias tales como sistemas de inteligencia artificial, sistemas de información gerencial, sofisticadas redes de comunicaciones y sistemas computarizados para control de procesos, la planeación ante eventuales contingencias que pueden ser de índole natural, ambiental o intencionales está tomando alta prioridad en la agenda de la gerencia de las organizaciones.

El desarrollo e implantación de un plan de recuperación de un desastre no constituye una garantía de que la empresa u organización continúe en operaciones ante la ocurrencia de una eventual situación de catástrofe, la existencia de un plan no representa garantía que estas situaciones de riesgo no impactarán a la organización. El contar con un plan en caso de desastre, permite reducir el riesgo como consecuencia de haber realizado, como parte del plan, el análisis de cuales son los potenciales riesgos y consecuencias a los cuales la organización está expuesta. Permite eliminar algunos riesgos pero en otros casos solo es posible aminorar sus consecuencias.

Un punto muy importante en cualquier implantación de sistemas tolerantes a fallas está dado por el compromiso que debe tener la alta gerencia para poder llevar a término proyectos de este tipo cuya implantación requiere de considerables recursos financieros y técnicos. Adicionalmente, una vez implantado un sistema tolerante a fallas, la garantía de que éste se mantenga operativo está dado por la realización de monitoreo continuo y la ejecución de pruebas a fin de evaluar constantemente la operatividad de la plataforma instalada y validez de los procedimientos desarrollados.

En SINCOR la implantación de un plan de recuperación de desastres para el sistema SAP R/3 representa una alta garantía de continuar las actividades administrativas de en procesos vitales para el negocio relacionados con Finanzas, Mantenimiento de Planta (PM), Manejo de Materiales (MM), Costos (CO), Ventas (SD), los cuales son ejecutados a través del sistema SAP R/3.

Este proyecto constituyó un reto para la organización ya que hasta el momento no se contaba con experiencia es este tipo de implantaciones especificas para un sistema SAP y la implantación de este plan representó el inicio de un proyecto corporativo cuya finalidad es contar con tolerancia a fallas es toda la plataforma tecnológica instalada en SINCOR.

Con la implantación del plan se obtuvo una infraestructura de sistemas tolerante a fallas que permite lograr alta disponibilidad y acceso continúo a los datos del sistema SAP R/3.

Se realizó el análisis y estimación de posibles riesgos para la plataforma tecnológica actualmente instalada en el centro de datos primario ubicado en las oficinas principales de SINCOR en Caracas.

Se realizó la implantación de estrategias de respaldo para recuperación de desastres, planeación de una metodología avanzada de respaldo para la protección en caso de fallas y para una rápida recuperación de los servidores de bases de datos en caso de desastre, así como la generación de procedimientos que permitan la activación del ambiente replica en caso de falla y posterior restauración, una vez solucionada la falla al centro de datos primario.

BIBLIOGRAFÍA

Gregor Neaga, Bruce Winters y Pat Laufman. (1997). *Prevención y Recuperación de Desastres.* International Technical Support Organization.

Myers, Kenneth N. (1996). *Total Contingency Planning for Disasters: Managing Risk... Minimizing Loss... Ensuring Business Continuity*. (2ª ed). John Wiley & Sons.

Marianne Swanson, Amy Wohl, Lucinda Pope, Tim Grance, Joan Hash, Ray Thomas. (June 2002). *Contingency Planning Guide for Information Technology Systems.* Special Publication 800-34. NIST - National Institute of Standards and Technologies.

Oracle Support Services (1999). Oracle8i Standby Database. [On-line]. Disponible en: http://otn.oracle.com/deploy/availability/pdf/stby8i_twp.pdf

Oracle Support Services (1999). How to Create a Oracle 8i StandBy Database. [On-line]. Disponible en: http://metalink.oracle.com/metalink

SAP AG (2002). Disaster Recovery for Oracle. [On-line]. Disponible en: https://websmp102.sap-ag.de/servicechannel

TechWeb - The Bussiness Technology Group. Time Divition Multiplexing. [On-line]. Disponible en: http://www.techweb.com/encyclopedia/defineterm?term=tdm&x=25&y=11

APÉNDICES

Apéndice A: Equipos de trabajo de recuperación de desastres y papeles clave

La solución de recuperación se implementará a través de una serie de tareas importantes asignadas a varios equipos de trabajo e individuos clave. Cada una de las tareas importantes constará de varias subtareas que pueden asignarse a miembros individuales de cada equipo de trabajo, de acuerdo con el conocimiento o la experiencia.

Las tareas y responsabilidades de estos grupos diferirán con base en la estrategia de recuperación elegida y la estructura organizacional implicada. Además, según el alcance del desastre y la cantidad de trabajo en los procesos de recuperación, algunas personas podrían participar de tiempo completo y otras de tiempo parcial.

En algunos casos tal vez no sea necesario que los equipos de trabajo que se requieren durante el proyecto de preparación sean parte del mantenimiento continuo o la ejecución de la recuperación.

Los equipos de trabajo de recuperación se establecerán de acuerdo con la complejidad de la solución de recuperación y tendrán cuatro responsabilidades principales:

- Escribir las tareas del proyecto del plan de recuperación, de acuerdo con lo requerido.
- Desarrollar e implementar los procedimientos necesarios en el ambiente de producción, para dar apoyo al plan de recuperación
- Ejecutar los pasos de recuperación, como se documentó en el plan de recuperación durante la prueba o el desastre
- Mantener los procedimientos y la documentación de recuperación relacionada con sus áreas.

A continuación se presenta una lista y descripciones de los individuos clave y los equipos de trabajo que podrían asignarse al desarrollo y la ejecución del plan de recuperación de desastres.

7.1.1.1 Líder de proyecto

El papel del líder de proyecto consiste en asumir la responsabilidad general. Esta persona da apoyo al coordinador de recuperación de desastres en el control y coordinación de las tareas; además, facilita la comunicación entre la administración, los equipos de trabajo y los usuarios. Asimismo debe asegurarse de que el proyecto cumpla con el calendario y se satisfaga el propósito de la solución de la recuperación.

7.1.1.2 Coordinador de recuperación de desastres

El coordinador de recuperación de desastres (CRD) por lo general administra la situación del problema y, en algún punto, informa a la alta gerencia que es necesaria la decisión de mudarse. Después de esta decisión, el coordinador de recuperación de desastres dirige a todos los equipos de trabajo que están relacionados con el movimiento de la carga de trabajo del centro de computación al sitio alterno. También asume la responsabilidad de coordinar y controlar todas las tareas, problemas y procedimientos durante la recuperación de desastres.
El CRD necesita tener la capacidad suficiente en procesamiento de datos para realizar estas tareas. Igual de importante es su capacidad para manejar un proyecto complejo y personal bajo presión. Entre sus cualidades deben incluirse:

- Capacidad sobresaliente para la organización
- Conocimiento práctico del trabajo técnico de todas las áreas involucradas
- Excelente habilidad para relaciones interpersonales
- Buena noción de la estructura v las responsabilidades organizacionales
- Entender las necesidades de negocios de la organización

7.1.1.3 Administrador del sitio alterno

El papel de administrador del sitio alterno requiere aclaración. Por lo general se trata del administrador del centro de datos normal de un negocio pequeño, o de los supervisores de operaciones en un negocio grande. Aunque estas personas tal vez tengan una responsabilidad mínima durante la fase de implementación, deben estar familiarizadas con las políticas y los procedimientos de recuperación de desastres. Están a cargo de las instalaciones del centro de datos de recuperación, una vez que se ha terminado ésta.

7.1.1.4 Auditores

Los auditores son importantes en la recuperación de desastres. La prueba de la viabilidad del plan de recuperación recae sobre todo en los hombros de los auditores. En muchas organizaciones existen auditores internos y externos. Puede contratarse a consultores que se especializan en la planeación de la recuperación de desastres, para que desempeñen el papel de auditores externos. Los auditores participan en la implementación y la prueba de la solución de recuperación para asegurarse de que se cumplan las obligaciones establecidas por la dirección de la organización.

El departamento de auditoria interna es responsable de asegurar la integridad y seguridad de los datos restaurados en la instalación alternativa de recuperación y, además, de la integridad del estado financiero de los datos del negocio. Esto supone conocimiento detallado de los procedimientos de conciliación de datos ejecutados en las instalaciones de recuperación, para reintegrar los datos del negocio y las transacciones a su estado actual. Deben considerarse todas las transacciones perdidas como resultado del desastre.

El departamento de auditoria interna debe ser especialmente diligente para desarrollar estas funciones durante la prueba del plan de recuperación de desastres, con el fin de asegurar la recuperación exitosa en el caso de un desastre real.

7.1.1.5 Equipo de trabajo del centro de ayuda

En una situación de desastre es vital distribuir la información correcta en el momento oportuno a quienes corresponda. Esto se explica con más detalle en "Política de información". Este equipo de trabajo debe tener una lista de lo que la gente y las organizaciones, internas y externas, deben conocer y de qué información deben recibir. Al preparar esta lista por anticipado se asegurará que no se ha perdido tiempo en iniciar esta comunicación y que nada se ha pasado por alto. Una vez que se haya notificado a todas las partes, el equipo de trabajo de información puede asumir funciones de centro de ayuda.

7.1.1.6 Equipo de trabajo de hardware e instalación

Se necesita un equipo de trabajo de hardware e instalación cuando su estrategia de recuperación requiera la compra y puesta a punto de hardware adicional. Todos los aspectos de capacidad e instalación deben planearse y prepararse de antemano y deben documentarse claramente los pasos y tareas de este equipo de trabajo.

7.1.1.7 Equipo de trabajo de almacenamiento del sitio externo

Este equipo de trabajo será responsable del traslado de las cintas o documentos del sitio externo al sitio principal, bajo situaciones normales de producción, además de la recuperación de las cintas del sitio externo durante la prueba y en el caso de un desastre real. Todas las tareas del equipo de trabajo de almacenamiento del sitio externo deben estar definidas y descritas en el plan de recuperación de desastres; por ejemplo:

- Instrucciones para llegar al sitio externo
- Acceso a las instalaciones del sitio externo
- Forma de identificar las cintas de respaldo diarias, semanales , mensuales o incrementales
- Empaque y transporte de las cintas al sitio de recuperación

7.1.1.8 Equipo de trabajo de red

En este trabajo puede incluirse la compra, instalación y personalización de los módems o líneas adicionales. Como parte de la planeación de recuperación de desastres también se debe confirmar el número de módems o líneas que deberán estar disponibles para su compra o instalación en caso de desastre.

Dependiendo del diseño de la red y la solución, tal vez sean necesarias actividades como cambio de líneas o personalización de controladores en las ubicaciones remotas. Para estas tareas, son requeridas capacidades de red predefinidas y planes de diseño que incluyan procedimientos con la descripción de

dónde y cómo habrán de realizarse las tareas. Algunos ejemplos de los pasos de recuperación de red son:

- Conmutación de líneas en el sitio alterno
- Mantenimiento de controladores externos de red
- Asignación de puertos
- Producción de esquemas de red para el sitio alterno
- Suministro del mantenimiento y la documentación para estos pasos de recuperación

7.1.1.9 Equipo de trabajo de software

El equipo de trabajo de recuperación de software está asignado a la recuperación de los sistemas y aplicaciones requeridos en el sitio alterno. En un ambiente grande de procesamiento de datos tal vez sea necesario decidir tener equipos de trabajo separados de software para el sistema operativo, la base de datos, la red, etc. En una instalación de procesamiento de datos pequeña, un equipo de trabajo de software puede abarcar todas estas áreas. Hablando de manera general, este equipo de trabajo es responsable de restaurar las plataformas de procesamiento de datos, catálogos y aplicaciones con los últimos respaldos disponibles. Las tareas y responsabilidades de estos equipos de trabajo son demasiado extensas como para tratarse aquí. Sin embargo, aquí hay algunos ejemplos:

- Identificación del software de sistema vital requerido en el sitio alterno
- Preparación de la estrategia del proceso de restauración
- Ejecución de procedimientos de restauración del sistema
- Ejecución de procedimientos de revisión del sistema
- Documentación del software de sistema

7.1.1.10 Equipo de trabajo de operaciones

El equipo de trabajo de operaciones por lo general es el equipo de trabajo que ejecuta los pasos de la recuperación, como se documentó en el plan de recuperación de desastres. Este equipo de trabajo proporciona el personal para manejar las consolas y atiende los requerimientos de impresión y de cintas. Una vez que se ha logrado la recuperación, asume la administración continua del centro de datos en el sitio alterno. Entre algunas de las responsabilidades que debe tener para dar apoyo a la recuperación de desastres se encuentran:

- Establecimiento de la duración y asignación de personal para los turnos durante la recuperación
- Modificación de los procedimientos para la remisión de procesamiento por lotes de acuerdo con lo requerido
- Modificación de los procedimientos de configuración y calendarios de trabajo
- Procedimientos de verificación del sistema
- Enmienda de la estructura del proceso iniciador

7.1.1.11 Equipo de trabajo de soporte a aplicaciones

Este equipo de trabajo debe estar integrado por personal, como los programadores y desarrolladores, responsable de las aplicaciones que dan soporte a los procesos vitales del negocio. Los miembros de este equipo de trabajo pueden ser llamados a desarrollar nuevos programas o procesos para ayudar a la continuidad de la recuperación de los procesos del negocio en el momento del desastre. El equipo de trabajo de soporte a aplicaciones funcionará en estrecha relación con las unidades de negocios durante el desarrollo del plan de recuperación. Entre algunas de las responsabilidades adicionales que debe desarrollar para dar soporte a la recuperación de desastres están:

- Determinación de la estrategia de prueba para las aplicaciones
- Desarrollo de los procedimientos de recuperación de aplicaciones
- Revisión de aplicaciones después de la recuperación

7.1.1.12 Equipo de trabajo de los usuarios del negocio

Los usuarios de negocios son los integrantes de las diversas unidades que utilizan las aplicaciones para desarrollar los procesos de negocios de la organización. Los miembros de este equipo de trabajo son responsables en general de asegurar que se hayan recuperado con éxito los procesos del negocio y que puedan efectuarse todas las funciones críticas dentro de los procesos. Entre sus responsabilidades de recuperación se incluyen:

- Desarrollo de los procedimientos de los procesos del negocio para el sitio alterno
- Documentación de los procedimientos de conciliación de datos
- Desarrollo de los procedimientos para los procesos del negocio
- Identificación de material del negocio requerido fuera del sitio
- Desarrollo de los procedimientos manuales, si se requieren

El número, estructura y tamaño de los equipos de trabajo de recuperación variará con cada organización. Lo importante es recordar que no debe solicitarse que algún miembro del equipo de trabajo efectúe varias funciones de recuperación en un mismo momento; por lo tanto, los miembros de equipos de trabajo deben pertenecer sólo a uno para evitar conflictos.

Apéndice B: Niveles de recuperación de desastres

En el evento SHARE 78, celebrado en Anaheim, 1992, en la sesión M028, la Automated Remote Site Recovery Task Force presentó siete niveles de recuperación. SHARE es una organización integrada por usuarios de procesamiento de datos[14].

Nivel 0: Sin datos fuera del sitio

No proporciona preparación para guardar información, ni para determinar requerimientos ni para establecer una plataforma de hardware de respaldo o desarrollar un plan de contingencia.

Nivel 1: PTAM (Pickup Truck Access Method)

Para estar en el nivel 1, una instalación necesitaría crear un plan de contingencia, respaldar la información requerida y almacenarla en un sitio de contingencia (ubicación fuera del sitio), determinar los requerimientos de recuperación y establecer de manera optativa una plataforma de respaldo que proporcione soporte a instalaciones acondicionadas, sin hardware de procesamiento.

Nivel 2: PTAM + Sitio Hot

Abarca todos los requerimientos del nivel 1 y necesitaría una plataforma de respaldo para tener suficientes recursos de hardware y de red que den soporte a los requerimientos críticos de procesamiento en la instalación. El procesamiento se considera vital si tiene que ser soportado por el hardware existente en el momento del desastre.

Nivel 3: Almacenaje electrónico de seguridad

Abarca todos los requerimientos del nivel 2 y, además, da soporte al almacenaje electrónico de seguridad de algún subconjunto de la información. El hardware que lo recibe debe estar separado físicamente de la plataforma primaria y de los datos almacenados para recuperación de desastres.

Nivel 4: Sitio secundario activo

Incluye los requerimientos de (1) administración activa de los datos de recuperación por un CPU en el sitio de recuperación y (2) recuperación bidireccional. El hardware receptor debe estar separado físicamente de la plataforma principal.

[14] Gregor Neaga, Bruce Winters y Pat Laufman. (1997). *Prevención y Recuperación de Desastres*, págs. 29, 30.

Nivel 5: Escritura de dos fases en dos sitios (Two-Site Two-Phase Commit)

Abarca todos los requerimientos del nivel 4 y además mantendrá los datos seleccionados en un estado de imagen (las actualizaciones se aplicarán tanto a la copia local como a la copia remota de las bases de datos dentro del alcance de una sola operación). El nivel 5 requiere que los datos de las plataformas primaria y secundaria se actualicen antes de que la solicitud de actualización se considere satisfecha. El nivel 5 requiere de hardware parcial o totalmente dedicado en la plataforma primaria, con capacidad para transferir automáticamente la carga de trabajo a la plataforma secundaria.

Nivel 6: Cero pérdida de datos

Abarca la nula o cero pérdida de datos y la transferencia inmediata y automática a la plataforma secundaria. Los datos se consideran perdidos si se ha aceptado la "ENTRADA" (ENTER) (en el terminal), pero no se ha satisfecho la solicitud.

Estos niveles pueden resultar útiles de manera general para la clasificación de las soluciones de recuperación; sin embargo, está limitada su capacidad para describir u ordenar soluciones específicas. Debido a las muchas permutaciones posibles en las diferentes variables de una solución, es imposible describir apropiadamente todas las soluciones potenciales con un pequeño número de niveles. Por ejemplo, una recuperación bidireccional que sólo utilice el transporte manual de cintas puede ser considerada del nivel 1 lo mismo que del nivel 4. Este problema se agudiza con la introducción de nuevos productos.

Apéndice C: Descomposición de los requerimientos (WBS: *Work Breakdown Structure*)

A continuación se muestran la descomposición de los requerimientos la cual fue realizada siguiendo las recomendaciones de la técnica de WBS.

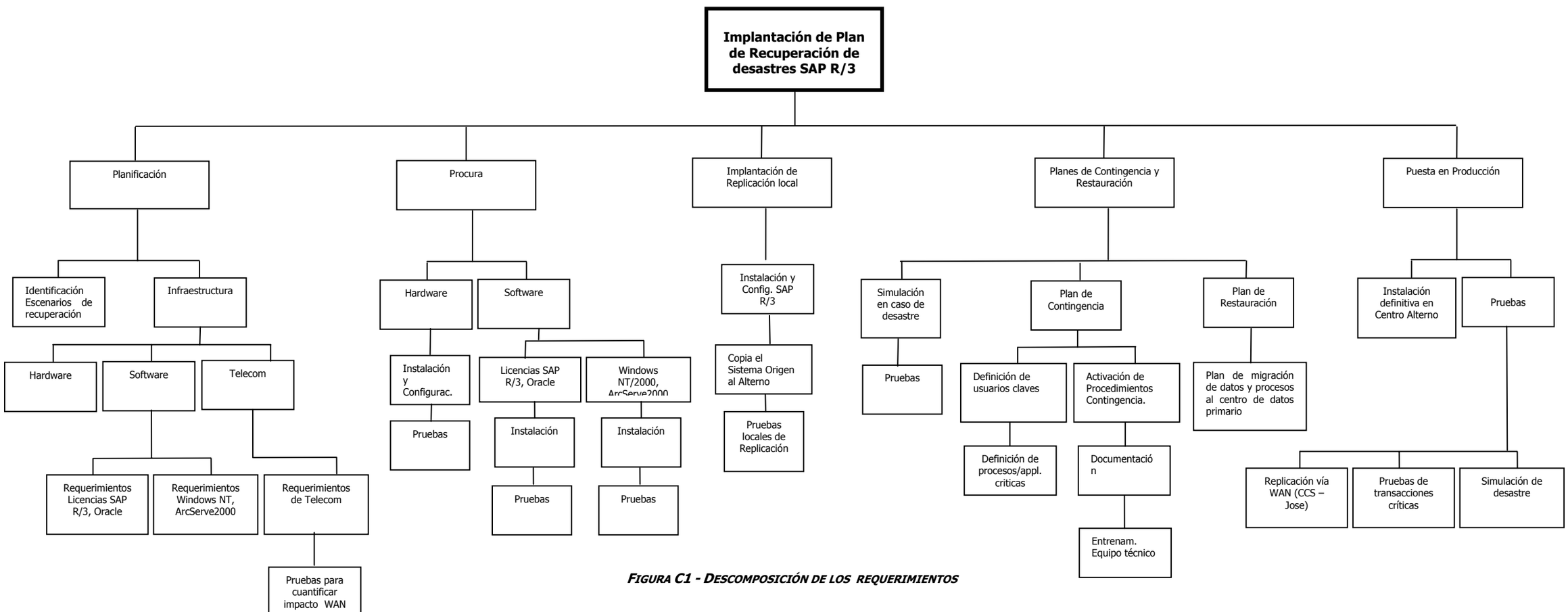

FIGURA C1 - DESCOMPOSICIÓN DE LOS REQUERIMIENTOS

GLOSARIO

Ancho de Banda *(bandwidth)*: Técnicamente es la diferencia en hertzios (Hz) entre la frecuencia mas alta y la mas baja de un canal de transmisión. Sin embargo este término se usa mucho más a menudo para definir la cantidad de datos que puede ser enviada en un periodo de tiempo determinado a través de un circuito de comunicación dado. Rango de frecuencias que deja pasar un circuito. Cuanto más alta es la velocidad de transmisión, mayores son los requerimientos de ancho de banda. Es una acepción común referirse al ancho de banda como el límite superior de la velocidad a la que se transfiere la información por la red. Se mide en hertz o bps (bits por segundo), por ejemplo 32 Kbps, 64 Kbps, 1 Mbps, etcétera.

Archive logs / Offline redo log: Oracle se refiere a los archivos generados en la base de datos en producción como consecuencia de las operaciones transaccionales regulares que involucran modificaciones a dicha base de datos. Estos archivos son utilizados en caso de ser requerido recuperar hasta un punto en el tiempo la base de datos.

Backup (Respaldo). Proceso de crear una copia de datos de computadora en un medio de almacenamiento externo como: disco suave, cinta o disco rígido externo.

Base de datos StandBy (*StandBy database*): La solución de base de datos StandBy surge en las nuevas versiones de la Base de Datos Oracle, desde la versión Oracle 7 y de manera más avanzada en versiones 8 y 8i. Esta solución consiste en la creación de una base de datos paralela a partir de una copia física (incluyendo datafiles, online redo logs y Archive Redo Logs) de una base de datos original. Posteriormente en la Base de Datos paralela se lleva una imagen actualizada de la base de datos original mediante la aplicación de los Archive Redo Logs de la base de datos original en la base de datos paralela ó StandBy.

Centro de Datos Alterno: Se refiere a un segundo sitio propiedad de la empresa que puede utilizarse como instalación de recuperación, si se destruye el sitio primario de la compañía y proporciona la capacidad de continuar o reanudar el procesamiento de la carga de trabajo crítica en caso de una interrupción de servicio primario.

Centro de datos primario: Se refiere al sitio principal propiedad de la empresa en donde se encuentra centralizada todas las operaciones, datos equipos, comunicaciones, etc.

Channel bank: Es un multiplexor que mezcla diversas líneas de voz o data de baja velocidad en una línea digital de alta velocidad. Channel banks usa TDM para combinar las diferentes señales en un sola para entrelazar los bits.

DBWR (Database Writer Process): Proceso de Oracle encargado de escribir todas las modificaciones realizadas a la base de datos y que se encuentran en memoria a los datafile correspondientes.

Desastre (*Disaster*): Evento que suspende la disponibilidad de los servicios de procesamiento de datos por un periodo lo bastante prolongado como para que las instalaciones de procesamiento de datos tengan que ser trasladadas a otro sitio.

Disponibilidad (*Availability*): Medida (a menudo especificada como porcentaje) de cuántos servicios de procesamiento de datos están disponibles para los usuarios en un periodo especificado.

FTP: Protocolo de Transferencia de Archivos. Protocolo de aplicación, parte de la pila de protocolos TCP/IP, que se utilizan para la transferencia de archivos entre los nodos de la red.

Gateway: Dispositivo de comunicación entre dos o más redes locales (LAN) y remotas, usualmente capaz de convertir distintos protocolos, actuando de traductor para permitir la comunicación. Como término genérico es utilizado para denominar a todo instrumento capaz de convertir o transformar datos que circulan entre dos medios o tecnologías.

Host: Sistema anfitrión, Sistema principal. Albergar, Hospedar. Computadora que, mediante la utilización de protocolos TCP/IP, permite a los usuarios comunicarse con otros sistemas anfitriones de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet, www y FTP.

LAN: *Local Area Network o* Red de Área Local. Conjunto de computadoras y otros dispositivos comunicados entre sí dentro de una área pequeña.

Línea dedicada *(Leased line).* Forma de conexión a Internet (con acceso las 24 horas) a través de un cable, hasta un proveedor de Internet. Esta conexión puede ser utilizada por varias personas en forma simultánea.

Log switch: Es el evento durante el cual LGWR detiene la escritura a uno de los Online Redo Logs e inicia la escritura el otro. Un log switch ocurre automáticamente cuando el actual archivo online Redo Log está lleno.

Modo Mount: Es uno de los estados en los cuales puede encontrarse una base de datos al momento de iniciar operaciones, en este modo aun no está accesible la data para los usuarios, es un estado de mantenimiento o es el modo de operación en el cual debe permanecer la base de datos StandBy en este modo la StandBy siempre está en espera de ser actualizada a partir de los Archive Redo Logs generados en producción.

Modo Open: Oracle se refiere al estado en el cual se encuentra la base de datos la cual está operativa y accesible para transacciones de usuario.

Modo recovery (*Recovery mode*): Oracle se refiere al estado en el cual se encuentra la base de datos StandBy, la cual está recibiendo los Archive logs generados en la base de datos en producción. La base de datos StandBy está em modo recovery cuando se están aplicando los Archive logs.

MTTR (Mean *Time To Repair, Mean Time To Restore*): Es el tiempo promedio que toma en solventar una falla o reparar un componente.

Nivel de acuerdo de servicio (*SLA - Service Level Agreement*): Es un contrato entre el proveedor y los usuarios, el cual especifica el nivel de servicio que se espera durante el término del dicho contrato. Los SLAs son usados por proveedores y clientes así como internamente entre IT y sus usuarios finales. Este puede especificar condiciones en términos de disponibilidad de ancho de banda, tiempos de respuesta para rutinas, resolución de problemas (redes, falla de equipos, etc.), así como actitudes y consideraciones del staff técnico.

Plan de Recuperación de Desastres (*Disaster Recovery Plan*): Es un procedimiento que garantiza la recuperación, total o parcial, del sistema en operación (Productivo), en caso de presentarse eventos que pueden ser calificados de desastre y que podrían de alguna manera comprometer la data transaccional de la empresa. Entre estos eventos podemos identificar desde Incendios ó Terremotos, que de alguna manera pueden poner riesgo la infraestructura tecnológica instalada.

Procesamiento de datos (*Data Processing*): Todo lo que se relaciona con las computadoras y su ambiente de soporte, como hardware, software, datos, redes, operadores, programadores, etcétera. Es una versión más global o moderna del concepto original del procesamiento de datos.

Proceso del negocio (*Business process*): Grupo de actividades interrelacionadas que dan soporte a a operación exitosa del negocio o de sus servicios.

Red de Telecomunicaciones: Estructura física de telecomunicaciones con accesos distribuidos. Puede ser punto a punto, por conmutación de paquetes o de circuitos, y tener capacidad (o no) de interconectividad con otras redes.

Registro (Log): Se refiere a un registro de comandos o transacciones. Es requerido para asegurar la capacidad de retomar dichos comandos y transacciones.

Replicación de datos (*Data Replication*): Consiste en realizar un duplicado o copia exacta de data para propositos de backup y tolerancia a desastre.

Respaldo en frío (*Cold Backup / Offline Backup*): Es el tipo de respaldo para bases de datos en el cual ésta se encuentra completamente cerrada, inaccesible

para transacciones, y en condiciones de ser respaldados todos los archivos pertenecientes a la base de datos. Es el tipo de respaldo más confiable y expedito en caso de ser requerido alguna recuperación.

Shutdown: Proceso mediante el cual la base de datos se cierra y no permite nuevas conexiones luego de ejecutado el comando shutdown, las sesiones existentes son desconectadas.

Shutdown immediate: Comando de emergencia para bajar inmediatamente la base de datos sin esperar a que los usuarios actuales cierren sus sesiones.

Shutdown normal: No permite nuevas conexiones a la base de datos y una vez ejecutado el comando se espera a los usuarios conectados cierren sus sesiones en la base de datos. El siguiente *startup* no requiere procedimientos de recuperación.

Servidor*(Server):* Computadora que ejecuta uno o más programas simultáneamente, con el fin de distribuir información a las computadoras que se conecten con él para dicho fin. Computadora que suministra espacio de disco, impresoras u otros servicios, a máquinas conectadas con ella a través de una red.

Servidor Firewall. Es un componente de seguridad entre dos redes, el cual vigila la entrada y salida de flujos de información de Internet.

Sistema Operativo de Red. Es quien rige y administra los recursos (archivos, periféricos y usuarios, entre otros) y lleva el control de seguridad de éstos.

TCP: *Transmission Control Protocol o* Protocolo- de Control de Transmisión. Conjunto de protocolos de comunicación, que se encargan de la seguridad y la integridad de los paquetes de datos que viajan por Internet. Complemento del IP en el TCP/IP.

TCP/IP: *Transmission Control Protocol / Internet Protocol* o Protocolo de Control de Transmisión / Protocolo de Internet. TCP corresponde a la capa de transporte del modelo de referencia OSI y ofrece la transmisión de datos. IP corresponde a la capa de red y ofrece servicios de datagramas sin conexión. Su principal función es comunicar sistemas diferentes.

Tolerancia a desastre (*Disaster Tolerante)*: Capacidad de una organización para sobrevivir, en cuanto a tecnología de información se refiere, a un desastre mayor, tales como inundación, terremoto, incendio, conflictos armados

T1: Una línea T1 es circuito digital dedicado, punto apunto, a una velocidad de 1.544Mbps y que es provisto por empresas de telefonía. Las líneas T1 son ampliamente usadas para redes privadas así como interconexiones entre PBXs de organizaciones o LANs y las empresas de telecomunicaciones (telco). Una línea T1 usa dos pares cableados (uno para transmission y el otro para recepción) así como

multiplexación por división de tiempo (TDM) para entrelazar canales de 2464 Kbps para voz o data.

WAN. *Wide Area Network o* Red de Área Amplia. Conjunto de computadoras y otros dispositivos comunicados entre sí, colocados dentro de un espacio geográfico de amplias dimensiones.

WBS (*Work Breakdown Structure*): Es la estructura degradada de trabajo, es la fase principal en el proceso de planificación de un proyecto. Corresponde a la descomposición de proyecto en todas las tareas a realizar.