# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERIA

**PLAN DE RECUPERACION DE DESASTRES DEL SISTEMA SAP CONSIDERANDO FALLA EN EL SERVIDOR APLICATIVO DE UN LABORATORIO FARMACEUTICO**

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERO ELECTRICO ELECTRONICO

P R E S E N T A:

**GENARO MENDEZ JIMENEZ**

DIRECTOR DE TESIS:

**M. EN C. EDGAR BALDEMAR AGUADO CRUZ**

Ciudad Universitaria, D.F. 2012

# Dedicatorias

A mis padres que han estado conmigo en todo momento. A ti mamá que me enseñaste a ser un hombre honesto y responsable, por todos los valores que me inculcaste, por tu interés y dedicación en mi educación personal y profesional

A ti papa que con tu ejemplo me enseñaste que el único camino para conseguir los objetivos es con esfuerzo y perseverancia, que con tu apoyo nunca me he sentido solo, espero llegar a ser un padre de familia como tú.

Gracias por haberme dado esta vida, son mi ejemplo y orgullo.

*Lo que soy es gracias a ustedes.*

A mis hermanas, cuñados y sobrino por brindarme su apoyo en todo momento, gracias familia.

A mi esposa por estar a mi lado, por comprenderme y apoyarme incondicionalmente, eres mi complemento y haces que surja lo mejor de mí. Podría dedicarte mil palabras pero con dos basta: Te amo.

A mis hijas Naomi y Emily son el motivo de mis logros, las amo son mi vida.

*Lo que seré es por ustedes…*

A la universidad por haberme dado mi formación profesional, es un orgullo ser Puma.

*"Basta un poco de espíritu aventurero para estar siempre satisfechos,*

*pues en esta vida, gracias a dios, nada sucede como deseábamos,*

*como suponíamos, ni como teníamos previsto."*

# INDICE

**CAPITULO III**



**CAPITULO IV**

# CAPITULO I

# INTRODUCCION

En toda operación o proceso está latente la posibilidad de un evento no programado a causa de un desastre o una contingencia mayor, las cuales pueden representar la no disponibilidad o pérdidas potenciales de información. Actualmente un gran porcentaje de la información vital para toda organización se encuentra en dentro de un sistemas ERP, almacenadas en dispositivos electrónicos y en la mayoría de los casos es consultada por sitios remotos.

En cualquier sistema de información es necesario estar protegido de las múltiples amenazas, garantizando la preservación de los siguientes aspectos:

1. Integridad. Que se proteja la exactitud y totalidad de los datos y los métodos de procesamiento
2. Confidencialidad. Que la información sea accesible solo a las personas autorizadas.
3. Disponibilidad. Que los usuarios autorizados tengan acceso a la información y a los recursos cuando los necesiten.

Normas oficiales como las representadas en el Sarbanes Oxley Act, o las emitidas por la Comisión Nacional Bancaria y de Valores de México (CNBV) o la Ley Orgánica de Protección de Datos de España (LOPD), entre otras, también obligan a las instituciones de diversos ramos a contar con planes de recuperación funcionales.

Razón por la cual es una prioridad para el área de TI y para el negocio, desarrollar, establecer, probar y mejorar un plan de recuperación de desastres que asegure la continuidad de la operación y de los sistemas de información. Este plan debe de establecer un escenario en donde se pueda proveer una alternativa de operación para el caso en cuestión en un tiempo razonable y predefinido.

Los riegos pueden ser eliminados, mitigados o previstos, dependiendo de los factores de probabilidad de ocurrencia, los objetivos del plan de recuperación de desastres son la planificación y descripción de cómo actuar de manera rápida y ordenada, con responsables predefinidos para cada tarea involucrada, escrito en un procedimiento que indique de manera clara como ejecutar los controles y procedimientos establecidos.

La solución de recuperación de desastres requerida por una empresa dependen de los objetivos específicos definidos por su negocio que deben ser estipulados dentro de su Plan de Continuidad de Negocio; dos métricas de vital importancia para este diseño son:

- El punto de recuperación de la información (RPO = Recovery Point Objective)
- Tiempo en el que se debe recuperar la operación (RTO= Recovery Time Objective).

Un estudio realizado por Symantec, informa:

Las Pequeñas y Medianas Empresas (PyME) no se encuentran preparadas para responder ante un desastre tanto en América Latina, como en el mundo, de acuerdo con una encuesta realizada por Symantec. Las PyME no cuentan con un plan de prevención y recuperación de desastres, lo que ocasionaría que cuando se presente un incidente no exista una estrategia para evitar que cause estragos en su operación y sus finanzas, reveló la Encuesta 2011 sobre Preparación ante Desastres en las PyME. Symantec destacó que 46% de las PyME de América Latina no considera una prioridad de su negocio diseñar un plan para prevenir desastres. Mientras que el promedio global se situó en 40%. Al resguardar su información, las PyME latinoamericanas tampoco se encontraron bien ubicadas. En la encuesta 46% confesó que perdería 40% de su información en caso de que se presentara un desastre. Symantec señala que esta cifra es el reflejo de los resultados arrojados al preguntar a las PyME sobre la realización de copias de seguridad. Únicamente 23% de las compañías realizan un respaldo diario, mientras que menos de 50% lo hace de manera regular, ambos resultados son presentados de manera global. Ahogado el niño tapan el pozo Symantec hace énfasis en el momento después del desastre, ya que, según la encuesta, es cuando más de la mitad de las PyME se preocupa por instalar un plan para asegurar la información de su negocio. Los resultados evidenciaron que, a nivel mundial, un desastre puede generar que las PyME tengan pérdidas de hasta $12,500 dólares por día. En América Latina la inactividad podría provocar que los clientes de una PyME pierdan hasta $3,000 dólares al día. Esa cifra puede generar desde el abandono de los clientes hasta el cierre de la empresa, según el estudio. La encuesta prevé que 36% de las PyME a nivel global considerará este año desarrollar un plan de preparación ante desastres. Para realizar el estudio Symantec analizó las respuestas de 1,840 encuestados a nivel global. Por parte de América Latina participaron Argentina, Brasil, Chile, Colombia, Costa Rica y México.

Nuestro escenario fue establecido para un Laboratorios Dermatológico Mexicano, el cual su columna de negocio es la producción y venta de productos dermatológicos.

A principios del 2009, fue implementado SAP con la finalidad de eficientar procesos administrativos, tras un análisis se determinó que el site donde se hospedaría el sistema ERP, fuera en la planta de producción situada en Cuernavaca Morelos. La compañía contaba con dos oficinas más, un CEDIS ubicado en el Estado de México y las oficinas centrales ubicadas en el Sur del DF.

SAP se convirtió en el sistema de mayor importancia para la compañía, razón por la cual se comenzó a gestionar y diseñar un Plan de recuperación de Desastres para el sistema SAP viable y sobre todo con una baja inversión económica.

Fueron analizadas las herramientas de Symantec BackupExec para Windows Server y BackupExec System Recovery, mediante las cuales soportamos la recuperación del desastre.

Una solución basada en disco, como Symantec BackupExec System Recovery, supera los procesos de recuperación de sistemas manuales mediante la captura de una copia exacta de un sistema, que incluye el sistema operativo, las aplicaciones, la configuración del sistema, los parámetros y los datos, en un único punto de recuperación.

Siempre ha sido un proceso predominantemente manual, arduo y prolongado una recuperación, que implica la reparación del hardware, la reinstalación del sistema operativo, aplicaciones, parches y actualizaciones del sistema, con varios reinicios durante el proceso. Luego, se debe de configurar nuevamente el sistema tal como estaba antes de la falla. En total, el proceso puede demorar días o incluso semanas.

Esto es insostenible en los entornos de uso crítico actuales. Hoy en día, todos los sistemas, desde servidores a equipos de escritorio y equipos portátiles, deben poder recuperarse rápidamente, ya sea en herramientas de hardware similares o distintas. La imposibilidad de volver de en un corto tiempo a un estado productivo puede tener como resultado una importante pérdida de ingresos, pérdida de la productividad, y un daño considerable en la reputación de la empresa.

El plan se desarrolló bajo el siguiente esquema:

- Se consideró un escenario en el cual se presentara una falla total en la infraestructura de SAP (servidores y almacenamiento SAN)
- El plan fue encaminado a recuperar la operación de la empresa mediante un hardware heterogéneo alterno ubicado en las oficinas administrativas mediante herramientas de recuperación basada en imágenes.

Dentro de la solución no solo está la elaboración de documentación y las pruebas del Plan de Recuperación de Desastres (DRP) sino también el entrenamiento al personal que lo efectuará , su actualización y mantenimiento y evidencia documental de las pruebas.

“El DRP no es solo un requisito”

# CAPITULO II

# MARCO TEÓRICO

## 2.1 Redes

¿Qué es una red? Una red es un sistema de interconexión entre computadores que permiten compartir recursos e información.

A principios de la década de 1970 se llevó a cabo un evento que ha tenido la mayor influencia en la evolución de redes de computadoras. Como resultado de los avances tecnológicos en el campo de los componentes para computadora, aparecieron los circuitos integrados de gran escala (LSI). Estos dispositivos estaban caracterizados por costo relativamente bajo, así como por funciones avanzadas. Lo anterior llevo al desarrollo de las microcomputadoras.

A partir de este momento, aun pequeñas compañías pudieron darse el lujo de tener sus propias computadoras, las cuales podían llevar a cabo tareas como el control de equipo técnico y la administración de las existencias en dicha compañía. Esto represento el origen del concepto de computo distribuido, en el que los recursos de computo estaban distribuidos por toda la compañía, sin embargo, todas las computadoras es la misma organización continuaron trabajando de forma independiente.

A medida de que transcurrió el tiempo, las necesidades de los usuarios evolucionaron, ya no podían trabajar independiente, necesitaban intercambio de información. Con el fin de satisfacer estas necesidades aparecieron las primeras LAN

### 2.1.1 Interacción entre computadoras

Las aplicaciones que corren en una computadora A no pueden acceder directamente a los recursos de la computadora B, como discos, archivos o impresoras. Para acceder a estos recursos debe de existir un aplicación que llame a otros programas que corran en la computadora cuyos recursos se necesiten utilizar. Dichas solicitudes están implantadas en forma de mensajes transmitidos a través de algún medio de comunicación. En las LAN dichas funciones son llevadas a cabo por las tarjetas de interface de red (NIC, por sus siglas en ingles), a menudo llamadas adaptadores de red, y por sus controladores

En un sentido amplio, la interface representa una lógica o física definida formalmente entre los objetos por comunicarse, los cuales son independientes entre sí. La interface define parámetros, procedimientos y características de interacción entre objetos.

La interface física se define como un conjunto de conexiones eléctricas y características de las señales

La interface lógica es un conjunto de mensajes de información con un formato predefinido que utilizan los dispositivos o programas para intercambiar datos entre si, además de un conjunto de reglas que determinan la lógica del intercambio.

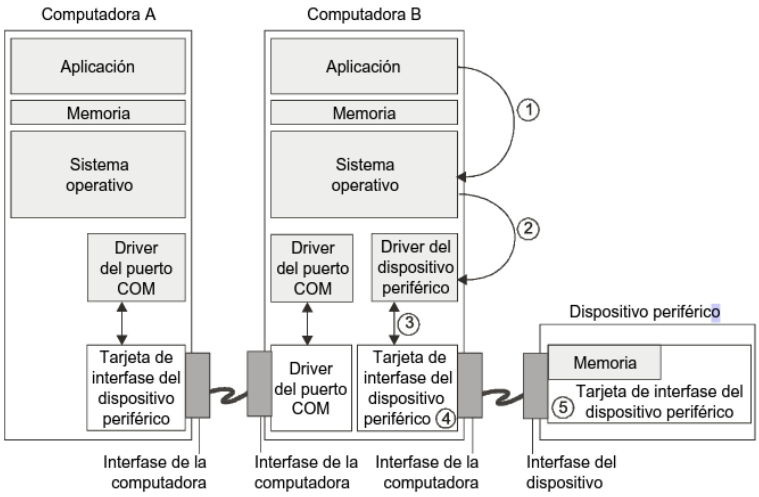


Fig 2.1.1 Lógica de intercambio

Estas reglas son determinadas por software conocido como clientes servidores en donde:

El cliente es el modulo diseñada para integrar mensajes de solicitud a una maquina remota desde diferentes aplicaciones, recibir y transferirlos a las aplicaciones correspondientes.

El servidor es el modulo que debe escuchar, de forma permanente, las solicitudes de los clientes que provienen de la red y que estén dirigidas hacia dispositivos específicos conectados a esa computadora. Una vez que el servidor recibe la solicitud del cliente, este trata de procesarla y realizarla, a veces con ayuda del sistema operativo. Un servidor puede atender las solicitudes de varios clientes de manera secuencial o en paralelo.

Existen también programas de usuarios distribuidos: aplicaciones. Una aplicación distribuida incluye varios componentes, cada uno de los cuales lleva a cabo ciertas operaciones con el fin de realizar determinadas tareas por el usuario. Por ejemplo, una parte de dicha aplicación que corre en la estación de trabajo del usuario final puede soportar una interface grafica de usuario (GUI). Otro modulo puede correr en una computadora dedicada de gran capacidad y llevar a cabo el procesamiento de los datos proporcionados por el usuario; la tercera parte podría cargar los resultados en la base de datos que reside en una computadora donde está instalado

el sistema estándar de administración de base de datos (DBMS). Las aplicaciones distribuidas emplean totalmente el potencial del procesamiento distribuido que proporcionan las redes de datos. Por tanto a menudo se llaman aplicaciones de red

### 2.1.2 Características de los enlaces físicos.

Existen múltiples características importantes relacionadas con la transmisión del tráfico que se utiliza en los enlaces físicos

La carga física que es el lujo de datos desde el usuario hasta la entrada de la red. La carga ofrecida puede caracterizarse por la velocidad de los datos de entrada a la red, midiéndose en Kbps, Mbps, etc.

La velocidad (tasa) de información o rendimiento, es la velocidad real del flujo de datos a través de la red. Puede ser menor que la carga ofrecida ya que la red, como cualquier otro sistema real, puede comportarse de una forma no deseable por el usuario.

La capacidad se define como la velocidad máxima posible de transmisión de datos utilizando un tipo de enlace especifico. La parte específica de esta característica consiste en que su valor depende de las características físicas del medio y del método seleccionado para transmitir la información discreta utilizando este medio. El transmisor de determinado dispositivo de comunicación debe trabajar a una velocidad igual a la capacidad de enlace, la cual a menudo se conoce como tasa de transferencia.

Ancho de banda, puede tener dos significados, el primero puede utilizarse para designar una característica física del medio de transmisión físico. En este caso el término se refiere al ancho de banda de frecuencias a la que una línea de comunicación transmite sin experimentar distorsiones significativas. Y también el término es utilizado como sinónimo de capacidad. En el primer caso el ancho de banda se mide en Hertz (Hz), mientras que el segundo se mide en bits por segundo (Kbps)

El siguiente grupo de características de un enlace de comunicación está relacionado con la posibilidad de trasmitir información por medio de este enlace en una o ambas direcciones. El intercambio de información es generalmente bidireccional. Existen dos flujos de datos: el flujo principal, que es de interés práctico al usuario, y el flujo auxiliar, que se transmite en la dirección opuesta. Este flujo auxiliar de datos está formado por los reconocimientos de recepción del flujo de datos principal.

Los enlaces físicos se clasifican en base en su capacidad para transmitir información en ambas direcciones.

En enlace dúplex asegura la transmisión simultánea de información en ambas direcciones.

Los enlaces half-duplex también aseguran la transmisión de información en ambas direcciones, solo que no simultanea sino por turnos.

El enlace simplex permite la transmisión de información en una sola dirección. Con frecuencia los enlaces dúplex están formados por dos simplex

### 2.1.3 Topologías de enlaces físicos

La topología de red se refiere a la configuración de una gráfica cuyos vértices corresponden a los nodos de una red y al equipo de comunicaciones, cuyos extremos representan las conexiones físicas de información entre ellos. Existe una gran variedad de posibles configuraciones, es posible distinguir entre topologías total y parcialmente conectadas

Una topología totalmente conectada corresponde a una red en la que cada computadora se encuentra conectada directamente a las demás. A pesar de su simplicidad esta topología es muy ineficaz, pues para conectar N nodos es necesario contar con N(n-1)/2 enlaces de conexión dúplex, es decir el número de enlaces está relacionado con el número de nodos mediante una función cuadrada.

Los demás tipos de red se basan en topologías parcialmente conectadas, en las que se lleva a cabo el intercambio de datos entre dos computadoras.

La topología de malla, se obtiene a partir de la topología totalmente conectada al suprimir algunos de sus enlaces.

En la redes con topología en anillo, los datos se transmiten alrededor del anillo de computadora a computadora. La principal ventaja del anillo consiste en proporcionar enlaces redundantes. Por otra parte en este tipo redes es necesario tomar medidas especiales para asegurar que cuando una computadora falle, no falle el circuito de comunicación de los demás nodos de la red.

La topología de estrella supone que cada computadora esté conectada directamente a un dispositivo central llamado concentrador. Las funciones del concentrador incluyen el re direccionamiento de la información. A veces tiene sentido construir la red utilizando varios concentradores conectados entre si en forma jerárquica mediante enlaces tipo estrella, resultando una topología conocida como jerárquica o de árbol.

### 2.1.4 Redes de Área Local (LAN)

Ethernet es en la actualidad el estándar más conocido de LAN. El término Ethernet por lo regular se refiere a una variante de la tecnología, las variantes son Fast Ethernet, Gigabit Ethernet y 10G Ethernet.

En un sentido restringido, Ethernet es un estándar de red para la transmisión de datos a una velocidad de 10Mbps que apareció a finales de la década de los 70's como estándar propietario de tres compañas: Digital Equipment Corp, Intel y Xerox. A principios de los 80's, Ethernet fue estandarizado por el grupo IEEE 802.3 y desde entonces se ha convertido en un estándar internacional. Ethernet fue la primera tecnología que sugirió usar un medio de transmisión compartido para tener acceso a la red.

Como son una red de conmutación de paquetes, las LAN emplean el principio de multiplexage por división de tiempo, lo cual significa que comparten el medio de transmisión en el tiempo. El algoritmo para compartir el tiempo, el control de acceso al medio de transmisión (MAC), es una de las características más importantes de cualquier tecnología LAN, debido a que tienen una influencia mucho mayor en el tipo de tecnología que le medio de codificación de las señales o el formato de la trama. Ethernet utiliza un método de acceso aleatorio como mecanismo para compartir el medio de transmisión, aunque su desventaja es que a medida de que la carga de la red aumenta el ancho de banda efectivo disminuye.

La amplia aceptación de la red Ethernet a 10Mbps sirvió como incentivo eficaz pasa si desarrollo, el estándar Fast Ethernet fue adoptado en 1195, el Gigabit Ethernet apareció en 19988 y el 10G Ethernet en 2000.

Como regla general las topologías LAN implementan solo las funciones de las dos capas inferiores del modelo OSI, eso se debe a que la funcionalidad de estas dos capas es suficiente para la entrega de tramas dentro e la estructura de las topologías LAN estándares.

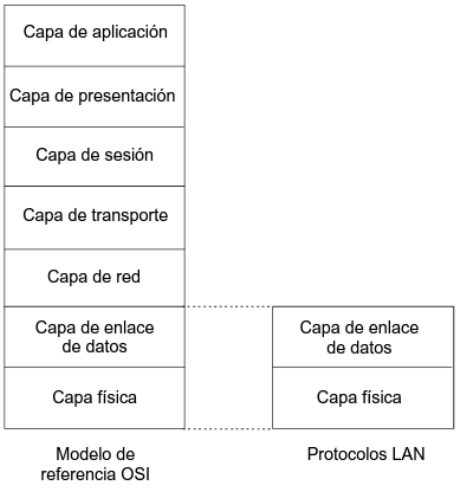


Fig 2.1.4 Modelo OSI

Aunque cada computadora conectada a una LAN debe de soportar la pila de protocolos en su totalidad, como IP o IPX.

La capa de enlace de datos de la LAN se divide en dos subcapas:

- Control de enlace lógico (LLC). Las principales funciones son, garantizar el acceso al medio de transmisión compartido y trasmitir tramas dentro los nodos terminales mediante la funcionalidad de los dispositivos de la capa física.

Las funciones LLC suelen implementarse mediante un módulo de software apropiado al sistema operativo y las funciones MAC están implementadas en hardware (adaptador de red) y en software (controlador de adaptador de red)

- Control de acceso al medio (MAC). Lleva a cabo las funciones de administrar la interfaz hacia la capa de red, la cual se encuentra adyacente a esta y garantizar la entrega de tramas confiable con el nivel de confiabilidad predefinido. También incluye la trasmisión de datos del usuario y de control entre la capa Mac y capa de red. Cuando se transmiten datos de arriba hacia abajo, la capa LLC recibe el paquete (IP o IPX) que contienen los datos del usuario. Además del paquete, transmite la dirección del paquete dentro de la LAN. En términos de pila de protocolo TCP/IP, este tipo de direcciones se conoce como direcciones de hardware. La capa LLC transmite los datos recibidos de la capa de red hacia la capa MAC para su procesamiento. Además la capa LLC también lleva a cabo el multiplexaje, pues los datos recibidos de varios protocolos de la capa de red se transmiten hacia un solo protocolo de capa MAC.

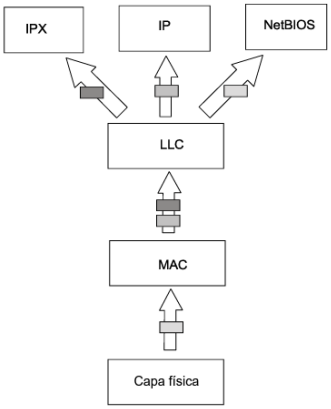


Fig. 2.1.4.1 Transmisión en la capa de red

### 2.1.5 Medios de transmisión

Históricamente las primeras Ethernet se crearon con cable coaxial, más adelante se definieron otras especificaciones.

El número 10 en los nombres de la especificación significa la velocidad de transmisión de los datos de acuerdo con el estándar. La componente base de refiere al método de codificación (banda base) cuando se usa una sola frecuencia base de 10 MHz (en contraste con los métodos que utilizan varias frecuencias de portadora, los cuales se llaman banda ancha). El último carácter en el estándar significa el tipo de cable.

| Parámetro | 10Base-5 | 10Base-2 | 10Base-T | 10Base-F |
|---|---|---|---|---|
| Cable | Cable coaxial grueso RG-8 o RG-11 | Cable coaxial delgado RG-58 | UTP categoría 3, 4 o 5 | Cable de fibra óptica multimodo |
| Longitud máxima del segmento (m) | 500 | 185 | 100 | 2 000 |
| Máxima distancia entre nodos de la red (cuando se utilizan repetidores) (m) | 2 500 | 925 | 500 | 2 500 (2 740 para 10Base-FB) |
| Número máximo de estaciones de trabajo en un segmento | 100 | 30 | 1 024 | 1 024 |
| Número máximo de repetidores entre dos estaciones de trabajo | 4 | 4 | 4 | 4 (5 para 10Base-BF) |

Fig 2.1.5 Especificaciones

El Ethernet clásico empezó a ser insuficiente en su ancho de banda. La tase de intercambio de 10Mbps fue significativamente más pequeña que las tasas del bus interno de las computadoras, las cuales por esa época (1990) aseguraban la transmisión de datos a 133 Mb/s, resultando en un funcionamiento más lento de la red no solo para los servidores, sino también para las estaciones de trabajo, que comenzaban a utilizar el bus PCI.

Todas las diferencias entre las tecnologías Fast Ethernet y Ethernet clásico están concentradas en la capa física. La estructura más compleja de la capa física se debe al usar de tres variantes de sistema de cableado.

- Cable multimodal de fibra óptica, de dos fibras.
- Par trenzado categoría 5, dos pares
- Par trenzado categoría 3, cuatro pares.

| Estándar | Tipo de cable | Longitud máxima de segmento |
|---|---|---|
| 100Base-TX | UTP categoría 5 | 100 m |
| 100Base-FX | Fibra óptica multimodal 62.5/125 µm | 412 m (half-dúplex) hasta 2 km (full-dúplex) |
| 100Base-T4 | UTP categorías 3, 4 o 5 | 100 m |

Fig. 2.1.5.1 Especificaciones por tipo de cable

| Tipo de cable | Diámetro máximo de la red (m) | Longitud máxima del segmento (m) |
|---|---|---|
| Solamente par trenzado (TX) | 200 | 100 |
| Solamente par trenzado (FX) | 272 | 136 |
| Varios segmentos basados en par trenzado y un segmento basado en fibra óptica | 260 | 100 (TX) 160 (FX) |
| Varios segmentos basados en par trenzado y varios segmentos basados en fibra óptica | 272 | 100 (TX) 136 (FX) |

Fig 2.1.5.2 Longitud de transmisión

Fast Ethernet, al igual que todas las variantes de Ethernet, está destinado para utilizar concentradores y repetidores con el fin de crear los enlaces de red.

Las reglas para construir de manera correcta los segmentos de Fast Ethernet son:

- Limitación sobre longitud máxima de los segmentos que conectan un equipo de datos (DTE) a un DTE.
- Limitaciones sobre la longitud máxima de segmentos que conectan CTE a un puerto del repetidor
- Limitaciones sobre el diámetro máximo de la red
- Limitaciones sobre el número máximo de repetidores y la longitud máxima de segmento que conecta los repetidores

No mucho después de que apareciera Fast Ethernet en el mercado, se detectaron ciertas limitaciones, por lo que en el verano de 1996 IEEE creó un grupo de trabajo 802.3z: el cual fue dirigido a crear un protocola tan próximo a Ethernet como fuera posible, pero suministrando una velocidad de 1 000 Mbps.

- Las características que preserva en común Giga Ethernet con sus predecesoras son:
- Se preservan todo los formatos de trama Ethernet
- A versión Half dúplex del protocolo que soporta CSMA/CD todavía está presente
- Se soportan todos los tipos principales de cables.

El estándar de esta tecnología es 802.3z, la cual define los siguientes tipos de medio físico.

- Cable de fibra óptica en modo simple
- Cable de fibra óptica multimodal 65.2/125
- Cable de fibra óptica multimodal 50/125
- Cable de cobre balanceado con protección (blindaje)

Los estándares son:

- 1000Base-SX
- 1000Base-CX
- Par trenzado.

## 2.2 Sistema Operativo Windows Server 2003.

El sistema operativo es un conjunto de programas que administra los recursos de una computadora y permite que el usuario los utilice.

Dependiendo de la forma y el nivel de empleo de los recursos, el usuario puede trabajar directamente con el sistema operativo para comunicarse con la computadora, o puede recurrir al software de aplicación para ello.

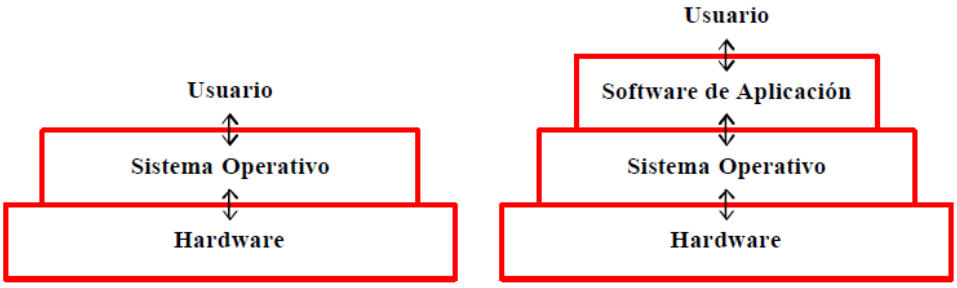


Fig. 2.2. Capas de operación

Para aplicaciones más complejas pueden existir modelos computacionales con varios niveles adicionales de software (modelos de “n” capas)

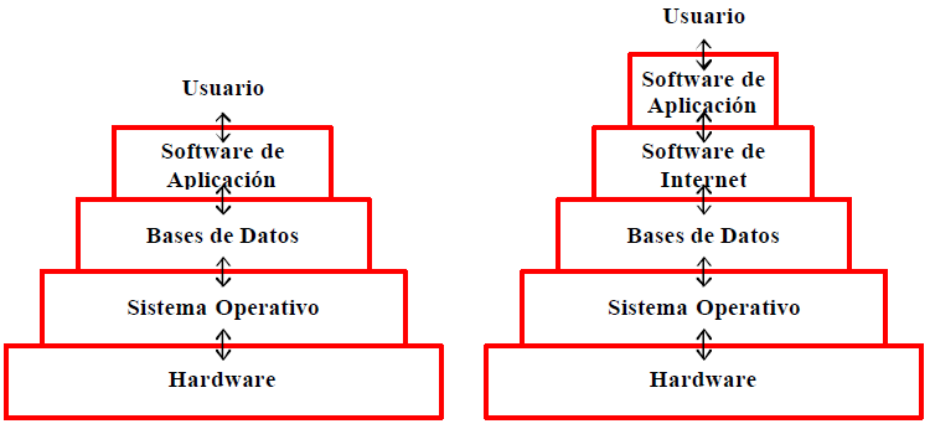


Fig. 2.2.1 Capas por software

La razón de la presencia de esas capas intermedias de software, entre el usuario y los equipos de computo, está en dos factores: por un lado las computadoras entienden y manejan un lenguaje binario (constituido por ceros y unos), que resulta incomprensible para el usuario común, razón por la que los desarrolladores de software crean programas que traducen las ordenes de los usuarios a ese lenguaje binario; por otro lado las aplicaciones son cada vez más complejas y se requiere de software especializado a distintos niveles.

El sistema operativo Windows es el de mayor difusión entre las computadores personales y servidores medianos y pequeños. Fue desarrollado por Microsoft, aunque muchas de sus ideas básicas provinieron del sistema operativo Mac OS, de los equipos Macintosh.

Las primeras versiones del Sistema Operativo de Microsoft recibieron la denominación de DOS (Disk Operating system – Sistema Operativo de Disco), software que trabaja en ambiente de texto, es decir que las instrucciones o comandos debían de ser escritas desde teclado.

La primera versión gráfica exitosa del Sistema Operativo de Microsoft fue Windows 3.1 para equipos stand alone (aislados), que en realidad era un ambiente gráfico que trabajaba sobre DOS (era una interfaz gráfica para DOS). Recibió el nombre de Windows pues la información se presentaba dentro de espacios rectangulares de la pantalla, con bordes a modo de ventanas.

Posteriormente apareció una versión mejorada, Windows 3.11 que permitía trabajar en un esquema básico de red, conocido como Windows para Trabajo de Grupo.

El primer S.O. gráfico de Microsoft pata estaciones de trabajo (clientes dentro de una red) fue Windows 95, además fue el primer sistema operativo de 32 bits para clientes tipo PC.

Posteriormente aparecieron Windows 98, Windows 2000, Windows XP y Windows 2003

La familia de Windows Server ofrece una base sólida para toda la carga de trabajo de un servidor y requisitos de aplicación al tiempo que es fácil de implementar y administrar.

Algunas de las funciones del servidor son:

- Servidor de archivos e impresión.
- Servidor Web y aplicaciones Web.
- Servidor de correo.
- Terminal Server.
- Servidor de acceso remoto/red privada virtual (VPN).
- Servicio de directorio, Sistema de dominio (DNS), y servidor DHCP.
- Servidor de infraestructura para aplicaciones de negocios en línea (tales como planificación de recursos de una empresa y software de administración de relaciones con el cliente).

Windows Server 2003 aparece en cuatro ediciones diferentes, que se ajustan a las necesidades impuestas por ciertos roles funcionales dentro de las infraestructuras de TI:

*1. Windows Server 2003, Edición Estándar*

Con soporte de hasta 4 procesadores y las funciones normales del producto, incluyendo servidor Web y Servidor de Terminales.

*2. Windows Server 2003, Edición Enterprise*

Escala hasta sistemas de 8 vías, con 32 GB de RAM y posibilita la configuración de plataformas de servidores de alta capacidad y disponibilidad mediante soluciones de tipo clúster con hasta 4 nodos. Esta edición tiene soporte para procesador de 64 bits

*3. Windows Server 2003, Edición Datacenter*

Orientada a entornos de alta demanda y misión crítica, en arquitectura centralizada, permitiendo configuraciones de multiprocesamiento simétrico de hasta 32 vías y 64 GB de RAM, clúster de hasta 8 nodos, balanceo de carga y soporte para arquitecturas de procesador de 64 bits con hasta 128 GB de RAM.

*4. Windows Server 2003, Edición Web*

Optimizado específicamente para las funciones de servidor Web y aplicaciones basadas en Web (Web Services, .NET Framework)

### 2.2.1 Ventajas del sistema operativo Windows Server

Las ventajas que presenta Windows server 2003 son:

Disponibilidad. Mediante arquitecturas en cluster, que son la base fundamental de las infraestructuras informáticas en entornos de misión crítica en muchas organizaciones, donde se aplican a comercio electrónico, aplicaciones de línea de negocio o servicios corporativos centralizados de alta disponibilidad.

Escalabilidad. Windows Server 2003 ofrece escalabilidad vertical, con soporte a sistemas de multiprocesamiento simétrico (SMP), y horizontal ("Scale-out") por medio de clusters. La gama de servidores Windows Server 2003 puede funcionar desde sistemas monoprocesador hasta multiprocesadores de 32 vías, y sistemas de 64 bits.

Fiabilidad. La escala que adquieren las redes extensas y locales hoy día, dan como resultado un mundo interconectado donde la seguridad es la preocupación principal de los usuarios y administradores. La gama de productos Windows Server System, y en particular Windows

Server 2003 han sido objeto de una revisión completa para reforzar su seguridad en todas las fases del ciclo de vida del producto, desde su mismo diseño hasta su mantenimiento.

Los negocios han hecho crecer la tradicional red de área local (LAN) al combinar redes internas, externas y sitios de Internet.

Windows Server 2003 en materia de productividad se extienden a numerosas áreas, entre ellas:

Servicios de impresión y archivos. Las nuevas mejoras introducidas se orientan a facilitar la administración y seguridad de los recursos de archivo compartido, a dar soporte a nuevas tecnologías de almacenamiento e impresión y a una mayor escalabilidad y rendimiento de las soluciones de recursos compartidos, reduciéndose así el TCO.

Active Directory. Windows Server 2003 incorpora muchas mejoras para Active Directory, haciéndolo más versátil, fiable y económico de usar, con una mayor escalabilidad y rendimiento. Añade además mejoras que permiten una mayor flexibilidad a la hora de diseñar, implantar y administrar el servicio de directorio corporativo, especialmente en grandes organizaciones.

Servicios de Administración. La proliferación de nuevas plataformas y dispositivos móviles ha provocado un aumento de la complejidad y coste de la administración de las redes corporativas. La clave para una reducción efectiva de los costes de mantenimiento está en la automatización de procesos, y para ello, Windows Server 2003 incluye diversas herramientas de administración automatizada, como Microsoft Software Update Services (SUS) y asistentes de configuración de servidor para ayudar a automatizar las instalaciones. La administración de Políticas de Grupo se hace más fácil con la nueva Consola para Administración de Políticas de Grupo (GPMC), y las nuevas herramientas de línea de comandos permiten que los administradores realicen la mayoría de las tareas desde la consola de comandos y con muy pocas operaciones.

Administración de almacenamiento. Windows Server 2003 introduce novedades y mejoras en las herramientas de administración del almacenamiento, haciendo que sea más fácil y más seguro manejar y dar mantenimiento a discos y volúmenes, respaldar y recuperar datos, y conectarse a una red de almacenamiento (SAN).

Terminal Services. Con este servicio, desde un servidor Windows Server 2003 se pueden ejecutar aplicaciones en modo de terminal remoto Windows, prácticamente desde cualquier dispositivo, incluso en sistemas que no son Windows.

## 2.3 SAP

SAP fue fundada en 1972 en la Ciudad de Mannheim, Alemania, por antiguos empleados de IBM (Claus Wellenreuther, Hans-Werner Hector, Klaus Tschira, Dietmar Hopp y Hasso Plattner)

bajo el nombre de "SAP System analyse, Anwendungenund Programmentwicklung". El nombre fue tomado de la división en la que trabajaban en IBM.

La corporación SAP fue fundada en 1972 y se ha desarrollado hasta convertirse en la quinta más grande compañía mundial de software. El nombre SAP R/3 es al mismo tiempo el nombre de una empresa y el de un sistema informático. Este sistema comprende muchos módulos completamente integrados, que abarca prácticamente todos los aspectos de la administración empresarial.

Ha sido desarrollado para cumplir con las necesidades crecientes de las organizaciones mundiales y su importancia está más allá de toda duda. SAP ha puesto su mirada en el negocio como un todo, así ofrece un sistema único que soporta prácticamente todas las áreas en una escala global. SAP proporciona la oportunidad de sustituir un gran número de sistemas independientes, que se han desarrollado e instalado en organizaciones ya establecidas, con un solo sistema modular.

Cada módulo realiza una función diferente, pero está diseñado para trabajar con otros módulos. Está totalmente integrado ofreciendo real compatibilidad a lo largo de las funciones de una empresa.

Después de haber dominado el mercado, la empresa afronta una mayor competencia de Microsoft e IBM. En marzo de 2004 cambió su enfoque de negocio en favor de crear la "plataforma" que desarrolla y utiliza, la nueva versión de su software NetWeaver

Es en este punto donde SAP se encuentra enfrentado con Microsoft e IBM, en lo que se conoce como "la guerra de las plataformas". Microsoft ha desarrollado una plataforma basada en la Web llamada .NET, mientras IBM ha desarrollado otra llamada WebSphere.

A comienzos de 2004 sostuvo conversaciones con Microsoft sobre una posible fusión. Las empresas dijeron que las conversaciones finalizaron sin un acuerdo. Sin embargo, a comienzos del 2006 fue anunciada una alianza muy importante entre SAP y Microsoft para integrar las aplicaciones ERP de SAP con las de Office de Microsoft bajo el nombre de proyecto "Duet".

La compra de SAP por parte de Microsoft habría sido uno de los acuerdos más grandes en la historia de la industria del software, dado el valor de mercado de la alemana, de más de 55.000 millones de euros (junio 2004).

SAP ha conquistado clientes de forma consistente para aumentar la cuota del mercado global entre sus cuatro principales competidores a un 55% a fines de 2004, desde un 48% dos años antes. La participación combinada de Oracle y People Soft declinó de un 29% a un 23%.

SAP es una compañía alemana, pero opera en todo el mundo, con 28 sucursales y afiliadas y 6 compañías asociadas, manteniendo oficinas en 40 países.

### 2.3.1 Productos de SAP

SAP trabaja en el sector de software de planificación de recursos empresariales (o ERP por las siglas en inglés de Enterprise Resource Planning). El principal producto de la compañía es R/3, en el que la R significa procesamiento en tiempo real y el número 3 se refiere a las tres capas de la arquitectura de proceso: bases de datos, servidor de aplicaciones y cliente. El predecesor de R/3 fúe R/2.

Otros productos de SAP son APO (Advanced Planner and Optimizer), BW (Business Information Warehouse), BI (Business Intelligence), Customer Relationship Management (CRM), SRM (Supplier Relationship Management), Human Resource Management Systems (EHRMS), Product Lifecycle Management (PLM), KW (Knowledge Warehouse) RE (Real Estate), FI/CO (Financial Accounting/Controlling).

SAP también ofrece una nueva plataforma tecnológica denominada SAP NetWeaver. Esta plataforma tecnológica convierte a SAP en un programa Web-enabled, lo que significa que estaría totalmente preparado para trabajar con él mediante la web, se puede trabajar con SAP mediante cualquier navegador de internet si se tienen los componentes apropiados de SAP NetWeaver (SAP Portals).

Aunque sus principales aplicaciones están destinadas a grandes empresas, SAP también se dirige a la pequeña y mediana empresa con productos como SAP Business One y my SAP All-in-one.

SAP cuenta también con verticales y micro verticales. Las verticales son conocidas también como IS o Industry Solution y son SAP orientados a diversas industrias, como por ejemplo periódicos, mineras, compañías de telecomunicaciones. Los micros verticales son SAP que atienden a industrias específicas, como por ejemplo: empresas agroexportadoras, piscifactorías, etc. Las Verticales son desarrolladas por SAP y los micros verticales por los socios de SAP.

## 2.4 Herramientas de recuperación

La nueva estrategia es tomar fotos de los discos tanto en servidores como estaciones y poder recuperar la máquina a un estado anterior en cuestión de minutos.

Esta funcionalidad la provee el BackupExec System Recovery Server, recuperación rápida de datos y del sistema.

El Symantec BackupExec System Recovery Server es una herramienta poderosa que provee un método rápido y no invasivo de realizar sus respaldos.

Es posible lograr restauraciones completas y rápidamente llevar el sistema a un punto específico en el tiempo sin que esto tome horas de reconstrucción manual, reinstalación de productos y restauración lenta de los datos desde cinta.

BackupExec System Recovery Server es una solución de Backup basada en disco diseñada para capturar y encapsular TODO el estado del servidor, configuración, datos, programas en un solo archivo de fácil administración. Se pueden realizar respaldos totales o parciales (incrementales).

El BackupExec System Recovery permite guardar las imágenes de respaldo a cualquier dispositivo incluyendo SAN, NAS, CD/DVD, Direct attached Storage entre otros. Elimina la necesidad de reconfigurar sistemas operativos, aplicaciones, parches, configuraciones y estado de la máquina, ya que preserva todo tal y como estaba antes de la falla.

## 2.5 Redes de Almacenamiento.

¿Cuáles son las redes de almacenamiento disponibles hoy en día? Existen muchas tecnologías que podemos encontrar hoy en día, las cuatro principales son:

- DAS (Direct Attach storage)
- FC SAN (Fibre Channel Attached Network)
- i-SCSI (Internet Small Computer system Interface)
- NAS (Network Attached Storage)

### 2.5.1 DAS (Conexión Directa de Almacenamiento)

Es una de las tecnologías más antiguas en almacenamientos directos. Han existido numerosos cambios en los ambientes DAS para lograr incrementar la conectividad, velocidad y el total de discos. Las DAS en algunas ocasiones son llamadas JBOD (Just a Bunch of Disk). Su arquitectura está compuesta por un servidor con un controlador SCSI/RAID, un cable SCSI y la unidad DAS. Dependiendo de la configuración de la unidad DAS el número máximo de servidores que puede ser conectados son dos.

Existen dos tipos de discos que se usan: SCSI Ultra 320 y SAS (Serial Attached SCSI). El Ultra 320 hace referencia al Fast 160, le dobla la velocidad de transferencia de datos a 320 Mbps

El SAS es otro nuevo estándar aprobado por American National Standars Institude (ANSI) el cual presume de lograr mayores distancias de transmisión en un punto a punto usando topologías de conexiones dedicadas. El costo operativo de SAS en más bajo que SCSI.

El almacenamiento de datos se ha convertido en uno de los más populares recursos para las corporaciones.

- Tradicionalmente los servidores forman “fondo” del negocio.
- Las redes de almacenamiento son construidas “delante” de los servidores permitiendo a los clientes el acceso local a las unidades de almacenamiento.
- La administración fue descentralizada

La tasa de transferencia SAS comienzo en 1Gbps o 150 Mbps, actualmente soporta 3 Gbps o 300 Mbps La siguiente generación de SAS promete 6 Gbps de capacidad de procesamiento. SAS ofrece el doble de velocidad de un SATA (serial advanced technology attachment).

DAS tiene limitantes para expandir su capacidad de almacenamiento. Porqué SCSI y SAS tienen limitaciones con el número de discos que pueden ser agregados a un mismo canal, esta tecnología no es escalable para necesidades de grandes almacenamientos. Adicionar dispositivos requiere un apagado del sistema. El máximo número de dispositivos que pueden ser agregados a un canal son 16 (mínimo para la controladora SCSI/SAS y otro probablemente para el controlador de backplane.

### 2.5.2 NAS (Red Adjunta de Almacenamiento)

Network attached storage es un servidor o disco duro de almacenamiento que viene montado sobre nuestro Sistema Operativo (Windows o Linux), configurado con la habilidad de aceptar conexiones de red mediante sistemas de archivos como CIFS (Common Internet File System) usado para conexiones Windows, NFS (Network Files System) usado por UNIX/LINUX.

La NAS es unido a la LAN y se le asigna una dirección IP. Las peticiones de archivos son mapeados por el servidor principal al servidor de archivos NAS.

La NAS consiste de un disco duro de almacenamiento, incluyendo una SAN o un arreglo múltiple de discos (RAID) y un software para configurar y mapear la ruta de los archivos al dispositivo adjuntado a la red. El software de la NAS usualmente soporta numerosos protocolos, como TCP/IP, Net BEUI, IPX/SPX y SUN.

**iSCSI** Conocido como Internet SCSI es una tecnología en desarrollo que está ganando terreno en el mercado de almacenamiento. iSCSI comenzó a usarse para implementar infraestructura de almacenamiento de bajo costo utilizando un dispositivo de almacenamiento ISCSI, un switch de red y servidores con manejadores iSCSI. Estas redes son normalmente implementadas en una red separada, pero pueden ser utilizadas redes LAN o WAN existentes.

iSCSI pueden ser fácilmente direccionada para mercados bajos y altos, utilizando redes Fast o Gigabit ethernet u otra red mediana para trasmitir datos entre dispositivos SCSI. Esta tecnología puede ser usada en SAN, NAS.

iSCSI trabajara sobre una LAN o WAN usando el estándar TCP/IP para acceder a los dispositivos iSCSI. Los datos pueden ser distribuidos sobre diferentes redes, para garantizar la seguridad pueden utilizarse servidores, routers, VLANs o Firewalls, dependiendo de la configuración utilizada.

### 2.5.3 SAN (Red de Área de Almacenamiento)

Storage Área Network en una red de alta velocidad para propósitos especiales que interconectan diferentes tipos de dispositivos de almacenamiento con servidores de datos en grandes redes de usuarios. Generalmente la SAN es usada para recursos en red de grandes empresas o aplicaciones críticas.

NAS provee una manera de administrar los sistemas de almacenamiento de datos en una empresa. Uno de los puntos clave pata un departamento de IT es la escalabilidad, NAS la proporciona, ya que pueden ser agregados servidores y unidades de almacenamiento si necesidad de tener tiempos fuera de línea. Otro punto importante en la actualidad es la disponibilidad de los datos, para atender esta necesidad, los dispositivos SAN implementan RAID y pueden ser usados como almacenamiento compartido en fallas. En adición SAN puede ser diseñado para ofrecer redundancia en rutas entre dispositivos.

- En un ambiente SAN, es posible que los servidores corran diferentes sistemas operativos y unirse al mismo dispositivo de almacenamiento.
- Los dispositivos de cintas comunes pueden ser accesadas sin agregar carga en la red principal. Es decir el mismo servidor puede acceder a la unidad de cinta unida a la SAN sin necesidad de generar carga en la red corporativa.
- La administración centralizada se convierte en una posibilidad

Una SAN consiste de:

- Un dispositivo de almacenamiento
- Conexión o infraestructura física
- Computadoras con un HBA (host bus adapter) o dispositivo iniciador.

Las características de los dispositivos de almacenamiento son:

- Procesador de almacenamiento: dos módulos destinados al procesamiento y memoria de lectura.

- Discos duros: discos duros Fiber Channel (Hot-pluggable) forman el sistema de almacenamiento
- Auto reconstrucción dentro de un grupo de RAID: Auto reconstrucción en el momento que se presenta la falla.
- Auto failback dentro de un grupo de RAID: Permite una vez reconstruido regresar al disco original donde se presentó la falla una vez que es reemplazado.

Los dispositivos iniciadores

Los FC HBA proveen conectividad a la SAN de los host, generalmente es una tarjeta PCI o que puede estar integrada al Server. Proveen un punto de entrada dentro de la infraestructura de la SAN para el host Server. Una HBA provee el direccionamiento físico de los paquetes FC, checando errores en la comunicación y secuencia, también maneja el control de flujo y concurrencia de los eventos de I/O. La HBA reside en las capas bajas del protocolo FC

La infraestructura SAN

Tradicionalmente cuando hablamos acerca de SAN, entendemos que la SAN usa el protocolo de Fibra Canal (FC). Con los avances de las nuevas tecnologías, otros protocolos están madurando, como el iSCSI (SCSI sobre IP). La SAN generalmente esta compuesta de dos componentes:

- El protocolo: iSCSI o FC
- El medio físico: Cables, Conectores, Switches.

El protocolo iSCSI es un protocolo de comunicación de almacenamiento sobre redes IP, basadas en SAN. El bloque de nivel de datos iSCSI es encapsulado en un TCP/IP frame. Los dos principales beneficios son:

- Grades distancias
- Bajos costos. No requiere de switches especiales

Para implementar iSCSI es necesario tener un iniciador, el cual puede ser implementado en cualquier hardware. Microsoft implementa un iniciador iSCSI en el sistema operativo Windows. Pueden ser implementados dispositivos especiales iSCSI.

El protocolo de Fibra Canal (FC) proporciona las siguientes características:

- Incorpora una interface canalizada
- Separa la operaciones de I/O de la interface física de I/O
- Permite para el transporte otros protocolos como iSCSI

El termino Fibra, no indica que el protocolo solo usa fibra óptica como medio. Indica que usa dos diferentes fibras en la comunicación, una para enviar datos (transmitir) o otra para recibir datos. FC puede utilizar tanto cobre y fibra óptica como medio de transporte. Además proporciona:

- Alta velocidad de transferencia (Up to 10 Gbps)
- Compatibilidad con otros protocolos
- Puede transportar por grandes distancias
- Soporta arquitecturas punto a punto, Loop arbitrario o topologías con switch de fibra.
- La trasferencia de datos es asíncrona

## 2.6 Respaldos de Información

El riesgo de la pérdida de información. Los datos recibidos, procesados, trasmitidos y archivados por una empresa son vitales para el funcionamiento del negocio. Contienen los correos, proyectos, datos de clientes, de proveedores y otras informaciones que no se debe correr el riesgo de perder.

Procedimiento para crear la estrategia del back-up

- Diseñar la estrategia de respaldo.
- Probar que la estrategia diseñada sea práctica, replanteándola si es necesario o mejorándola sobre la marcha.
- Establecer la rotación del medio de almacenamiento.
- Guardar copias de los medios de almacenamiento, con no más de una semana de antigüedad, fuera de la oficina donde está el sistema.
- Establecer la elaboración de un backup semanal para crear la seguridad y conveniencia necesaria en los sistemas pequeños. Los servidores y las estaciones de trabajo requieren una aproximación diferente.
- Establecer el empleo diario en corto tiempo de demora para el back-up incremental con los datos modificados, ya que la mayoría de los datos se vuelven obsoletos rápidamente.

La información de la empresa se almacena en discos rígidos, CD y otros medios, que al igual que los equipos y el trabajo de las personas, están constantemente sometidos a siniestros que es necesario prever y solucionar con el back-up.

Las causas de estos siniestros son:

- Fallas en el Medio. Ocurren cuando hay daños en los componentes electrónicos y mecánicos, como la caída de un disco rígido a más de un metro de altura con la consecuente pérdida parcial o total de datos.
- Operación incorrecta. Ocurre cuando de forma intencional o no, se operan incorrectamente las aplicaciones eliminando archivos de información, como el borrar una partición o hacer un formateo accidental.
- Ataques externos. Ocurre cuando los equipos adquieren virus o ingresan al sistema usuarios con malas intenciones y producen pérdidas considerables de información.
- Incompatibilidades de Hardware. Ocurre cuando el hardware asociado al medio de almacenamiento no es apropiado y produce pérdidas de información, como el caso del hardware incompatible con el control de los discos rígidos.
- Bugs. Ocurre cuando bugs en drivers, relacionados al medio del almacenamiento o subsistema asociado, generan problemas de lectura o escritura de datos con pérdidas de información. También cuando los bugs en las aplicaciones generan repentinamente comportamientos inesperados que afectan a los datos presentes en el medio.
- Desaparición del Medio. Ocurre cuando se pierde el medio de almacenamiento que contiene los datos, por robo o accidentes.

Las posibilidades para realizar un backup son muchas, si bien unas más adecuadas que otras según se considere el caso:

- Se puede realizar una simple copia con el viejo, conocido y querido COPY/CP de DOS/UNIX.
- Se puede grabar un CD.
- Se puede grabar una cinta.
- Se puede copiar la información a un disco removible/PC espejo del original.
- Se puede subir la información a la web a hostings que cuenten con backups.

Aunque parezca obvio, todas estas posibilidades SIEMPRE deben contemplar que la copia se realizó correctamente y como requisito extra esta verificación debe realizarse cada cierto tiempo prudencial.

En lo que respecta a empresas las acciones a realizar son un poco más complejas pero el concepto es el mismo: hacer backup es ahorrar tiempo y dinero.

En este caso será necesario realizar un análisis costo/beneficio para determinar qué información será almacenada, los espacios de almacenamiento destinados a tal fin, la forma de realización, las estaciones de trabajo que cubrirá el backup, etc.

Para una correcta realización y seguridad de backups se deberán tener en cuenta estos puntos:

- Se debe contar con un procedimiento de respaldo de los sistemas operativos y de la información de los usuarios, para poder reinstalar fácilmente en caso de sufrir un accidente.
- Se debe determinar el medio y las herramientas correctas para realizar las copias, basándose en análisis de espacios, tiempos de lectura/escritura, tipo de backup a realizar, etc.
- El almacenamiento de los Backups debe realizarse en locales diferentes de donde reside la información primaria. De este modo se evita la pérdida si el desastre alcanza todo el edificio o local.
- Se debe verificar, periódicamente, la integridad de los respaldos que se están almacenando. No hay que esperar hasta el momento en que se necesitan para darse cuenta de que están incompletos, dañados, mal almacenado, etc.
- Se debe contar con un procedimiento para garantizar la integridad física de los respaldos, en previsión de robo o destrucción.
- Se debe contar con una política para garantizar la privacidad de la información que se respalda en medios de almacenamiento secundarios. Por ejemplo, la información se puede encriptar antes de respaldarse.
- Se debe contar con un procedimiento para borrar físicamente la información de los medios de almacenamiento, antes de desecharlos.
- Mantener equipos de hardware, de características similares a los utilizados para el proceso normal, en condiciones para comenzar a procesar en caso de desastres físicos.

Puede optarse por:

Modalidad Externa: otra organización tiene los equipos similares que brindan la seguridad de poder procesar la información, al ocurrir una contingencia, mientras se busca una solución definitiva al siniestro producido.

Modalidad Interna: se tiene más de un local, en donde uno es espejo del otro en cuanto a equipamiento, características técnicas y capacidades físicas. Ambos son susceptibles de ser usados como equipos de emergencia.

En todos los casos se debe asegurar reproducir toda la información necesaria para la posterior recuperación sin pasos secundarios ni operación que dificulte o imposibilite la recuperación.

### 2.6.1 Tipos de Respaldos de información

Los principales métodos de respaldos son:

| Tipo | Descripción |
|---|---|
| Copia | Copia todos los archivos seleccionados, pero no marca cada archivo como respaldado, en otras palabras, el archivo de atributo no es borrado). Este tipo de respaldo es Utuado se quiere realizar un respaldo sobre demanda, sin interferir con las estrategias de respaldo calendarizadas. |
| Diario | Copia todos los archivos seleccionados que hayan sido modificados en el día que respaldo hay sido ejecutado. Los archivos respaldados no so marcados como si hubieran sido respaldados (el archivo de atributo no es borrado) |
| Diferencial | Copia los archivos que hayan sido modificados o creados desde el último respaldo normal o incremental. La presencia del archivo de atributo indica que el archivo fue modificado y solo los archivos con este atributo son respaldados. No marca los archivos que fueron respaldados (no borra el archive de atributo), por lo cual si se realizan dos diferentes respaldos consecutivos de un archivo, el archivo es respaldado en los dos respaldos.<br><br>Este tipo de respaldo utiliza más medios que un incremental, pero cuando se restaura a disco solo es necesario el medio que contenga el último respaldo normal y el más reciente respaldo diferencial. Con lo cual el tiempo de restauración en menor. |
| Incremental | Diseñado para crear respaldos de archivos modificados desde el ultimo respaldo normal o incremental. La presencia del archivo de atributo indica que el archivo fue modificado, y solo los archivos con este atributo son respaldados. Cuando el archivo es respaldado el atributo es borrado.<br><br>Como el respaldo incremental borra el archivo de atributo, si se realizan dos respaldos consecutivos, el archivo no es respaldado en el segundo trabajo. Este respaldo usa un mínimo de medios y de tiempo de ejecución, pero el inconveniente al realizar una restauración se debe de contar con el último respaldo normal y todos los incrementales hasta donde se desee restaurar. |
| Normal o Full | Copia todos los archivos seleccionados, marcándolos como respaldados (borra el archivo de atributo).Con estos respaldos solo se necesita la más reciente copia del medio para restaurar todos los archivos. Generalmente se utiliza la primera vez que se crea una estrategia de respaldos. |

Tabla 2.6.1 Tipos de respaldos

Si se quiere un método más rápido de respaldo que requiera el mínimo de espacio de almacenamiento, se debería de respaldar usando una combinación de respaldo normal e incremental.

Pero la recuperación puede consumir un tiempo mayor y dificultades, porque los respaldos pueden estar en muchos discos o cintas

Si se requiere un método más fácil de restauración, se debería usar una combinación de respaldos normales y diferenciales.

Este tipo de combinación ocupa menor espacio de almacenamiento, pero el tiempo empleado para el respaldo es mayor.

## 2.7 Análisis del riesgo en la administración de proyectos de tecnología de información

Se establece que la administración del riesgo del proyecto es el arte y la ciencia de identificar, analizar, y responder a los riesgos a lo largo de la vida de un proyecto, con el propósito de lograr los objetivos del proyecto.

La administración de riesgo del proyecto puede tener un impacto positivo en la selección de proyectos, en la determinación del alcance de los proyectos, y desarrollar estimados más reales de costos y plazos.

Una buena administración del riesgo de proyectos a menudo pasa desapercibida. Cuando la administración de riesgos es efectiva, los resultados se reflejan en el menor número de problemas. En algunas ocasiones es difícil determinar si la administración de riesgos o la buena suerte fue la responsable de un adecuado desarrollo de un proyecto de tecnología de información. Pero los integrantes de un proyecto saben que sus proyectos trabajaron mejor debido a la buena administración de riesgos.

### 2.7.1 Bases Teóricas

Definiremos algunos términos claves que serán utilizados en la presente propuesta.

- Un riesgo es un evento, el cual es incierto y tiene un impacto negativo.
- Análisis de riesgo es el proceso cuantitativo o cualitativo que permite evaluar los riesgos. Esto involucra una estimación de incertidumbre del riesgo y su impacto.
- Administración de riesgo es la práctica de usar el análisis de riesgo paradiseñar estrategias que permitan reducir o mitigar los riesgos.

En la administración de los proyectos de tecnología de información los gerentes de proyectos se plantean preguntas tales como:

- ¿Cuánto tiempo tomará el proyecto?
- ¿Cuál será el costo total del proyecto?
- ¿La ejecución del proyecto permitirá obtener los productos o entregables de acuerdo a las especificaciones requeridas?

Antes que un proyecto comience y mientras se está desarrollando ninguna de las preguntas anteriores puede ser respondida con certidumbre, y los gerentes de proyectos y los clientes están preocupados con la incertidumbre de las respuestas y el impactos de las posibles desviaciones. Las herramientas del análisis de riesgo y administración de riesgo están diseñadas para responder estas preguntas.

La primera técnica cuantitativa de la administración moderna de proyecto en el área del análisis de riesgos relacionado con los tiempos o plazos del proyecto fue el diagrama de Gantt, desarrollada por Henry Gantt en 1917. El diagrama de Gantt proporciona un resumen gráfico del progreso de un listado de actividades que son mostradas verticalmente, representando el inicio y la duración de cada actividad por una línea horizontal a lo largo de una escala de tiempo. De esta manera se muestra cuándo cada tarea debe empezar y el estatus actual de su ejecución. Sin embargo, el diagrama de Gantt tiene una limitación para administrar proyectos complejos por que no muestra la interrelación entre las actividades.

Ante esta limitación, y en la búsqueda de nuevas herramientas, a mediados de los años 1950, la Oficina de Proyectos Especiales Polaris desarrolló la técnica PERT (Program Evaluation Review Technique).

La base del PERT fue un detallado diagrama de todas las tareas anticipadas en un proyecto, organizadas en una red, la cual representa la dependencia de cada tarea con relación a aquellas tareas que las preceden. Además, los planificadores estimarían o asumirían una distribución de probabilidades para el tiempo, que tomaría realizar cada una de las tareas.

Para cada estimación del tiempo se tenía que proponer tres escenarios: pesimista, optimista, y el más probable.

Por otro lado, en los mismos años 1950 se desarrolló una técnica de planificación y administración fue desarrollada por Du Pont. La técnica CPM (Critical Path Method). Esta técnica también utiliza la representación de una red, pero inicialmente no utilizaba distribuciones de probabilidades para determinar la duración o el plazo de las tareas. Con el avance de las capacidades de los computadores, la técnica CPM fue mejorada utilizando el método de simulación de Monte Carlo. De esta manera la estimación de los tiempos o plazo de cada tarea aplicando la técnica de Monte Carlo dio lugar a la técnica a CPM estocástico, la

cual es ahora la metodología preferida para evaluar el riesgo en la estimación del tiempo en la administración de proyectos.

Otro de los riesgos que causa preocupación a los administradores de proyectos de tecnología de información es el costo de ejecución del proyecto. La técnica usada está basada en la Estructura de Descomposición del Trabajo (EDT o WBS Work Breakdown Structure). La técnica EDT descompone un proyecto en componentes, servicios, facilidades, entre otros; en diferentes niveles. Y en la medida que se va pasando de un nivel a otro, se va mostrando un mayor detalle. La técnica del EDT estimación de costo se formula a partir del EDT al cual se asigna un costo a cada elemento y luego se adicionan los costos de todos los elementos, y se obtiene el costo total. Para poder realizar un análisis cuantitativo del riesgo, los expertos en proyectos tienen que especificar una distribución de probabilidad para cada elemento de la estructura de descomposición de trabajo, y luego la simulación de Monte Carlo es utilizada para estimar una distribución de probabilidad para el costo total del proyecto.

En tanto que en el análisis de riesgo del desempeño del proyecto se utilizan técnicas cualitativas y cuantitativas. En este caso, las técnicas no son genéricas como en el caso de los riesgos asociados con los plazos o los costos; las técnicas utilizadas son más específicas.

### 2.7.2 Proceso de la Administración de Riesgos

#### 2.7.2.1 Planificación de la administración de riesgos

La planificación de la administración de los riesgos es el proceso de decidir cómo enfocar y planear las actividades de la administración de riesgos para un proyecto, y su principal resultado es el plan de administración de riesgo. Un plan de administración de riesgos documenta los procedimientos para administrar los riesgos de un proyecto.

Un plan de administración de riesgos resume cómo la administración de riesgos será ejecutada en un proyecto en particular. Los elementos que se deben incluir en un plan de administración de riesgos son:

**Metodología:**

Se debe establecer cómo la administración de riesgo que será ejecutada en el proyecto. Determinar qué herramientas y fuentes de información estádisponible y aplicable.

**Roles y responsabilidades:**

Determinar quiénes son las personas responsables de implementar las tareas específicas y proporcionar los informes relacionados a la administración de riesgo.

**Presupuesto y plazos:**

Determinar cuáles son los costos y plazos estimados para ejecutar las tareas relacionadas con los riesgos.

**Categoría de riesgos:**

Determinar cuáles son las categorías de los riesgos que serán identificados.

**Probabilidad de riesgo e impacto:**

Cuáles son las probabilidades y los impactos de los riesgos que serán evaluados. Cuáles son las técnicas cualitativas o cuantitativas que serán utilizadas para evaluar los riesgos.

**Documentación de los riesgos:**

Determinarlos formatos de los reportes y los procesos que serán utilizados para las actividades de la administración de riesgos.

#### 2.7.2.2 Identificación de riesgos

La identificación de riesgos es el proceso de comprender qué eventos potencialmente podría dañar o mejorar a un proyecto en particular. Es importante identificar los riesgos potenciales lo más pronto posible, pero también se debe continuar con la identificación de los riesgos basados en los cambios en el entorno del proyecto.

Se cuenta con varias herramientas y técnicas para identificar riesgos. Los administradores de proyectos a menudo empiezan el proceso de identificación de los riesgos revisando la documentación, y la información reciente e histórica relacionada a la organización, y los supuestos que pueden afectar el proyecto.

Después de identificar los riesgos potenciales, los administradores del proyecto pueden utilizar diferentes técnicas para identificar los riesgos. Las cinco técnicas más utilizadas son: la tormenta de ideas, el método Delphi, las entrevistas, el análisis causa efecto, y el análisis FODA (Fortalezas, debilidades, oportunidades, y amenazas).

#### 2.7.2.3 Análisis cualitativo de riesgos

El análisis cuantitativo de riesgos involucra evaluar la probabilidad y el impacto de la identificación de riesgos, para determinar su magnitud y prioridad.

Para poder evaluar cuantitativamente los riesgos se cuenta fundamentalmente con tres herramientas: La matriz de probabilidad e impacto para calcular los factores de riesgos, la técnica de seguimiento de los diez factores de riesgo más importantes, y la evaluación del juicio de expertos.

#### 2.7.2.4 Análisis cuantitativo de los riesgos.

El análisis cuantitativo del riesgo a menudo sucede al análisis cualitativo del riesgo, aunque ambos procesos pueden llevarse por separado o en forma simultánea.

En algunos proyectos, el equipo puede solamente ejecutar el análisis cualitativo. La naturaleza del proyecto y la disponibilidad de tiempo y dinero influyen en el tipo de técnica a utilizar. Los proyectos grandes y complejos que involucran tecnología de punta requieren la aplicación de técnicas cuantitativas. Las principales técnicas para el análisis cuantitativo exigen la recolección de datos, la aplicación de técnicas cuantitativas, y técnicas de modelamiento. Las técnicas de análisis cuantitativo más utilizadas son: el análisis de árboles de decisión, la simulación, y el análisis de sensibilidad.

#### 2.7.2.5 Planificación de la respuesta de los riesgos.

Después que una organización identifica y cuantifica los riesgos, debe desarrollar una apropiada estrategia para poder enfrentarlos.

Las cuatro estrategias de respuesta riesgos negativos son:

a) Evitar los riesgos o eliminar una amenaza específica, generalmente se logra al eliminar sus causas.
b) Aceptar los riesgos o aceptar las consecuencias si el riesgo ocurriese.
c) Transferir los riesgos o trasladar la consecuencia de un riesgo y la responsabilidad por su administración a terceros.
d) Mitigar los riesgos o reducir el impacto de un evento riesgoso al reducir la probabilidad de su ocurrencia.

Las cuatro estrategias para enfrentar los riesgos positivos son:

1) Explotación del riesgo para asegurarnos que el riesgo positivo ocurra.

2) Compartir el riesgo o asignar la propiedad del riesgo a un tercero.
3) Mejora del riesgo o cambiar el tamaño de la oportunidad al identificar y maximizar los inductores claves de un riesgo positivo.
4) Aceptar el riesgo también se aplica a los riesgos positivos cuando el equipo del proyecto no puede o escoge no tomar ninguna acción para enfrentar el riesgo.

#### 2.7.2.6 Monitoreo y control de los riesgos.

El monitoreo y control de los riesgos involucra la ejecución de los procesos de la administración de riesgo para responder a los eventos riesgosos.

Ejecutar los procesos de la administración de riesgos significa asegurar que el reconocimiento de los riesgos es una actividad permanente ejecutada por todos los miembros del equipo a lo largo de la vida del proyecto.

#### 2.7.2.7 Variables independientes

Las variables independientes del proceso de la Administración de Riesgos de los Proyectos son:

Las variables del entorno de la empresa. Estas variables están referidas a aquellos factores y/o variables exógenas que influyen sobre el desempeño de la empresa y del éxito del proyecto. Entre estas variables se tiene: la cultura organizacional, estándares de la industria, la infraestructura, los recursos humanos, las condiciones del mercado, entre otros.

Los activos de los procesos de la organización.

Estos activos de la empresa y son utilizados para lograr el éxito del proyecto. Entre los activos más relevantes podremos citar: las normas y procedimientos administrativos de la empresa, requerimientos de comunicación de la empresa, procedimientos de control financiero de la empresa, procedimientos de administración de riesgos, entre otros.

#### 2.7.2.8 Variables dependientes

• Riesgo de la variabilidad del costo. Cuando se planifica un proyecto de tecnología de información se presupuesta su costo. El administrador del proyecto enfrenta el riesgo que el costo pueda ser mayor o menor.

- Riesgo de la variabilidad del plazo o tiempo. Cuando se planifica un proyecto de tecnología de información se estima el tiempo o el plazo en el cual se culminará el proyecto. El administrador del proyecto enfrenta el riesgo que el tiempo o el plazo pueda ser mayor o menor.

- Riesgo de la variabilidad de la calidad del proyecto. Cuando se planifica un proyecto de tecnología de información se fijan metas para lograr ciertos estándares de calidad. El administrador del proyecto enfrenta el riesgo que las metas de calidad se satisfagan, las excedamos, o no se logren.

# CAPITULO III

# ESTABLECIMIENTO DEL PLAN DE RECUPERACION DE DESASTRES

## 3.1 Establecimiento de escenario considerado.

En esta primera etapa del Plan de Recuperación de Desastres el objetivo es identificar y delimitar el escenario que será objeto de estudio. Estableceremos:

1. Las condiciones físicas del entorno
2. Los servicios y aplicaciones existentes
3. Los equipos presentes

### 3.1.1 Condiciones físicas del entorno.

Estamos considerando una infraestructura SAN y arreglo de servidores, en la cual esta implementado el sistema central de la empresa (SAP). Físicamente de encuentra en la planta de producción.

El site de cómputo abarca una superficie de 10 $m^2$ (2.5 m x 4.0 m) y 3 m de altura de piso falso a plafón.

#### 3.1.1.1 Sistema de Piso Falso

El piso falso está formado por paneles modulares, antiestáticos y de materiales no combustibles, soportados en cada esquina por pedestal y travesaño formando un patrón de cuadricula. La altura de loza a piso falso es de 40 cm.

Debajo del piso falso se encuentra todo el sistema de canalización de datos y eléctrico, separados para evitar cualquier tipo de interferencia electromagnética.

#### 3.1.1.2 Sistema de Climatización

Consta de un aire acondicionado de precisión, el cual mantiene el control de la temperatura y control de humedad. Es un sistema autónomo, independiente a los demás sistemas de enfriamiento del edificio, el cual da servicio de 24x7x365.

#### 3.1.1.3 Seguridad Física.

Existe un sistema de control de accesos de tipo lector de tarjetas, una al exterior y un botón liberador en el interior, mediante los cuales se valida el acceso al site, almacenándolos en una base de datos de los accesos permitidos, accesos denegados y salidas.

#### 3.1.1.4 Sistema de UPS

Se cuenta con 2 UPS de 5KVA marca APC tipo NEMA de 220 V, los cuales soportan la infraestructura del site de computo.

Soportan una carga de 10 KVA en conjunto, dando un periodo de autonomía eléctrica de 15 minutos en un corte de energía eléctrica.

Cabe mencionar que el fin de estos equipos es solo soportar la entrada de la planta eléctrica existente que alimenta a todo el edificio.

### 3.2 Los servicios y aplicaciones existentes

En general, los sistemas SAP tienen la siguiente estructura:

*Ambiente de Desarrollo (DEV,development):* Aquí se realizan los desarrollos y parametrizaciones del sistema. Al realizar un nuevo desarrollo, se genera una orden de transporte. Mediante la misma, el desarrollo pasará a los demás ambientes.

*Ambiente de Testing/Calidad (QA,Quality):* Los objetos generados en Desarrollo pasan a este ambiente por medio de la orden de transporte. En este ambiente, se realizan las pruebas integrales para verificar el correcto funcionamiento de los programas y parametrizaciones.

*Ambiente Productivo (PROD, Production):* Aquí están los datos reales y es el ambiente con el que opera la compañía que posee el sistema SAP.

Adicionalmente, puede usarse un ambiente Sandbox para testeo de configuraciones y desarrollos.

Las aplicaciones soportadas son:

1. SAP ECC (Componente central empresarial, *Enterprise Central Components*) que es el ERP de la empresa. Dentro de los módulos implementados se encuentran:

- FI: Finanzas
- SD: Ventas y Distribución
- MM: Gestión de Materiales
- PP: Gestión de Producción
- WF: Work Flow

En ambientes DEV, QA, PROD

2. BI (Inteligencia de Negocios, *Bussines Inteligent*) Básicamente es un repositorio de la información transaccional del sistema ERP, organizada de tal manera que se adapte mejor a las necesidades de reporteo, disminuyendo los tiempos de consulta y optimizando el uso de recursos de hardware, con el fin de que las gerencias y direcciones puedan obtener información para gestión, plantación y toma de decisiones.

   En ambientes DEV, QA, PROD

3. Portal NETWEAVER. Es en principio un servicio web, que brinda la posibilidad de usarlo como cara (*Frontend*) para aplicaciones SAP, utilizarlo como parte de la Intranet de la organización, exponer aplicaciones a la Extranet (para que los clientes puedan consultar sus facturas a través de la web) y como visualizador de reportes gerenciales de SAP BI

   En ambientes DEV, QA, PROD

El DRP está enfocado en el aplicativo SAP ECC ambiente productivo, que es el ambiente donde la empresa opera, y sobre el cual se realizan todas las operaciones diarias de la organización, contiene toda la información sobre compras, pagos, cobranzas, contabilidad, etc y al mismo acceden los usuarios de las áreas específicas

### 3.3 Equipos Existentes

La infraestructura está formada por una granja de servidores en los cuales se encuentra instalado exclusivamente el sistema operativo.

- El kernel, bases de datos y logs se encuentran almacenados en la SAN.
- La SAN, está formado por dos switches de fibra, unidades de procesamiento, unidades de almacenamiento.
- La estructura de respaldos está formado por una unidad de cintas y un equipo DAS.

Estos dispositivos de describen a continuación.

### 3.3.1 Servidores

La aplicación *SAP ECC en su ambiente Productivo* se encuentra instalada en los siguientes servidores que se describen en la tabla siguiente.

| Descripción | Host Name | Sistema Operativo | Marca | Modelo |
|---|---|---|---|---|
| Servidor | DARECCCL1 | Windows Server 2003 R2 Enterprise x64 | Dell | PowerEdge 2950 |
| Servidor | DARECCCL2 | Windows Server 2003 R2 Enterprise x64 | Dell | PowerEdge 2950 |

Tabla 3.1 Descripción de Servidores Productivos

Los dos servidores están configurados en un arreglo de cluster modo Activo – Pasivo. Es decir que uno de los equipos es el que está prestando el rol de forma continua (activo) y el otro solo está en espera para entrar en funcionamiento en caso de que el otro falle (pasivo).

Fig. 3.1 Cluster

Las aplicaciones de *SAP ECC Desarrollo y Calidad* comparten el mismo servidor, ya que por funciones no requieren un servidor dedicado. Las principales características del servidor se muestran en la tabla siguiente.

| Descripción | Host Name | Sistema Operativo | Marca | Modelo |
|---|---|---|---|---|
| Servidor | DARECCQD | Windows Server 2003 R2 Standar x64 | Dell | PowerEdge 2950 |

Tabla 3.2 Descripción del servidor de calidad y desarrollo

Cada instancia o ambientes (QA y DEV) se encuentran debidamente separados.

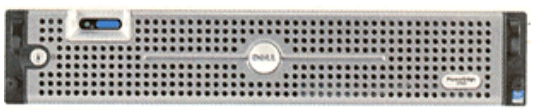

Fig 3.2 Servidor DARECCQD

**Servidor SAP BI**

La aplicación de *SAP BI Productivo* esta implementado sobre un solo servidor, con las características mencionadas en la siguiente tabla.

| Descripción | Host Name | Sistema Operativo | Marca | Modelo |
|---|---|---|---|---|
| Servidor | DARBWP | Windows Server 2003 R2 Standard x64 | Dell | PowerEdge 2950 |

Tabla 3.3 Características del Servidor BI Productivo

Fig 3.3 Servidor DARBWP

Las aplicaciones de *SAP BI Desarrollo y Calidad* comparten el mismo servidor, ya que por funciones no requieren un servidor dedicado. Las principales características del servidor se muestran en la tabla siguiente.

| Descripción | Host Name | Sistema Operativo | Marca | Modelo |
|---|---|---|---|---|
| Servidor | DARBWQD | Windows Server 2003 R2 Standar x64 | Dell | PowerEdge 2950 |

Tabla 3.4 Descripción de Servidor Bi desarrollo y calidad

Cada instancia o ambientes (QA y DEV) se encuentran debidamente separados

Fig 3.4 Servidor DARBWQD

**SAP PORTAL Netwiever**

La aplicación de *SAP PORTAL Netwiever* esta implementado sobre un solo servidor, con las características mencionadas en la siguiente tabla.

| Descripción | Host Name | Sistema Operativo | Marca | Modelo |
|---|---|---|---|---|
| Servidor | DEREPP | Windows Server 2003 R2 Standard x64 | Dell | PowerEdge 2950 |

Tabla 3.5 Descripción de Servidor Netwiever Productivo

Fig 3.5 Servidor DAREPP

Las aplicaciones de *SAP PORTAL NETWEAVER QA y DEV* comparten el mismo servidor, ya que por funciones no requieren un servidor dedicado. Las principales características del servidor se muestran en la tabla siguiente.

| Descripción | Host Name | Sistema Operativo | Marca | Modelo |
|---|---|---|---|---|
| Servidor | DAREPQD | Windows Server 2003 R2 Standar x64 | Dell | PowerEdge 2950 |

Tabla 3.6 Características de Servidor Netweaver QA y DEV

Fig 3.6 Servidor DAREPQD

### 3.3.2 SAN

La red SAN es un modelo DELL/EMC CX300 con tecnología de fibrechannel, formado por los siguientes dispositivos

En esta red de almacenamiento se encuentra la instalación de las aplicaciones de SAP, la base de datos y los logs de cada aplicación.

El sistema de almacenamiento SAN se compone de:

- Unidad de almacenamiento del procesador
- Unidades de almacenamiento en discos
- Dispositivos de interconexión (Switch FC)

**Unidad de almacenamiento del procesador (SP, *Storage Processor*)**

Es el cerebro del sistema de almacenamiento, es equivalente al procesador y la memoria RAM de una computadora personal. A través de un software gestiona la lectura o escritura de cada unidad de almacenamiento y discos. Gestiona tráfico de I/O al mismo tiempo, además de monitorear el estado de los discos.

El modelo empleado se muestra en la siguiente tabla.

| Descripción | Marca | Modelo |
|---|---|---|
| SP | Dell | E-CX3-40C |

Tabla 3.7 Descripción de la unidad de procesamiento SAN

Se cuentan con dos unidades para redundancia.

Fig 3.7 Unidades SP

**Unidades de Arreglos de disco Fibre Channel (DAE, *Disk Array Enclosure*)**

Son sistemas de almacenamiento que soporta de 2 a 4 operaciones Gb/s en discos de FibreChannel. Detecta la velocidad de almacenamiento del anfitrión de entrada de E/S y ajusta la velocidad de los puertos de front-end para la velocidad más baja que los sentidos. La velocidad de cada puerto de back-end se determina por la velocidad de la DAE conectados a él.

El sistema de almacenamiento requiere de al menos cinco discos y trabaja en conjunto con uno o más recintos de arreglo de discos (DAE) para proporcionar terabytes de disco de almacenamiento de alta disponibilidad, el modelo utilizado se muestra en la siguiente tabla.

| Descripción | Marca | Modelo |
|---|---|---|
| DAE | Dell | E-FC4 |

Tabla 3.8 Descripción de Unidades DAE

Se cuenta con 6 unidades DAE de almacenamiento

Fig 3.8 Unidades DAE

**Dispositivos de interconexión: Switch Fiber Channel (FC).**

Una de las partes más importantes de una red de almacenamiento SAN, y al igual que ocurre en redes Ethernet, son los Conmutadores o Switch, es decir, la electrónica de red. Estos dispositivos son los que permitirán interconectar al resto de dispositivos de la red de almacenamiento SAN, como los Servidores, las unidades de Almacenamiento y las Librerías de Cintas.

El modelo se muestra en la siguiente tabla.

| Descripción | Host Name | Sistema Operativo | Marca | Modelo |
|---|---|---|---|---|
| Switch FC | | NA | Dell | E-Switch |
| Switch FC | | NA | Dell | E-Switch |

Tabla 3.9 Descripción de los Switches de fibra

Fig. 3.9 Swittch de Fibra

La SAN cuenta con dos canales de comunicación de Fibre Channel, para redundancia de comunicación.

**Diagrama de Red**

A la red de almacenamiento SAN, están conectados los servidores de las instancias de SAP, (ECC, BI, Portal, en sus tres ambientes desarrollo, calidad y producción). El kernel de cada aplicación se encuentra en la unidad de almacenamiento, al igual que las bases de datos.

En los servidores solo se encuentra el sistema operativo Windows Server 2003, el cual mapea los accesos a las unidades de la SAN Los usuarios accesan a los servidores mediante la LAN de la empresa, y a su vez los servidores accesan a la unidad de almacenamiento a través de los canales de fibre cannel (Canal A y Canal B)

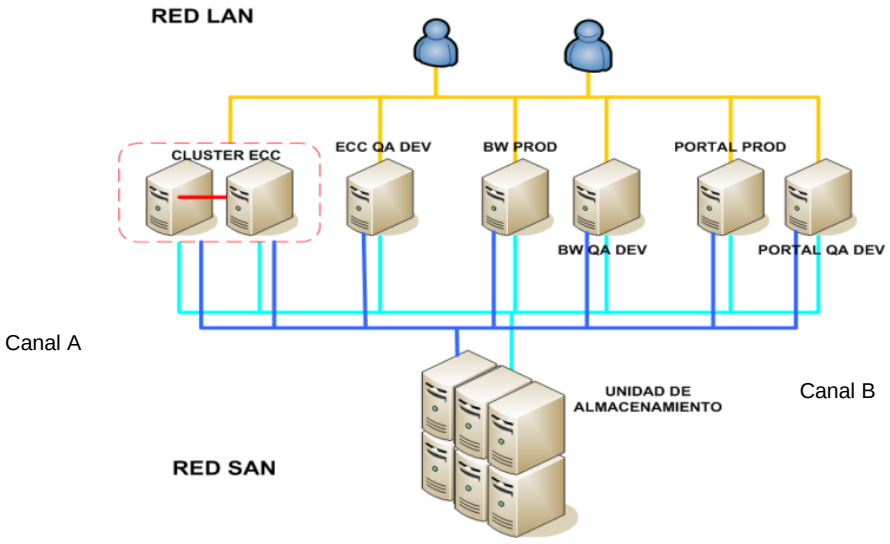


Fig 3.10 Red SAN

Físicamente los servidores de las aplicaciones de SAP y la red de almacenamiento (SAN) con todos sus componentes están montados en un gabinete de 42 Unidades de Rack, como se muestra en las figuras siguientes.

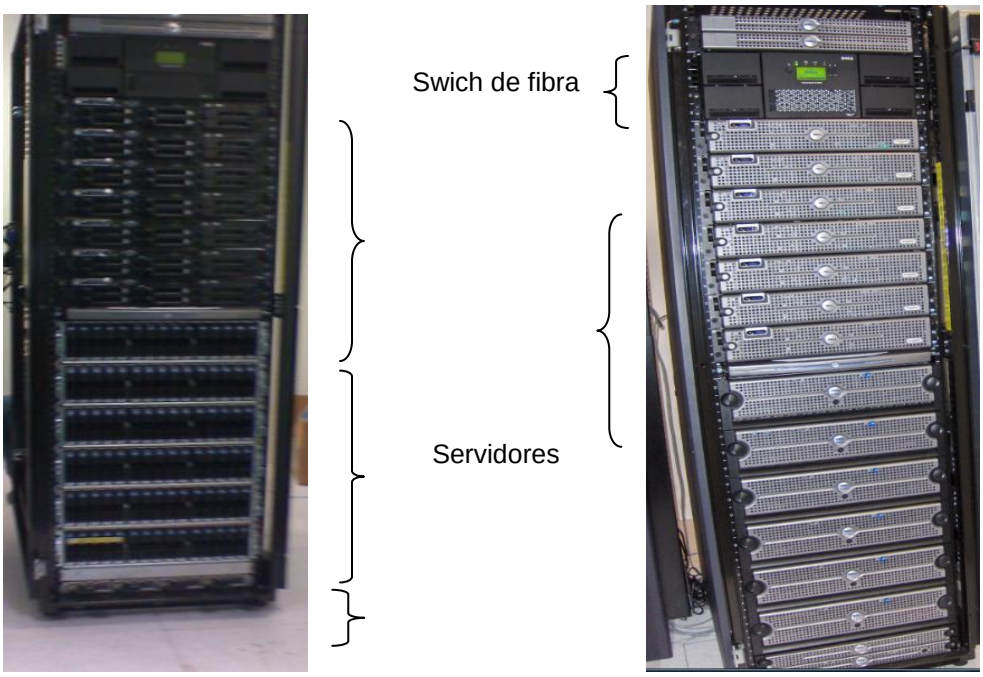


Fig 3.11 Red SAN (Instalados)

## 3.4 Definición del tipo de operación en una contingencia

Los principales tipos de operación considerados en una emergencia son:

### 3.4.1 Operación Normal Inicial

Es la operación que se registraba antes de ocurrir el desastre. Asimismo define las condiciones que se deben alcanzar como objetivo final mediante la ejecución del DRP (*Plan de Recuperación de Desastres*).

El escenario del DRP contempla el ambiente productivo de SAP ECC montado sobre un cluster de Windows.

Los principales componentes del cluster son:

**Nodo** (node): se trata de uno cualquiera de los servidores que componen el cluster, los nodos se pueden agregar o quitar del cluster a lo largo del tiempo. Paradójicamente puede existir un cluster de un único nodo aunque no parezca de gran utilidad.

**Recurso** (resource): se trata de un componente hardware (disco fisico, red) o software (dirección IP, nombre de red, script...) que forma parte del cluster. Entre los recursos se producen dependencias que se han de reflejar en la configuración de los mismos. Por ejemplo entre un nombre de red netbios y una dirección IP, si la dirección falla entonces el nombre de red deberá fallar en cadena al ser componentes directamente relacionados.

**Grupo** (group): es una agrupación de recursos, un grupo de recursos es la única unidad del cluster donde se puede realizar failover, cuando esto ocurre se mueven todos los recursos que lo componen de un nodo a otro. Esta es la razón que los diferentes recursos componentes de un servicio o instancia de aplicación se agrupen en un mismo grupo, un recurso determinado no puede pertenecer a más de un grupo de recursos. Cada grupo tiene una lista de nodos (preferedowner) que por orden de preferencia se escogen a la hora de determinar hacia que nodo mover el grupo cuando se realiza un failover.

**Quorum**: es un disco usado para compartir, entre los distintos nodos, información respecto a la configuración del cluster además en el caso de fallo en las comunicaciones entre los distintos nodos el que tenga en ese momento la propiedad del recurso Quorum. Dentro del quorum disk podemos encontrar la carpeta MSCS en la cual se alojan el log del quorum (quolog.log), que es en realidad un log de transacciones de los cambios realizados en la base de datos del cluster. También se encuentra dentro de la carpeta MSCS un fichero con nombre chk*.tmp hacia el cual cada nodo replica desde local el fichero local de registro de cluster %SystemRoot%\Cluster\CLUSDB, este fichero se encuentra cada nodo y es al que van primero los cambios realizados a la configuración del cluster.

**Shared Quorum**: se trata de la configuración más habitual y recomendada, todos los clusters comparten el acceso a este recurso de disco físico.

**Local Quorum**: aquí el quorum se localizaría en uno de los discos locales de uno de los nodos del cluster, este tipo de configuración solo tienen sentido para recuperación de desastres o durante mantenimientos o fallos del disco compartido de quorum, iniciando el servicio de cluster, ClusterService (clussvc.exe), con el parámetro /FIXQUORUM se creara un quorum local y solo tendríamos que seleccionarlo como quorum.

Recordemos que SAP ECC productivo está instalado sobre un cluster activo pasivo, formado por dos nodos.

- Nodo 1
- Nodo 2

Ambos servidores se encuentran en dominio, con tres adaptadores de red cada uno, el adaptador de red PRIVADA es para la red del clúster, para que se comuniquen de forma interna los servidores.

Otro adaptador es PUBLICA que sirve para conectar los servidores a la LAN donde están sus PC's clientes y puedan acceder a los recursos o para que mis servidores accedan a ellos.

Y finalmente otro adaptador llamado HBA (*iniciador FibreChannel*) para conectar a la NAS cada servidor.

Recordemos que el kernell de SAP así como la configuración y parametrizacion, residen en los discos de la SAN, al igual que la base de datos.

En la siguiente figura se muestra un diagrama de conexión del cluster en donde está montada la aplicación de SAP ECC considerada para el DRP

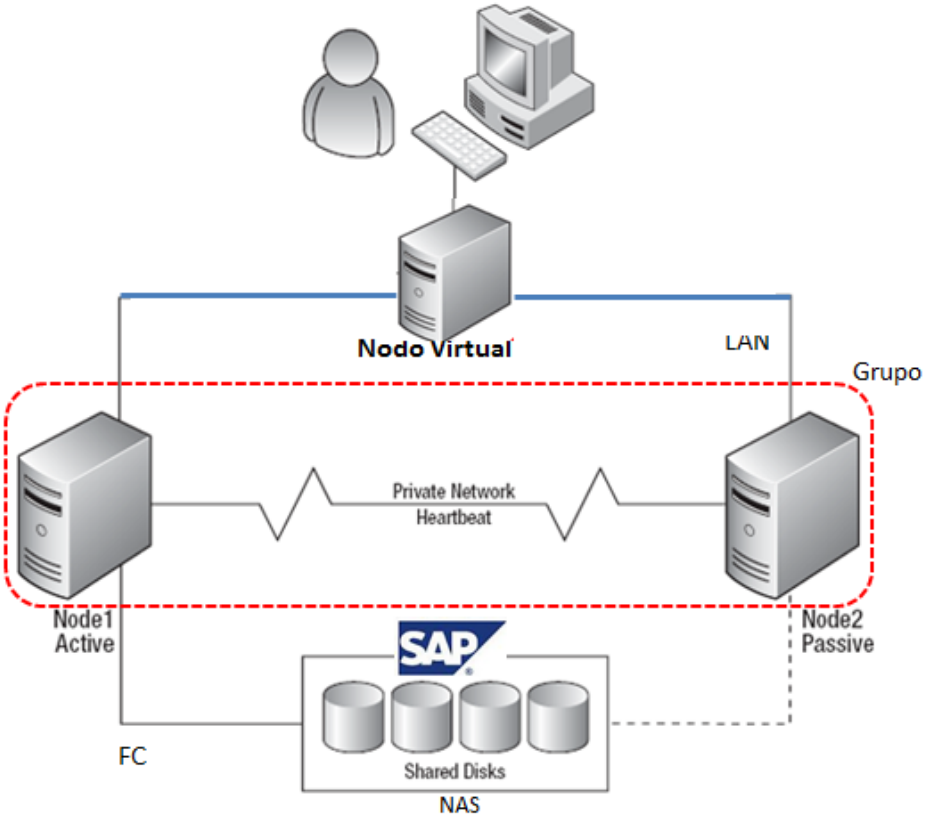


Fig. 3.12 Diagrama de Escenario Considerado

Los usuarios realizan el inicio de sesión a SAP a través de SAP LOGON, que es un programa de Windows que se utiliza para iniciar sesión en los sistemas SAP en una PC Windows.

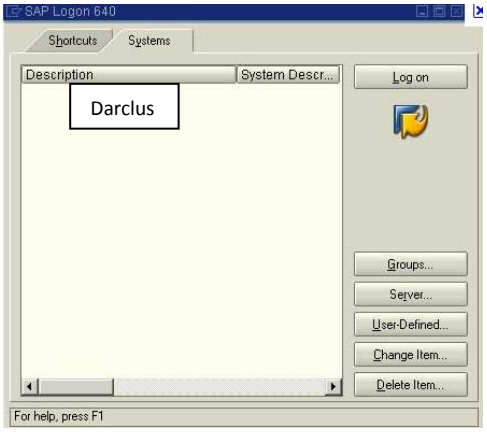


Fig. 3.13 Pantalla de acceso a SAP

En esta aplicación el acceso apunta a el servidor llamado “DARCLUS” que es el nombre del host virtual del cluster de windows formado por los dos nodos.

El servidor provee el servicio a los sitios de:

- Oficinas
- Planta
- Centro de distribución

Todos los usuarios acceden a este servidor para sus operaciones diarias.

### 3.4.2 Operación durante el desastre

Mediante la ejecución de los procedimientos que reciben el nombre de DRP, se llega a esta instancia en la cual los servicios y aplicaciones han sido recuperados, pero no se encuentran ejecutando en su lugar original o bajo las mismas condiciones en que se encontraban originalmente.

El tiempo desde que se declara la emergencia hasta que se alcanza la operación durante el desastre no debe de ser superior a los tiempos máximos tolerables de suspensión definidos para cada una de las prestaciones.

En nuestro escenario considerado el ambiente de SAP ECC productivo será restaurado en un solo servidor en una ubicación alterna. Sera un servidor con todos sus recursos de manera interna, es decir no estará conectado a ningún medio de almacenamiento externo. Para los usuarios el escenario será transparente ya que no se cambiaran los nombres de los host de conexión.

El direccionamiento IP cambiara pero se realizarán loa ajustes en el DNS (*Sistema de Resolución de Nombres, DomainNameSystem*) para que no sea necesario cambiar configuraciones a nivel usuario o aplicación.

El servidor considerado es un equipo DELL POWER EDGE 2950, con espacio necesario de almacenamiento para soportar la configuración de SAP y base de datos de manera interna.

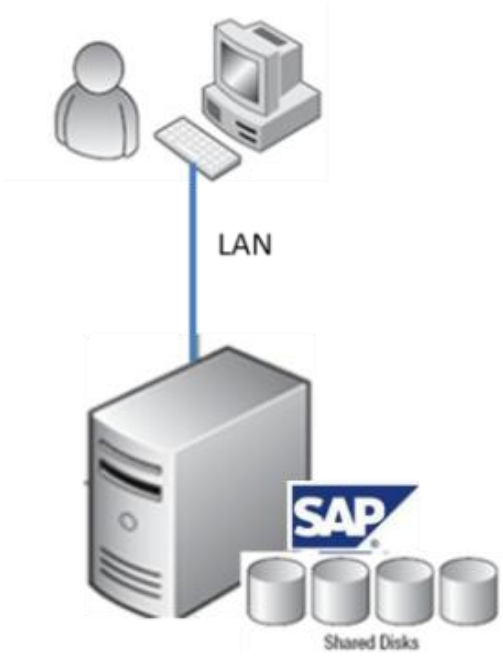


Fig. 3.14 Esquema de conexión en el DRP

El acceso a SAP es mediante SAP LOGON, sin necesidad de realizar cambio alguno en la configuración del cliente.


Fig. 3.15 Acceso al sistema SAP

Con lo que se tendrá acceso al sistema sin ningún cambio para el usuario de manera aplicativa.

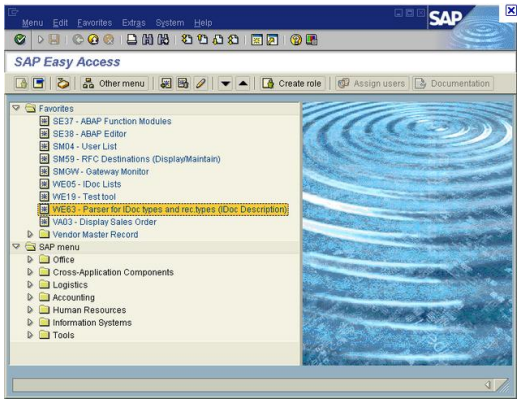


Fig. 3.16 Pantalla de inicio de SAP

### 3.4.3 Operación Normal Restablecida

Mediante la ejecución de los procedimientos llamados Restablecimiento de las condiciones normales se alcanza la última instancia, en la cual todos los servicios y aplicaciones se encuentran ejecutando correctamente y bajo las mismas condiciones que presentaban antes de la contingencia.

Para alcanzar este tipo de operación, es posible que haya que considerar una suspensión de programada de alcance total o parcial de las prestaciones, para lo cual es necesario acotar el tiempo de interrupción al mínimo indispensable. Este procedimiento esta fuera de nuestro alcance el este caso de estudio. El siguiente diagrama muestra un diagrama con los tipos de operaciones durante una contingencia.

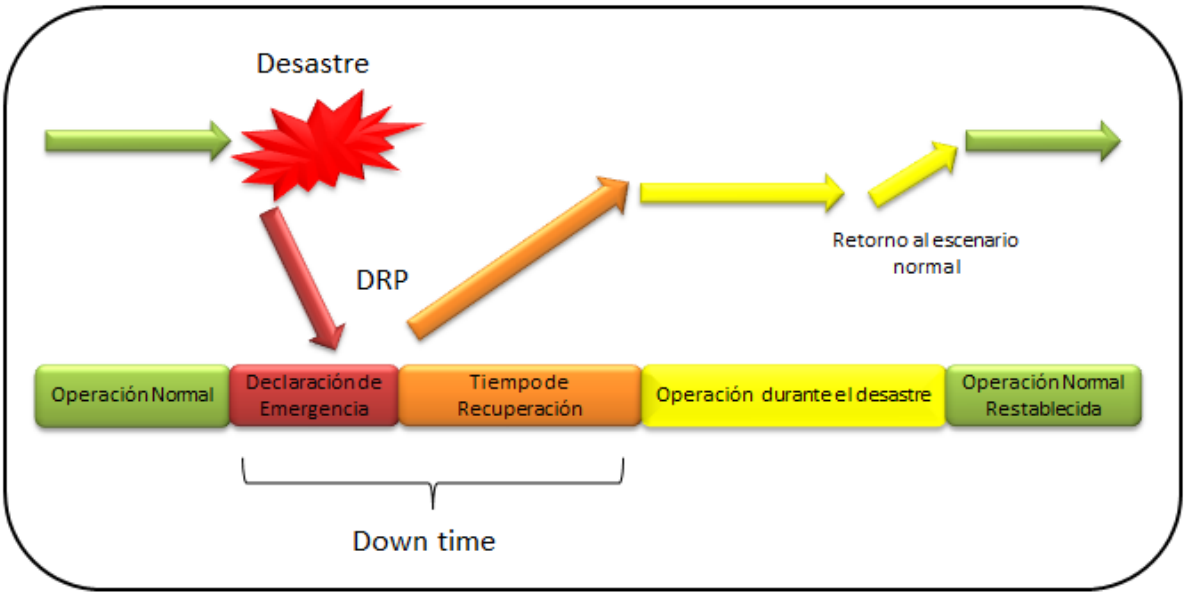


Fig. 3.17 Diagrama de fases durante la contingencia

### 3.5 Establecimiento de criticidades

El siguiente paso en la construcción de un Plan de Recuperación de Desastres, es la determinación de la criticidad de los activos o BIA (Análisis de Impacto de Negocio, *Business Impact Analysis*)

La idea es que esta etapa se establezca la criticidad de las aplicaciones, de los equipos y de los servicios que sostienen al negocio. En función del impacto producido por la suspensión de las prestaciones del entorno sistematizado, se determina la criticidad y el tiempo máximo de tolerancia de corte de las mismas.

El propósito fundamental del Análisis de Impacto sobre el negocio, conocido más comúnmente como BIA, (Business Impact Análisis) es determinar y entender qué procesos son esenciales para la continuidad de las operaciones y calcular su posible impacto.

De acuerdo al Business Continuity Institute se tienen cuatro objetivos principales al realizar un análisis de impacto:

- Entender los procesos críticos que soportan el servicio, la prioridad de cada uno de estos servicios y los tiempos estimados de recuperación (RTO, Recovery Time Objective – tiempo de recuperación objetivo)
- Determinar los tiempos máximos tolerables de interrupción (MTD, Maximum Tolerable
- Downtime – tiempo máximo tolerable fuera de servicio)
- Apoyar el proceso de determinar las estrategias adecuadas de recuperación.

### 3.5.1 Clasificación de impactos

**Críticos**

- Funciones que pueden realizarse sólo si las capacidades se reemplazan por otras idénticas.
- No pueden reemplazarse por métodos manuales.
- Muy baja tolerancia a interrupciones.

**Vitales**

- Pueden realizarse manualmente por un periodo breve.
- Costo de interrupción un poco más bajos, sólo si son restaurados dentro de un tiempo determinado (5 ó menos días, por ejemplo).

**Sensitivos**

- Funciones que pueden realizarse manualmente por un periodo prolongado a un costo tolerable.
- El proceso manual puede ser complicado y requeriría de personal adicional.

**No críticos**

- Funciones que pueden interrumpirse por tiempos prolongados a un costo pequeño o nulo.

El análisis de impacto sobre el negocio, está basado en escenarios catastróficos que al darse su ocurrencia impactarían la infraestructura y procesos que soporta la realización de las operaciones y servicios, lo que requerirá que el sistema posea unas estrategias de recuperación a corto, mediano y largo plazo, que garanticen su supervivencia por el periodo que duren las consecuencias del desastre.

### 3.5.2 Tiempos de recuperación necesitados en el proceso

Una vez definidos los procesos críticos del sistema, se debe proceder a realizar un análisis de impacto identificando qué sucede si uno de estos procesos permanece por fuera una determinada cantidad de tiempo. Se busca de esta manera estimar el tiempo máximo que estando el sistema interrumpido, pondría en riesgo la continuidad del negocio.

Para calcular este intervalo de tiempo no solamente se deben considerar los costos asociados de la interrupción del servicio, sino que también se deben considerar los costos asociados a la estrategia de recuperación, la cual entre más corta sea el tiempo que se establezca de recuperación mayor será el valor monetario de su implementación.

### 3.6 Análisis de Impacto

Para afrontar esta fase con garantías de éxito, hay que obtener un entendimiento de la organización, procesos de negocio clave y los recursos de TI utilizados por la organización para soportar los procesos de negocio clave. Esta fase requiere un alto grado de soporte por la alta gerencia y una gran involucración tanto del personal de TI y de usuario final. Debe determinarse la criticidad de los recursos de información (aplicaciones, datos, redes, software de sistemas, instalaciones, etc.) que soportan a los procesos críticos de negocio de una organización. Es importante incluir todo tipo de recursos de información e ir más allá de los tradicionales, por ejemplo, muchos grupos de usuario final han instalado sofisticadas redes de área local y estaciones de trabajo en las que se realizan funciones críticas diariamente.

Una de las formas de afrontar este análisis es respondiendo, por las personas adecuadas, a cuestiones como:

***A. ¿Cuáles son los recursos críticos de información relacionados con un proceso de negocio crítico de la organización?***

Esta es la primera consideración, porque una interrupción de un recurso de información no es un desastre en sí mismo, a 170 menos que este recurso dé soporte a un proceso crítico de negocio. Ejemplos de procesos críticos de negocio pueden ser:

- recepción de pagos
- producción
- nóminas
- entrega de productos terminados

Se tiene que evaluar cada proceso para determinar su criticidad. Indicaciones de la criticidad son, por ejemplo:

- el proceso involucra vidas y salud de las personas
- la interrupción del proceso puede causar un pérdida beneficios a la organización o incurrir en costes extras no aceptables
- el proceso debe cumplir requerimientos legales o estatutarios.

***B. ¿Cuál es tiempo crítico de recuperación para los recursos de información en el que se debe restaurar el proceso de negocio sin incurrir en pérdidas significativas o no aceptables?***

El impacto de una interrupción se incrementa en función de su duración. Sin embargo, el coste de su recuperación se reduce si se requiere con menos urgencia. Hay un punto en tiempo, a partir del cual el impacto de la interrupción comenzará a ser mayor que el coste de la recuperación.

La duración de este periodo de tiempo depende de la naturaleza del negocio interrumpido. Por ejemplo, instituciones financieras, tales como bancos, normalmente tendrán un mucho más corto periodo de tiempo de recuperación que instituciones manufactureras. También, el momento del año o el día de la semana pueden afectar a la ventana de tiempo de recuperación.

Por ejemplo, un banco con una interrupción mayor en un sábado a medianoche tiene un tiempo más largo para la recuperación que en un lunes a medianoche (basándose en la asunción que el banco no procesa los domingos)

***C. ¿Cuál es la clasificación de riesgos de los sistemas?***

Esto involucra una determinación basada en riesgos del impacto derivado de un periodo de tiempo de recuperación crítico, así como de la probabilidad de que ocurra una interrupción adversa. Muchas organizaciones utilizan un riesgo de ocurrencia para determinar un razonable coste que deben preparar. Por ejemplo, si se determina que hay un 0.1% de que en los próximos cinco años la organización sufrirá un desastre serio. Si se evaluar que el impacto de la interrupción será de $100 millones de pesos, entonces el máximo razonable coste a preparar será de 0.1% * $100 millones de pesos = $ 100,000.00 pesos durante los próximos cinco años. Este tema será tratado a detalle en el siguiente capítulo.

Con este proceso de análisis, se pueden priorizar los sistemas para desarrollar las estrategias de recuperación. El procedimiento de clasificación de riesgos debe realizarse en coordinación con el personal de procesamiento de la información y el de usuario final.

### 3.6.1 Caso Práctico.

En la determinación de criticidades para nuestro escenario considerado procederemos con realizar un listado de los equipos presentes. Identificaremos la función que realizan, cuantas horas de servicio brindan al día, a cuantas localidades y número de usuarios soportan.

En base a este listado se identificaran los equipos que deban de tener un alto grado de:

- Disponibilidad
- Soporte a usuarios

En la siguiente tabla se muestra el listado de los equipos presentes con sus características de servicio.

| Equipos | Función | Horas de servicio | Localidades | Número de usuarios | Aplicaciones Soportadas |
|---|---|---|---|---|---|
| Darecccl1<br>Darecccl2 | Cluster SAP ERP | 18 hrs | Oficinas<br>Planta<br>CEDIS | 100 | SAP ERP Productivo<br>Módulos de:<br>MM, SD, FI, CO, MRP |
| Dareccqd | Servidor de calidad y desarrollo | 10hrs | Oficinas | 5 | SAP ERP Productivo<br>Módulos de:<br>MM, SD, FI, CO, MRP |
| Darbwp | Servidor productivo | 12 hrs | Oficinas<br>Planta<br>CEDIS | 30 | Reporteador BI de SAP |
| Darbwqd | Servidor de calidad y desarrollo | 10 hrs | Oficinas | 5 | Reporteador BI de SAP |
| Darepp | Servidor productivo | 12 hrs | Oficinas<br>Planta<br>CEDIS | 30 | Portal de SAP |
| Darepqd | Servidor de calidad y desarrollo | 10 hrs | Oficinas | 5 | Portal SAP |
| SP | Unidad procesamiento de almacenamiento SAN | 20 hrs | Oficinas<br>Planta<br>CEDIS | 100 | Navhisphere<br>Gestiona el acceso a los medios de almacenamiento |
| DAE | Unidades de almacenamiento | 20 hrs | Oficinas<br>Planta<br>CEDIS | 100 | Almacenamiento de información |
| SWsan1 | Switch FC | 20 hrs | Oficinas<br>Planta<br>CEDIS | 100 | Acceso a la SAN |
| SWsan2 | Switch FC | 20 hrs | Oficinas<br>Planta<br>CEDIS | 100 | Acceso a la SAN |

Tabla 3.6.1 Equipos presentes

De la tabla anterior podemos determinar que los equipos que brinda un servicio mayor de usuarios y más alta disponibilidad requieren, son:

- Darecccl1
- Dareeccl2
- DAE
- SP
- Switch1
- Switch2

El siguiente paso es determinar las criticidades e impactos de no contar con un equipo, construiremos una tabla indicando el impacto de no contar con el equipo y en conjunto con las áreas involucradas se determinará la parada máxima que pueden tener estos equipos.

Es necesario considerar establecer este tiempo en base a un previo acuerdo con los líderes de las área afectas, ya que este tiempo no debe de ser establecido únicamente por el área de IT, ya que es una decisión de negocio. En este caso se consideró a los directores de:

- Operaciones
- Producción
- Finanzas
- RH
- Comercial y Ventas

Mediante la información recabada podemos realizar la siguiente tabla en donde estableceremos el impacto de cada equipo.

| ID | Equipo | Función | Impacto | Tolerancia Máxima | Afectación |
|---|---|---|---|---|---|
| 1 | Darecccl1 | Nodo 1 SAP ECC Productivo | Critico | 8 hrs | No es posible el acceso a SAP. |
| 2 | Darecccl2 | Nodo 2 SAP ECC Productivo | Critico | 8 hrs | No es posible el acceso a SAP. |
| 3 | Dareccqd | ECCSAPQA y DEV | Sensitivo | 72 hrs | Afectación a pruebas de nuevos desarrollos. No es posible realizar nuevos desarrollos |
| 4 | Darbwp | BI de SAP Productivo | Vital | 36hrs | Afectación en la consulta de información directiva. |
| 5 | Darbwqd | BI de SAP QA y DEv | Sensitivo | 72hrs | Afectación a pruebas de nuevos desarrollos. No es posible realizar nuevos desarrollos |
| 6 | Darepp | Portal de SAP Productivo | Vital | 36hrs | Afectación en el acceso al portal WEB. |
| 7 | Darepqd | Portal de SAP Productivo | Sensitivo | 72hrs | Afectación a pruebas de nuevos desarrollos. No es posible realizar nuevos desarrollos |
| 8 | SP | Unidad procesamiento de almacenamiento SAN | Critico | 8 hrs | Perdida de acceso a la información de: Bases de datos Configuración del sistema SAP |
| 9 | DAE | Unidades de almacenamiento | Critico | 8 hrs | Perdida de información de: Bases de datos Configuración del sistema SAP |
| 10 | SWsan1 | Switch FC | Critico | 8 hrs | Perdida de acceso a la información de: Bases de datos Configuración del sistema SAP |
| 11 | SWsan2 | Switch FC | Critico | 8 hrs | Perdida de acceso a la información de: Bases de datos Configuración del sistema SAP |

Tabla 3.6.2 Impactos por equipos

De la tabla anterior podemos identificar que los equipos con un impacto crítico y en los cuales el tiempo de caída debe de ser menor son:

- Darecccl1
- Darecccl2
- SP
- SAE
- SWsan1
- SWsan2

Ahora se identificara las criticidades por aplicaciones, empleando el mismo procedimiento empleado para las criticidades de los equipos.

La siguiente tabla muestra los servicios y aplicaciones en el entorno SAP.

| ID | Aplicación | Función | Impacto | Tolerancia Máxima | Afectación |
|---|---|---|---|---|---|
| 1 | ECC Productivo | Sistema ERP | Crítico | 8 hrs | Afectación a todos los usuarios de Oficinas, Planta y CEDIS, el acceso a SAP no es posible<br>Paro total de actividades administrativas.<br>Usuarios afectados: Todos |
| 2 | ECC QA y DEV | Ambiente de QA y Dev del ERP | Sensitivo | 72 hrs | Afectación de nuevos desarrollos y pruebas.<br>Usuarios afectados: Desarrolladores y usuarios que solicitan nuevos desarrollos |
| 3 | BW Productivo | Reportador BI de ERP | Vital | 36hrs | Afectación en la consulta de información directiva.<br>Usuarios afectados: gerencias y direcciones de Oficinas, Planta y CEDIS |
| 4 | BW QA y DEV | Ambiente QA y DEv de reportador BI | Sensitivo | 72 hrs | Afectación de nuevos desarrollos y pruebas.<br>Usuarios afectados: Desarrolladores y usuarios que solicitan nuevos desarrollos |
| 5 | EP Productivo | Portal de ERP | Vital | 36hrs | Afectación en la consulta del portal WEB.<br>Usuario afectados: Usuarios móviles de Oficinas, Planta y CEDIS |
| 6 | EP QA y DEV | Ambiente QA y DEV de Portal ERP | Sensitivo | 72 hrs | Afectación de nuevos desarrollos y pruebas.<br>Usuarios afectados: Desarrolladores y usuarios que solicitan nuevos desarrollos |

Tabla 3.6.3 Impactos de aplicaciones y servicios

De la tabla anterior podemos identificar que la aplicación con un mayor impacto es:

- ✓ ***Sistema SAP ERP***

Bajo este análisis podemos determinar los siguientes resultados.

| Equipo/ Aplicación | Función | Impacto | Tolerancia Máxima | Afectación |
|---|---|---|---|---|
| Darecccl1 | Nodo 1 SAP ECC Productivo | Critico | 8 Hrs | No es posible el acceso a SAP. |
| Dareccl2 | Nodo 2 SAP ECC Productivo | Critico | 8 Hrs | No es posible el acceso a SAP |
| SP | Unidad de procesamiento de almacenamiento SAN | Critico | 8 Hrs | Perdida de acceso a la información de:<br>• Bases de datos<br>• Configuración del sistema SAP |
| DAE | Unidades de almacenamiento | Critico | 8 Hrs | Perdida de información de:<br>• Bases de datos<br>• Configuración del sistema SAP |
| Swsan1 | Switch FC | Crítico | 8 Hrs | Perdida de acceso a la información de:<br>• Bases de datos<br>• Configuración del sistema SAP |
| SWsan2 | Switch FC | Crítico | 8 Hrs | Perdida de acceso a la información de:<br>• Bases de datos<br>• Configuración del sistema SAP |
| SAP ERP Productivo | Sistema Productivo | Critico | 8 Hrs | Afectación a todos los usuarios de Oficinas, Planta y CEDIS, el acceso a SAP no es posible<br>Paro total de actividades administrativas.<br>Usuarios afectados: Todos |

Tabla 3.6.3 Resultados

## 3.7 Análisis de riesgos

Se establece que la administración del riesgo del proyecto es el arte y la ciencia de identificar, analizar, y responder a los riesgos a lo largo de la vida de un proyecto, con el propósito de lograr los objetivos del proyecto.

La administración de riesgo del proyecto puede tener un impacto positivo en la selección de proyectos, en la determinación del alcance de los proyectos, y desarrollar estimados más reales de costos y plazos.

Una buena administración del riesgo de proyectos a menudo pasa desapercibida. Cuando la administración de riesgos es efectiva, los resultados se reflejan en el menor número de problemas. En algunas ocasiones es difícil determinar si la administración de riesgos o la buena suerte fue la responsable de un adecuado desarrollo de un proyecto de tecnología de información.

Pero los integrantes de un proyecto saben que sus proyectos trabajaron mejor debido a la buena administración de riesgos.

En esta etapa se analizan los riesgos presentes en el entorno, para determinar que riesgos se pueden mitigar, cuales pueden transferirse y cuales se deben de asumir.

No es posible eliminar todos los riesgos sino que se pueden mitigar (empleando medidas para reducirlos), transferir (ceder su responsabilidad a otra persona) o asumir (cuando se decide correr el riesgo con sus posibles consecuencias.

Sin embargo siempre existen riesgos remanentes y desconocidos.

Es más, constantemente surgen nuevos riesgos a medida que la tecnología avanza y los sistemas cambian. Los entornos informáticos suelen acompañar estos cambios adaptándose a los requerimientos tecnológicos del momento. Es por eso que surgen nuevos riesgos día a día.

Los riesgos pueden ser:

> **Tecnológicos:** Si tienen origen o afectan aspectos técnicos del entorno (como deterioro de los equipos, falta de disponibilidad de recursos, etc.)
>
> **Funcionales:** Si tienen origen o afectan aspectos funcionales del entorno (como posibles descubrimiento de información pos la existencia de contraseña por default, el acceso no autorizado a los recursos por una pobre autenticación de usuarios, etc.)

Todos los entornos están expuestos a amenazas, vulnerabilidades, algunas conocidas, otras no, pero están presentes. Existe una relación entre tipo de desastre y sus efectos, y por supuesto su probabilidad de ocurrencia. Los riesgos reales y potenciales son variables en el tiempo y lugar.

### 3.7.1 Calculo del Análisis de riesgos

En esta parte de la elaboración del DRP se debe evaluar su riesgo asociado a cada uno de los activos (aplicaciones, servidores, etc.), determinar su probabilidad de ocurrencia y medir su impacto del entorno.

Comencemos este análisis identificando los riesgos (mediante la identificación de sus elementos) y estableciendo el riesgo total (o exposición bruta al riesgo) y luego residual, en términos cuantitativos y cualitativos.

Cuando se refiere al riesgo total, se refiere la combinación de los elementos que lo conforman. Comúnmente se calcula el valor del impacto promedio por la probabilidad de ocurrencia para cada amenaza y activo.

De esta manera tendremos, para cada combinación válida de activos y amenazas:

**RT (Riesgo total) = Probabilidad x Impacto Promedio.**

Por ejemplo, si la probabilidad de un incendio es de 0.0001 y el impacto promedio en términos monetarios de los activos amenazados por un incendio es de $ 1, 200,000.00, la exposición al riesgo anual es de:

*RT= 0.0001 x $ 1, 200,000.00 = $ 120*

A este cálculo se debe agregar el efecto de medidas mitigantes de las amenazas, generándose él riesgo residual. Es riesgo residual es el riesgo remanente luego de la aplicación de medidas destinadas a mitigar los riesgos existentes.

Las medidas mencionadas son aquellas que generalmente se conocen como controles. De hecho, el riesgo residual es una medida del riesgo total remanente luego de contemplar la efectividad de las acciones mitigantes existentes.

De esta manera siguiendo con el ejemplo anterior, si se contrata un seguro sobre la totalidad de los activos, el riego residual sería cero. Por otra parte si se asegurará solo la mitad del capital, el riesgo residual sería igual a $ 60.

No es nada sencillo cuantificar adecuadamente los riesgos, por lo que generalmente se utiliza un enfoque cualitativo, expresando los riesgos en:

1. **Altos**
2. **Medios**
3. **Bajos**

El proceso de análisis descrito genera habitualmente un documento que se conoce como matriz de riesgos. En este documento se ilustran todos los elementos identificados, sus relaciones y los cálculos realizados. La sumatoria de los riesgos residuales calculados es la exposición neta total de la organización a los riesgos.

La afirmación anterior fue efectuada con el supuesto de que el resultado obtenido es positivo. En caso que el resultado sea negativo se establece que la organización se encuentra cubierta de todos los riesgos analizados, pero sin embargo, por que tiene más controles que los

necesarios. Realizar el análisis de riesgos es indispensable para lograr administrar adecuadamente los mismos.

Administrar el riesgo refiere a gestionar los recursos de la organización para lograr un nivel de exposición determinado. Este nivel es generalmente establecido por tipo de activo, permitiendo menor exposición cuanto más crítico es ese activo.

El ciclo de administración de riesgo se cierra (luego de efectuar las tareas referentes al análisis) con la determinación de las acciones a seguir respecto a los riesgos residuales identificados.

Estas acciones pueden ser:

- **Controlar el riesgo:** Se fortalecen los controles existentes o se agregan nuevos.
- **Eliminar riesgos:** Se elimina el activo relacionado o por ende el riesgo
- **Compartir el riesgo:** Mediante acuerdos se traspasa parte del riesgo a un tercero.
- **Aceptar el riesgo:** Determinar que el nivel de exposición es el adecuado.

La opción elegida deberá de ser adecuadamente fundamentada y autorizada por el nivel jerárquico correspondiente sobre la base del riesgo asociado.

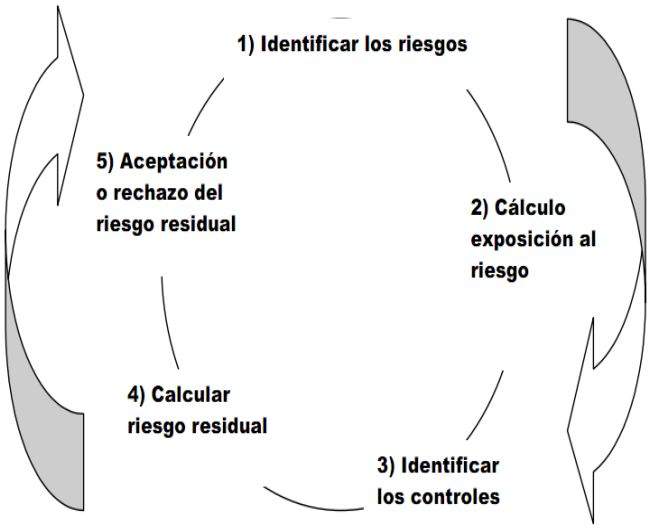


Fig. 3.18 Análisis de Riesgos

### 3.7.2 Realización de la matriz de riesgos.

En la siguiente tabla desarrollaremos una matriz de riesgos, donde:

- En cada fila de presenta una amenaza identificada.

- En la columna de probabilidad se indica cuan probable es que esa amenaza actúe con independencia de los controles que existan o que se establezcan. La certeza es el 100% y la imposibilidad es 0%. Cada porcentaje de cada fila es manejado en forma independiente.
- En la columnas siguientes de indica para cada uno de los activos a proteger cuál es el importe de la pérdida media estimada que ocasionaría esa amenaza en ese activo.
- Los datos precedentes permiten calcular la columna siguiente, riesgo total, el cual sumariza los productos de las probabilidad de la amenaza por el impacto, de toda la fila.
- A continuación se presenta la efectividad del control actuante, o sea a qué nivel del riego total se puede mitigar. Por ejemplo, la amenaza de inundación puede ser mitigada ubicando el centro de cómputo en un piso elevado.
- Finalmente, en la última columna, se indica cuál es el riesgo residual, que resulta de aplicar la efectividad del control del riesgo total.

#### 3.7.2.1 La probabilidad de ocurrencia de desastres

Los riesgos considerados para e plan de recuperación de desastres, son aquellos que presentan una probabilidad de ocurrencia no despreciable en función de las características del entorno, como:

- Características meteorológicas o ambientales de la región
- Características generales del edificio y edificios contiuos
- Equipamiento alojado
- Condiciones de acceso

Para obtener la probabilidad de desastres en este caso se construyó la siguiente tabla en base a los eventos registrados durante un año.

| Amenazas | Probabilidad |
|---|---|
| Fallas eléctricas | 30 % |
| Fallas en aire acondicionado | 25 % |
| Accesos no autorizados | 4 % |
| Administración por personal no especializado | 5 % |
| Fallas en hardware | 20 % |
| Fallas en software | 15 % |
| Desastre natural | 1 % |
| TOTAL | 100 % |

Tabla 3.7.2.1 Probabilidad de Riesgos

Consideraremos para esta matriz a los equipos y aplicaciones marcadas como críticos en la Tabla de Equipos (Página 56)

| Amenazas | Probabilidad | Servidores miles $ | Aplicaciones miles $ | Riesgo total miles $ | Efectividad del control | Riesgo Residual miles $ |
|---|---|---|---|---|---|---|
| Fallas eléctricas | 0.25 | $600 | $200 | $200 | 0.95 | $10 |
| Fallas en aire acondicionado | 0.25 | $600 | $200 | $200 | 0.95 | $10 |
| Accesos no autorizados | 0.04 | $300 | $600 | $36 | 0.95 | $2 |
| Administración por personal no especializado | 0.05 | $200 | $600 | $40 | 0.95 | $2 |
| Fallas en hardware | 0.2 | $400 | $200 | $120 | 0.95 | $6 |
| Fallas en software | 0.2 | $200 | $600 | $160 | 0.8 | $32 |
| Derrumbe de instalaciones | 0.01 | $1,600 | $1,600 | $32 | 0.1 | $29 |

Tabla 3.7.2.2 Matriz de Riesgos.

Ver Anexo 1 para la explicación detallada de la tabla

.

### 3.7.3 Controles

Los procedimientos efectuados para lograr asegurar el cumplimiento de los objetivos son definidos como controles.

El ayudar al cumplimiento de las metas indica claramente que estos procedimientos tienen un efecto directo mitigante sobre los riesgos existentes.

Como describimos en el punto anterior estas acciones mitigantes logran actuar sobre el riesgo total reduciendo la exposición al mismo a una medida menor (riesgo residual).

Por lo establecido anteriormente existe una relación biunívoca entre riesgo y control.

Es por ello intentamos cuantificar el riesgo al calcular el Riesgo Total (RT). El valor resultante nos indica cual debería ser el costo asociado al control que actúa sobre ese riesgo para ser eficiente.

El RT calculado para un activo referente a la amenaza: incendio, es de $ 120, por lo tanto los costos anuales asociados al control que debo implantar no deben ser muy superiores a esa cifra, dado que si lo fueran estarían gastando más en la realidad que lo que eventualmente podría perder.

Los distintos procedimientos de controles puede ser agrupado (sobre la base de los objetivos primarios que quieren satisfacer) en tres categorías, aquellos integrantes del sistemas de control interno, aquellos referidos a brindar seguridad y aquellos destinados a brindar calidad de las operaciones.

Estas categorías no son excluyentes, o sea existen procedimientos que se repetirán dentro de las tres categorías.

Como establecíamos anteriormente la agrupación se realiza sobre la base de objetivos de alto nivel que se quiere satisfacer, o sea estos procedimientos buscan que la información que procesan cuente con ciertas características independientemente del objetivo específico por el cual fue creado (que como establecimos lo determinan los riesgos existentes).

De esta manera establecemos para cada grupo los objetivos a cumplir. Esta definición no es arbitraria sino que se basa en los marcos de referencia más recibidos, a saber COSO,ISO, SAC, etc.Esta definición no es arbitraria sino que se basa en los marcos de referencia más recibidos, a saber COSO,ISO, SAC, etc.:

- **Control interno**. Busca asegurar eficiencia y eficacia de las operaciones, cumplimiento de leyes, normas y regulaciones y confiabilidad de la información (básicamente aquella publicable).
- **Seguridad**. Busca asegurar la disponibilidad, confidencialidad e integridad de las operaciones.
- **La gestión de calidad**. Busca asegurar la adecuada calidad, entrega y costo de las operaciones.

El adecuado cumplimiento de los objetivos anteriormente detallados permitirá alcanzar una razonable seguridad en el cumplimiento de los objetivos planteados para los diversos procedimientos de TI.

### 3.8 Posibles Estrategias de Recuperación

Es esta etapa se analizan las distintas alternativas que aporten una solución al problema, teniendo en cuenta todo el análisis anterior.

Las distintas estrategias de recuperación van estar inclinadas a:

1. Recuperación total de los centros de computo
2. Recuperación parcial de los equipos
3. Recuperación individual de los equipos, aplicaciones o servicios.

Las distintas alternativas brindarán la oportunidad de elegir la más conveniente para el negocio.

Para determinar las posibles estrategias de recuperación nos basaremos en los análisis de:

1. Análisis de Impacto*(Tabla de Analisis de Impacto)*
2. Matriz de Riesgo*(Tabla Matriz de Riesgos)*

Del Análisis de Impacto de determino que los sistemas y equipos que representan un impacto Crítico para el negocio son:

| | |
|---|---|
| **Equipos** | Servidores Darecccl1 y Darecccl2 |
| | Red de Almacenamiento (SAN) |
| | Unidad de Procesamiento de almacenamiento (SP) |
| | Unidades de almacenamiento (DAE) |
| | Switches de FC |
| **Aplicaciones** | Sistema SAP ERP Productivo |

Fig. 3.19 Equipos Críticos

Para los cuales no puede presentarse una falla que cause que la disponibilidad de estos servicios sea mayor a 8 hrs.

De la Matriz de Impacto se obtuvo que las amenazas que mayor riesgo residual presentan son:

- Fallas en Software
- Desastre natural (Derrumbe de instalaciones)

Por lo que las posibles estrategias de recuperación estarán encaminadas en proteger la infraestructura que soporta al sistema SAP ERP productivo de posibles fallas de software (aplicación, corrupción de datos) y un desastre natural (derrumbe de instalaciones).

### 3.8.1 Propuesta 1. Replica de Información a una Infraestructura en Espejo en una ubicación alterna.

Este método de Vista es Espejo *(MirrorView)* consiste en tener dos infraestructuras iguales ubicadas en sitios diferentes, con una réplica de información en ambos sistemas. Este esquema nos asegura la protección del sistema y de una falla del site completo.

MirrorView mantiene una copia (imagen) de una LUN (Logical Unit Number) en una ubicación alterna en caso de un desastre. La imagen de producción (espejo 1) es llamado imagen primaria, la copia de la imagen es llamada imagen secundaria. Este método soporta varias imágenes remotas, cada una alojada en un sistema de almacenamiento. La imagen primaria recíbelas peticiones de los equipos de usuarios de I/O (entrada/salida) de datos, la imagen secundaria solo recibe las copias de la imagen principal.

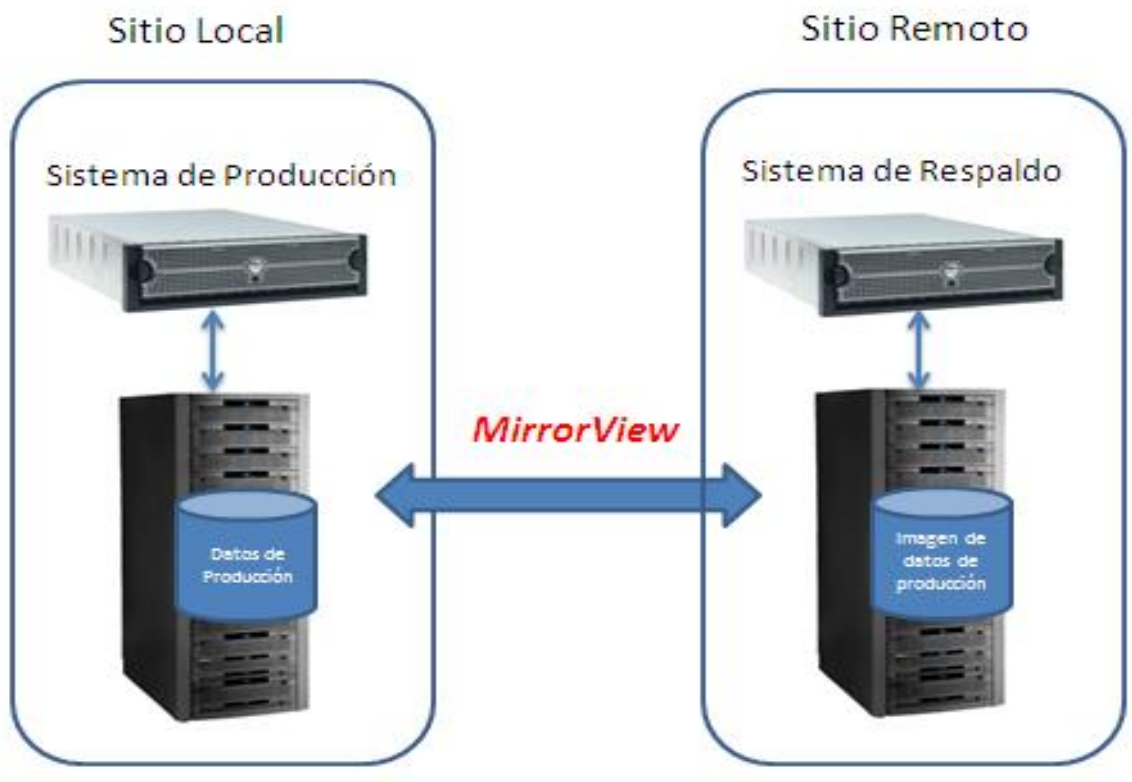


Fig. 3.20 Diagrama del escenario propuesto

Para los equipos y aplicaciones este método es transparente, ya que no saben cuál LUN es un espejo. Este método usa escritura síncrona, lo que significa que lo que se escribe en el sistema primario es reconocido solo después de que el sistema secundario confirma el dato.

Puede ser usado en dos formas, Síncrona y Asíncrona.

**Síncrona**. Mediante una aplicación permite mantener una copia síncrona de la imagen de una LUN en una localidad separada en espera de una recuperación de desastre, si el sistema primario esta inaccesible.

**Asíncrona.** Permite una actualización periódica de la copia de los datos de producción. Por medio de una aplicación mantiene una copia en un "punto del tiempo" y por lo tanto mantiene una copia periódica en una ubicación alterna en espera de una recuperación de desastre.

En la siguiente tabla realizaremos una comparación de ambos modos de replicación.

| Tecnología | Síncrona | Asíncrona |
|---|---|---|
| Metodología de replicación | En línea, provee en tiempo real un espejo de la escritura | Actualización periódica de la escritura |
| Efecto de una interrupción en la comunicación | Mantiene en Logs los intentos de I/O para reanudarlos después de una interrupción | Puntos de revisión, reanudará la réplica desde el último I/O exitoso |
| Impacto en Rendimiento | A mayor demanda mayor es el tiempo de reconocimiento de peticiones de I/O remotos | La demanda no depende de peticiones de I/O remotos |
| Límites de distancia | Para distancias grandes es necesario un enlace dedicado con un alto ancho de banda | Se puede fraccionar el consumo de ancho de banda |
| Copias de Imágenes | Mantiene actualizaciones en línea en una localidad remota | Mantiene una copia de un punto en el tiempo en un sitio remoto |

Tabla 3.8.1 Comparativa de Replicas

### 3.8.2 Propuesta 2. Replica de Información a través de imágenes a una ubicación alterna, con un servidor es espera.

Este método es en esencia un esquema similar a una replicación Asíncrona, pero sin contar con una infraestructura en espejo en una ubicación remota.

Mediante herramientas que permiten obtener Imágenes, que son puntos de control en un tiempo dado, respaldaremos la información de:

- Sistema Operativo
- Sistema
- Datos

Se capture y protege todo el sistema, incluidos el SO, las aplicaciones, todos los archivos, los controladores de dispositivo, etc. en un punto de recuperación fácil de administrar mediante tecnología basada en imágenes.

Permite la recuperación de servidores físicos y virtuales en minutos desde ubicaciones locales o externas, incluso a estado bare-metal, que es una técnica para recuperación de datos que consiste en una especie de "reinstalación" completa del equipo sin necesidad de ningún software previo. Lo que se suele hacer es una vez que el equipo está en perfecto funcionamiento se crea una "imagen" de su contenido, si por alguna razón el equipo falla, se puede volver al estado anterior "volcando" la imagen. Para hacer esto el equipo donde se creó la imagen y al que se vuelca debe tener el mismo hardware y configuración.

También soporta hardware heterogéneo, que es aquel que se encuentra compuesto por hardware con características físicas distintas entre el original y el destino.

Soportando también entornos virtuales y ubicaciones remotas.

La función de creación de imágenes "en caliente" (Hot imaging) se combina con la capacidad de restaurar en plataformas de hardware diferentes sobre la marcha y sobrepasa la barrera de las capas de abstracción de hardware y los controladores de almacenamiento que no son compatibles.

Tendremos también respaldos realzados con agentes que se integran a la Base de Datos, para obtener datos íntegros, permitiendo protección granular de espacios individuales de tablas o la creación de una copia de respaldo completa de las aplicaciones o bases de datos, y la protección de registros de rehacer y archivos de control archivados, sin tener que colocarlos fuera de línea.

Compatible con Recovery Manager (RMAN) de Oracle. Inicie tareas de copia de respaldo o restauración desde el servidor de soportes de BackupExec o desde la consola Oracle RMAN.

Es posible utilizar la transmisión múltiple para mejorar el rendimiento de las operaciones de copia de respaldo y restauración.

Estas imágenes y respaldos son almacenados en medios extraíbles, como cintas de alto desempeño, las cuales serán enviadas bajo una calendarización a un sitio remoto.

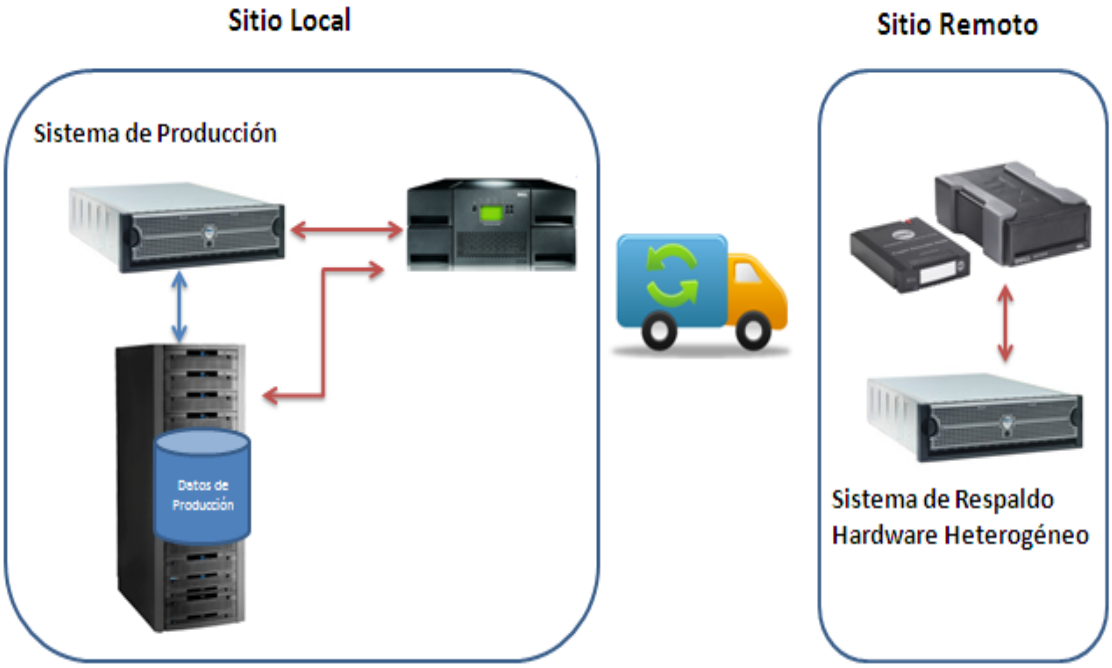


Fig. 3.20 Diagrama descriptivo del escenario propuesto.

### 3.8.3 Comparativa entre ambas estrategias

De las dos posibles estrategias de recuperación realizaremos una tabla comparativa con el fin de analizar las ventajas y desventajas de cada estrategia.

| Característica | MirrorView Síncrono | MirrorView Asíncrono | Imágenes a hardware heterogéneo remoto |
|---|---|---|---|
| Hardware | Espejo del sistema productivo | Espejo del sistema productivo | Hardware Heterogéneo |
| Software | MirrorViewConsole | MirrorViewConsole | Symantec Backup exece<br>System Recovery |
| Método de Replicación | En línea | Actualizaciones periódicas | Envió a cinta y traslado terrestre |
| Medios de comunicación | Enlace dedicado | Enlace dedicado | No necesita |
| Respaldo | En línea | Calendarizado | Calendarizado |
| Recuperación | Casi inmediata | Tiempo de recuperación corto | Tiempo de recuperación mediano |
| Perdida de información | Ninguna | Desde el último punto de respaldo | Desde el último punto de respaldo |
| Costo | Muy alto | Muy alto | Bajo |
| Tiempo de implementación | 3 meses | 3 meses | 1 mes |
| Adecuaciones en site remoto | Si | Si | No |
| Seguridad en replicación | Alta | Alta | Mediana |

Tabla 3.8.3 Comparativa de Estrategias de DRP

Recordando el valor resultante de calcular el Riesgo Total (RT). El valor resultante nos indica cual debería ser el costo asociado al control que actúa sobre ese riesgo para ser eficiente y no invertir más de lo necesario.

Por lo que para el negocio analizando el costo beneficio (el cual fue determinado por la la Dirección General y Dirección de Finanzas) la opción seleccionada fue:

***Replica de Información a través de imágenes a una ubicación alterna, con hardware heterogéneo***

# CAPITULO 4

# ESTRATEGIA DE RECUPERACIÓN

## 4 Descripción de la estrategia

Es esta etapa se describe detalladamente la estrategia seleccionada, especificando las medidas a tomar para la eficaz recuperación del entorno, luego del desastre.

La estrategia seleccionada es una decisión de negocio, influenciada fuertemente por el presupuesto y los límites de tiempo, por lo que puede ser implementado de dos maneras:

1. En etapas, comenzando con servidores, continuando con aplicaciones, luego comunicaciones y por último el centro de datos (Site)
2. En un solo plan completo, en donde abarque todos los bienes, activos físicos y lógicos.

En general, en la descripción de la estrategia se definirán las medidas a tomar para la recuperación del entorno.

Recordemos que este caso de estudio, el alcance es establecer un escenario alterno para el sistema SAP productivo.

## 4.1 Requerimientos para llevar a cabo el Plan

Los requerimientos conforman una guía de las principales características y condiciones que deben cumplir los elementos sobre los cuales se basa el documento, afín de ser utilizados en el procedimiento.

### 4.1.1 Software

Debemos de contar con el software de recuperación en CD, etiquetado como:

i. Symantec Recovery Disk
ii. DELL Drivers for Power Edge
iii. Windows Server 2003 Enterprise Edition

El Software está en resguardo y es provisto por el responsable del software en la empresa.

### 4.1.2 Respaldos de Información

Un punto primordial para el éxito del Plan de Recuperación de Desastres son los respaldos de información.

Estos respaldos están compuestos por:

i. Respaldos de bases de datos del ambiente productivo ECC.
   Full Diario
   Incremental
ii. Imágenes de las unidades del servidor DARECCCL1

- C:
- D:
- L:
- O:
- S:
- T:

Los respaldos se encuentran en la unidad de cintas enviada de Planta, y también están replicados en la unidad G: del servidor en espera.

Estos respaldos son provistos por el responsable de los respaldos de información de la empresa.

### 4.1.3 Hardware

El Hardware necesario para la recuperación es:

i. Servidor en espera, montado sobre el rack de servidores del site alterno, ubicado en las oficinas corporativas.

   Etiquetado como DARDRP

ii. Unidad de cintas, conectada por FC al servidor en espera.

## 4.2 Esquemas y pasos a seguir

La estrategia consiste en restaurar el ambiente de ECC productivo en un servidor alterno ubicado en el site de piso 8 del corporativo México. Consta de las siguientes etapas:

1) Restauración de la imagen del sistema operativo Darecccl1
2) Restauración de los discos locales del servidor Darecccl1
3) Revisión de parametrizaciones de Windows, Oracle y SAP

Recordemos que el escenario original esta compuesto por un Cluster Activo – Pasivo. En donde el nodo activo es el servidor DARECCCL2 y el nodo pasivo es el DARECCCL1

En la pantalla siguiente podemos observar la consola de Administración del Cluster, en donde podemos observar los dos nodos que forman al arreglo de cluster.

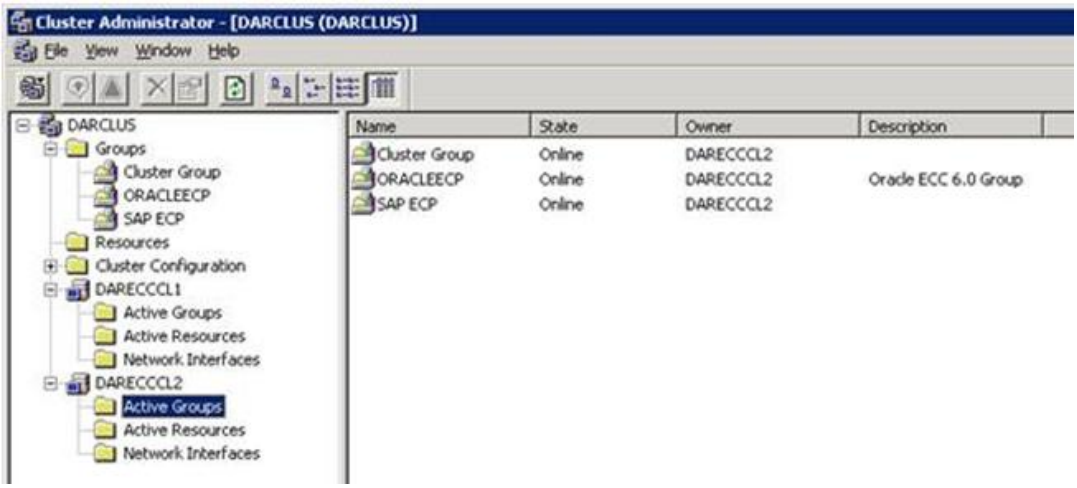


Fig. 4.2.1 Cluster de Windows

En el caso que se presente una falla en el nodo activo, todos los recursos pasaran automáticamente al nodo pasivo.

Podemos observar como todos los recursos están montados sobre el nodo 2. Recordemos que las unidades lógicas están contenidas en la SAN, el cluster lo que indica es donde está la información.

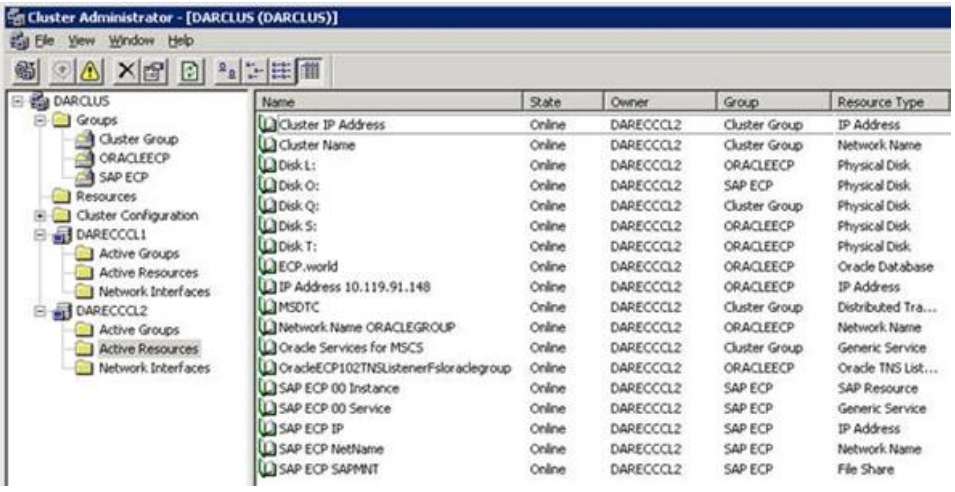


Fig. 4.2.2 Recursos del Cluster

Incluso las conexiones de red son administradas por el nodo activo.

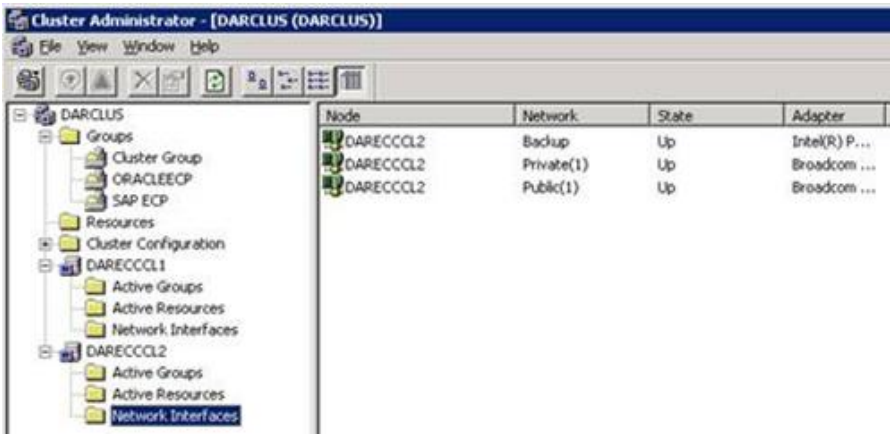


Fig. 4.2.3 Grupos del Cluster

La intención del DRP es prescindir de un cluster, SAN y restaurar la información un servidor con características que soporten la operación temporal del sistema ERP SAP.

Por lo que en el escenario alterno, no contaremos con un cluster y las información estará almacenada en los discos internos del servidor.

### 4.2.1 Etapa 1 Restauración del Sistema Operativo

Una vez que la emergencia es declarada (este proceso de verá a detalle más adelante), el primer paso del Plan de Recuperación de Desastres es restaurar el sistema operativo del servidor de producción de SAP, DAREECCL1.

Primero se obtendrán las imágenes a restaurar. Estas imágenes deben de ser las de la fecha más cercana al desastre. Se encuentran almacenadas en el servidor a restaurar en la ruta G:\Imagenes_DARCLUS

**Paso 1.**

Encender el servidor etiquetado como DARDRP, ubicado en el Site alterno. Insertar el CD de recuperación Symantec Recovery 8.5 y oprimiremos cualquier tecla para inicia desde CD

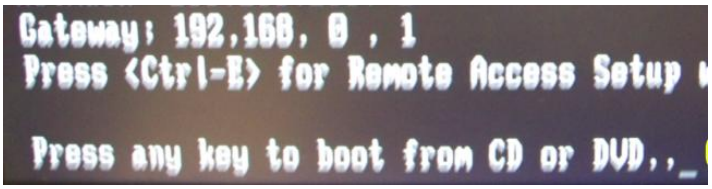


Fig. 4.2.1 Imagen del arranque

Iniciará un sistema operativo virtual para la recuperación de la imagen del sistema operativo.


Fig. 4.2.2 Carga del sistema operativo

Aceptamos los términos de uso

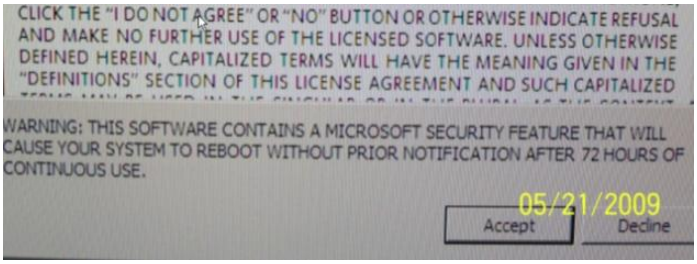


Fig. 4.2.3 Términos de uso

Aparecerá una pantalla para instalar servicios de red, en donde seleccionaremos el botón de ***N0***

Aparecerá la pantalla principal de Symantec Backup Exec System Recovery

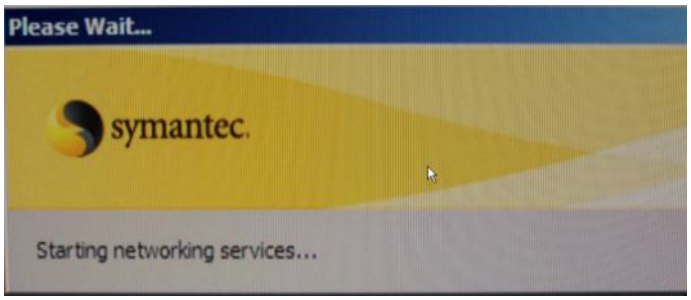


Fig. 4.2.4 Inicio de Aplicación de restauración

**Paso 2.**

Seleccionamos la opción de ***Recover my Computer*** para iniciar con el proceso de recuperación del sistema operativo.

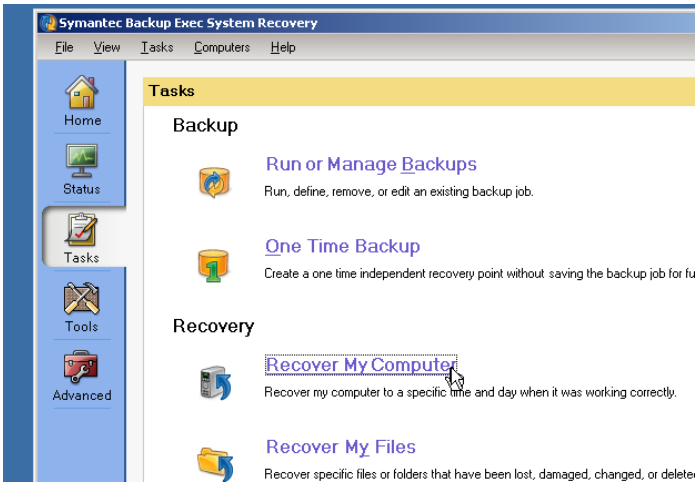


Fig. 4.2.5 inicio de recuperación

Damos clic en el botón de ***Next*** en la siguiente pantalla

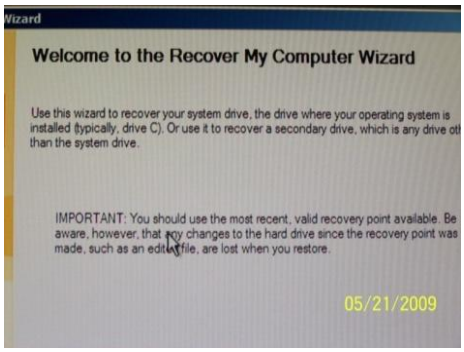


Fig. 4.2.6 Pantalla de inicio

En la pantalla informativa damos un clic en ***OK***

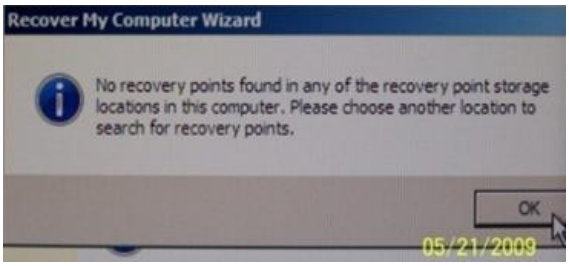


Fig. 4.2.7 Informe de puntos de recuperación

**Paso 3**.

En la siguiente pantalla seleccionaremos la opción de vista de puntos de recuperación por ***Filename*** y damos un clic en ***Browse,*** en donde indicaremos la ruta donde se encuentra la imagen a restaurar.

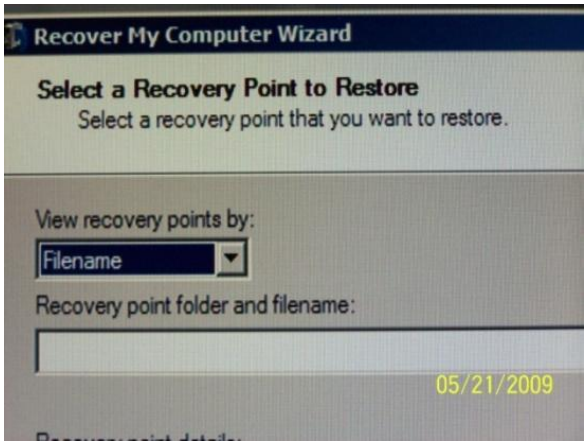


Fig. 4.2 8 Selección de archivo a restaurar

Seleccionamos ***Computer***

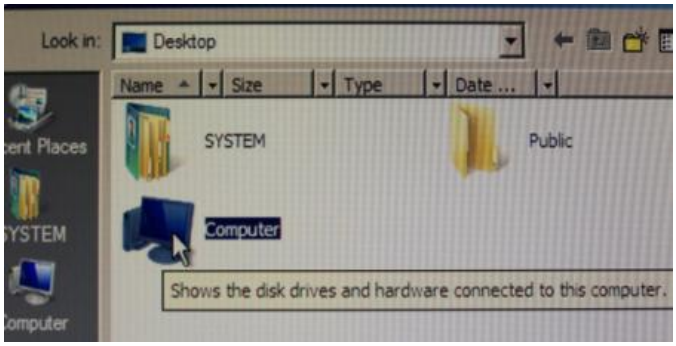


Fig. 4.2.9 Selección de ubicación

Seleccionamos la ***unidad (G:)*** en entramos en la ruta \Imagenes_DARCLUS\ddmmmaaaa y seleccionamos la carpeta más reciente

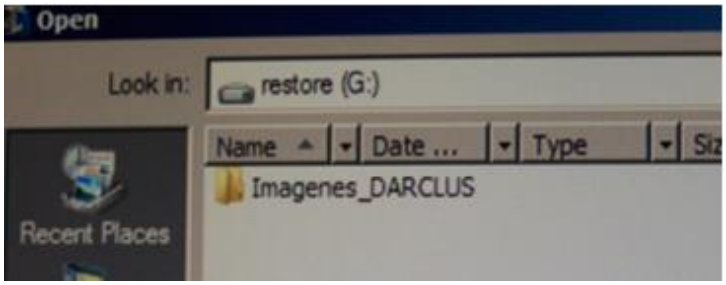


Fig. 4.2.10 Selección de carpeta

Seleccionamos el archivo darecccl1_C_XXXXX.v2i (Donde XXXX puede variar de nombre) y damos un clic en ***Open***

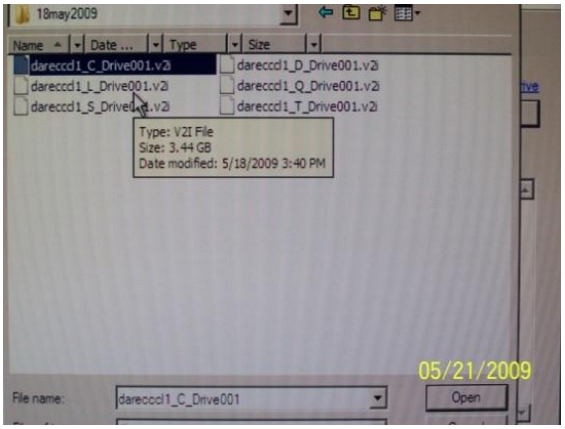


Fig. 4.2.11 Selección de archivo (imagen)

Se desplegara una pantalla con el resumen de la restauración, damos un clic ***Next***

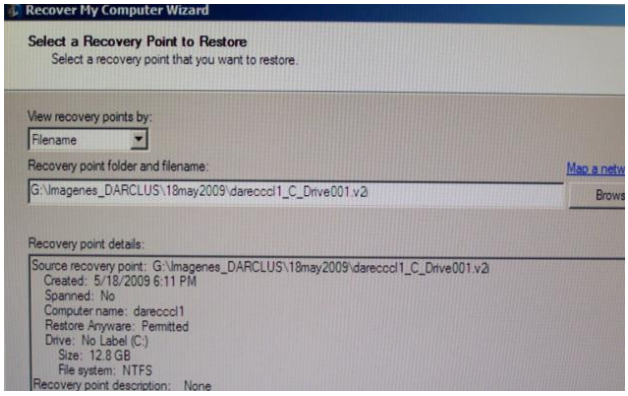


Fig.4.2.12 Pantalla de resumen

**Paso 4.**

En la pantalla de detalle seleccionamos la opción de ***Edit***, con lo que prepararemos los discos y sus particiones para realizar la restauración de las imágenes.

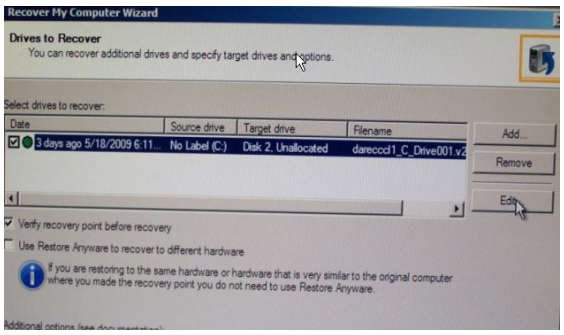


Fig. 4.2.13 Pantalla informativa

Seleccionamos el disk 1 y damos ***Delete Drive*** este procedimiento se deberá realizar con los discos 1 al 5. Con la intención de poder formatear y dejar los discos preparados para las restauraciones.

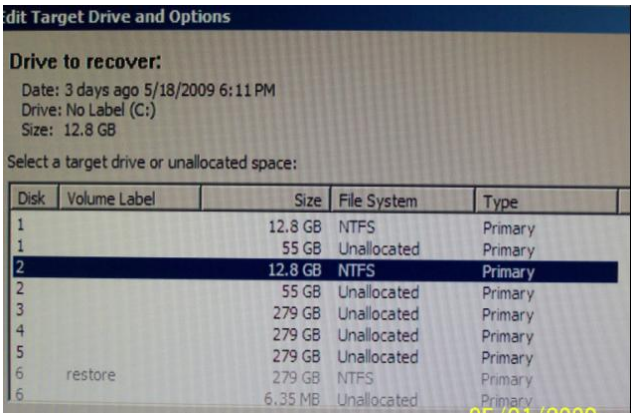


Fig. 4.2.14 Selección de unidad

Deberán de quedar particiones de la siguiente forma

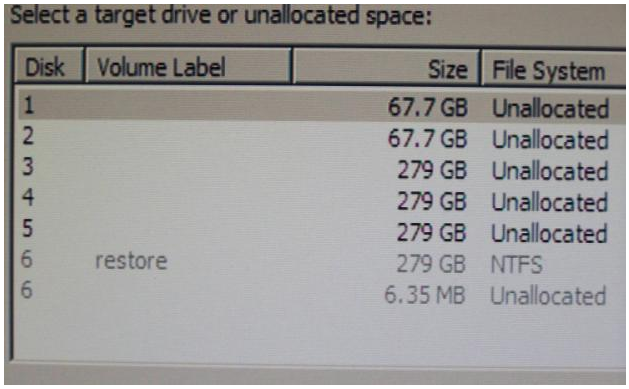


Fig. 4.2.15 Tamaño de unidades

Seleccionamos el disco 1, damos siguiente y seleccionamos las siguientes opciones para crearla partición:

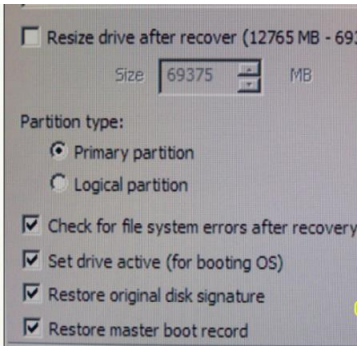


Fig. 4.2.16 Detalles de formateo

Damos un clic en ***OK***

**Paso 5.**

Seleccionamos las opciones y damos un clic en ***Next***, comenzaremos con la restauración del sistema operativo del servidor productivo de SAP

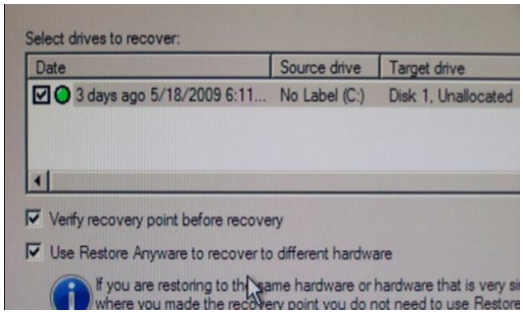


Fig. 4.2.17 Opciones de restauración

En la pantalla de resumen de la restauración habilitamos la opción de reboot when finished y damos un clic en ***Finish***


Fig. 4.2.18 Resumen de parámetros de restauración

Aparecerá una pantalla de advertencia en la cual daremos un clic en ***Yes***

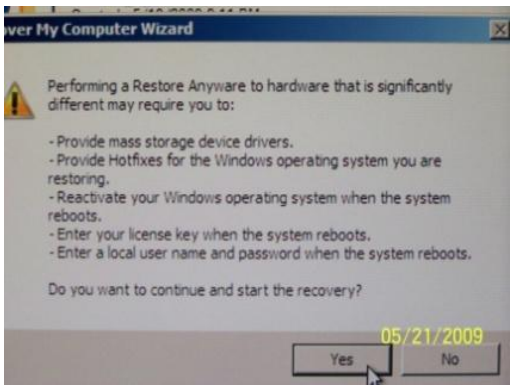


Fig. 4.2.19 Confirmación de restauración

Se reiniciará el servidor y comenzará la configuración del sistema operativo restaurado

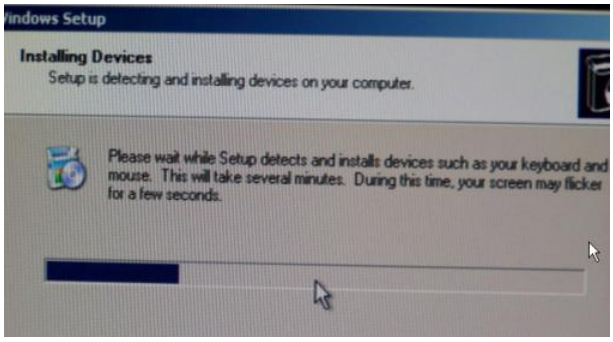


Fig.4.2. 20 Proceso de restauración

Se mostrará la pantalla de configuración de horario de Windows, seleccionaremos el horario de México City y damos un clic en ***Next***

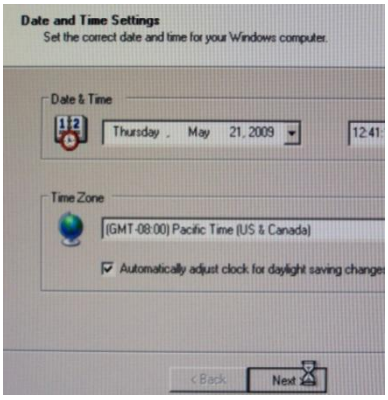


Fig. 4.2.21 Configuración de tiempo

En la pantalla de Workgroup or Computer Domain seleccionaremos la primer opción (Trabajar en workgroup) y damos un clic en ***Next***

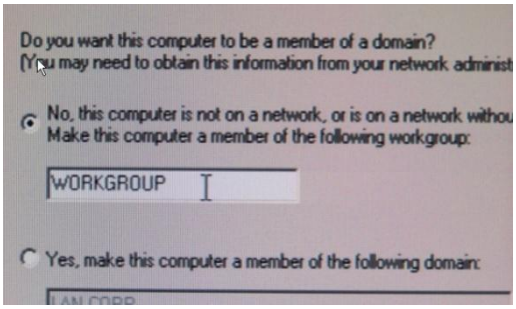


Fig. 4.2.22 Configuración de red

Al final de proceso damos un clic en el botón de ***OK*** y se iniciará el sistema operativo. Aparecerá una pantalla de aviso informando que algunos servicio no se iniciaron, daremos un clic en el botón de ***OK***

Accesaremos el equipo con el usuario de administración local del servidor DARECCCL1


Fig. 4.2. 23 Pantalla de acceso a Windows Server

### 4.2.2 Etapa 2. Configuración de Sistema Operativo restaurado y discos locales

**Paso 1.**

**Configuración del direccionamiento IP y dominio de Windows**

Seleccionamos desde el botón de inicio, Panel de control, Network Connections, ***Local Area Network***

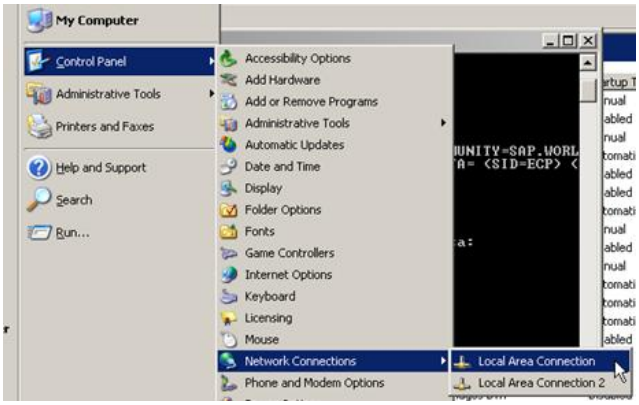


Fig. 4.2.24 Selección de conexión de área local

Damos un clic en el botón de ***Propiedades***

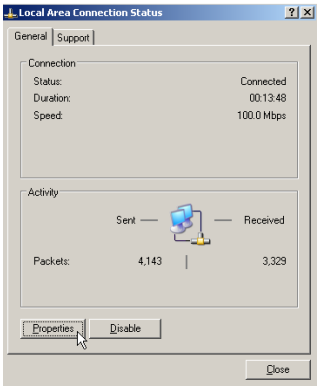


Fig. 4.2.25 Estado de conexión de red

En la pestaña de ***General*** seleccionamos ***Protocolo TCP/IP*** y damos un clic en el botón de ***Propiedades***

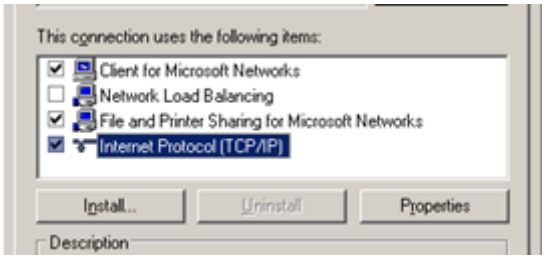


Fig. 4.2.26 Selección de Protocolo

Colocamos el siguiente direccionamiento IP

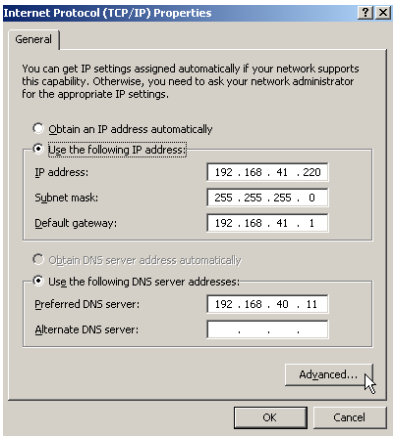


Fig. 4.2.27 Asignación de IP

Damos in clic en el botón de ***Advanced*** y agregaremos tres IP más

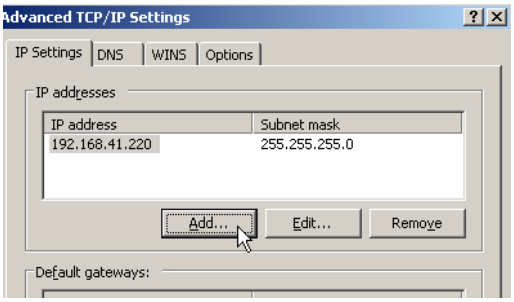


Fig. 4.2.28 Direccionamiento IP adicional

Colocamos el siguiente direccionamiento y damos un clic en ***Add***

IP adress: 192.168.40.221
Subnet mask: 255.255.255.0

IP adress: 192.168.40.210
Subnet mask: 255.255.255.0

IP adress: 192.168.41.221
Subnet mask: 255.255.255.0

Damos un clic en ***OK***, de nuevo damos clic en ***OK***. Cerramos la pantalla con el botón de ***Close***

Por último cambiamos el nombre al equipo, y asignaremos **DARCLUS** que es el nombre que buscan los clientes para la conexión del cliente de SAP.

Esto Debido a que la restauración de la unidad C es el correspondiente a uno de los nodos del Cluster, DARECCCL1

**Paso 2.**

**Restauración de discos locales**

Habilitaremos la unidad lógica donde se encuentran almacenadas las imágenes de los disco locales del servidor darecccl1 para poder realizar la restauración.

Nos vamos a mi PC > botón derecho >***Manage***

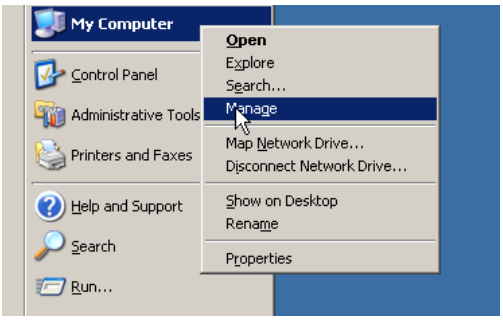


Fig. 4.2.29 Administrar PC

Desplegará la consola de Computer Management, damos un clic en ***Disk Management.*** En el panel de lado inferior derecho buscamos el disco no. 5

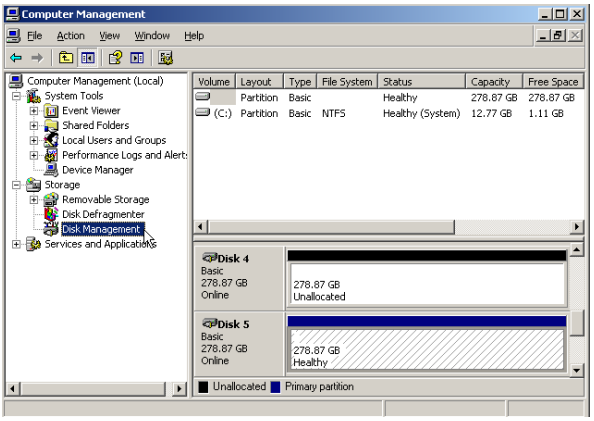


Fig. 4.2.30 Administrador de discos de windows

Damos botón derecho y seleccionamos ***Change Drive Letter and Paths***

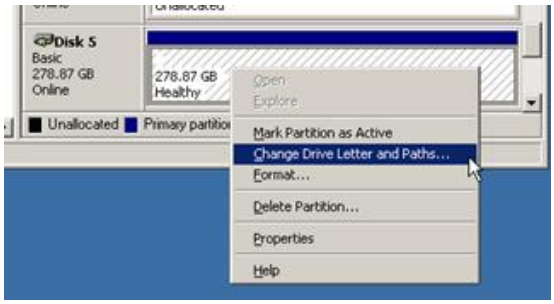


Fig. 4.2.31 Cambio de letra al disco

Seleccionamos el botón de ***Add***y a asignamos la unidad **G**, para finalizar damos un clic en el botón de ***OK***

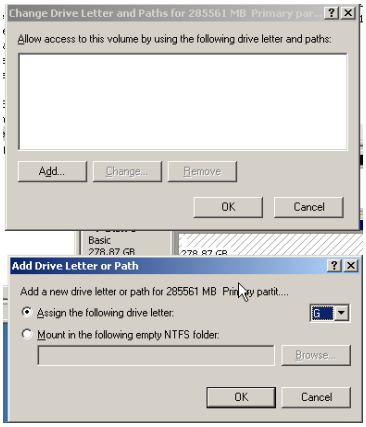


Fig. 4.2.32 Asignación de unidad

Realizamos el mismo procedimiento para la unidad de CD, seleccionamos la unidad asignada al CD, dando un clic con el botón derecho seleccionamos ***Change Drive Letter and Paths***y asignamos la letra **E**

**Paso 3.**

**Recuperación de las unidades almacenadas en la SAN.**

Abrimos la application Backup Exec System Recovery desde el botón de Inicio> All Programs > Symantec > Backup Exec System Recovery

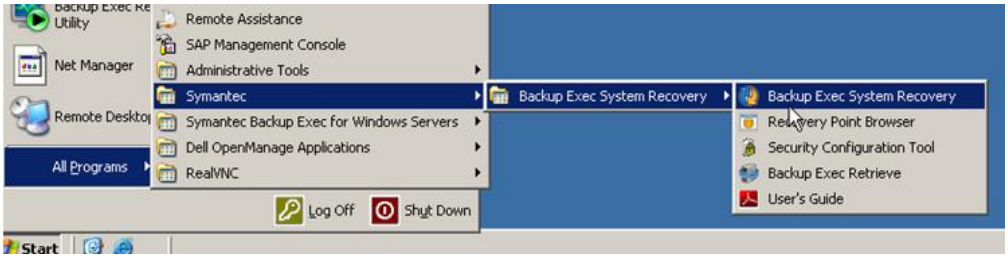


Fig. 4.2.33 Acceso a Backup Exec

Nos mostrará la siguiente pantalla


Fig. 4.2.34 Pantalla de inicio de Backup Exec

Se iniciara la carga de la interface de la aplicación

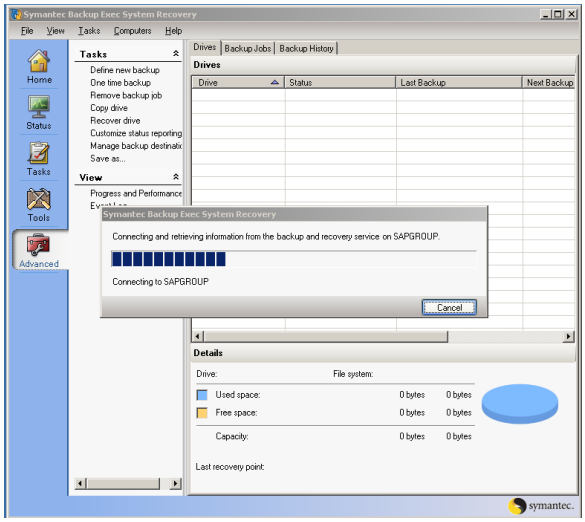


Fig.4.2.35 Carga de la aplicación

Seleccionamos la opción de ***Recover my Computer***


Fig. 4.2.36 Selección de recuperación

Seleccionamos la opción de ***File Name***

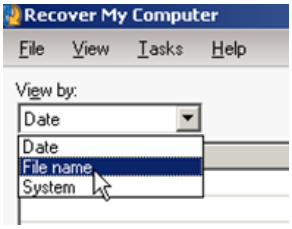


Fig. 4.2.37 Tipo de seleccion

Seleccionamos la ruta donde se encuentra la imagen con el botón de ***Browse***


Fig. 4.2.38 Selección de ubicación del respaldo

Las imágenes de las unidades lógicas estarán en la ruta G:\imagenes_darecccl1\ddmmmaaa y se seleccionará la carpeta con la fecha más reciente. Seleccionamos el archivo que hace referencia a la unidad "**D**" y damos un clic en ***Open***

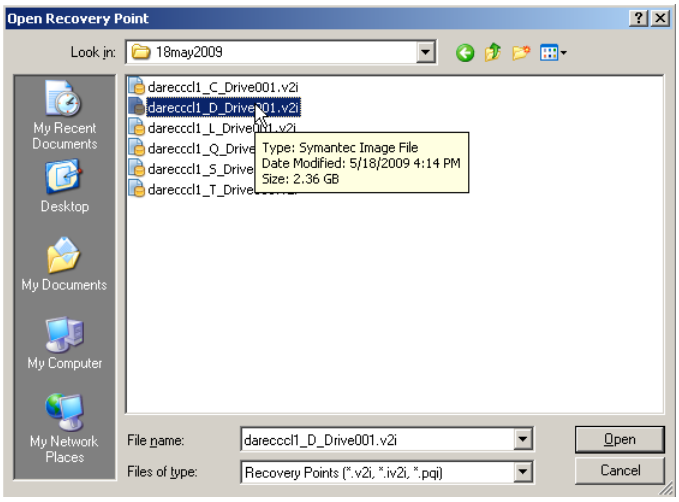


Fig. 4.2.39 Selección de archivo de respaldo

En la pantalla seleccionamos ***Recover Now***

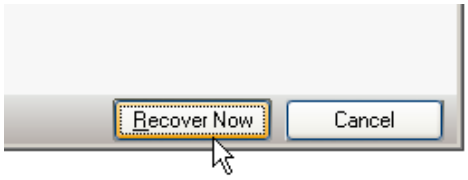


Fig. 4.2.40 Inicio de recuperación

Daremos clic en ***Siguiente*** para iniciar el proceso


Fig. 4.2.41 Pantalla de aviso de recuperación

En la siguiente pantalla nos muestra la ruta del archivo a recuperar, daremos ***Siguiente***

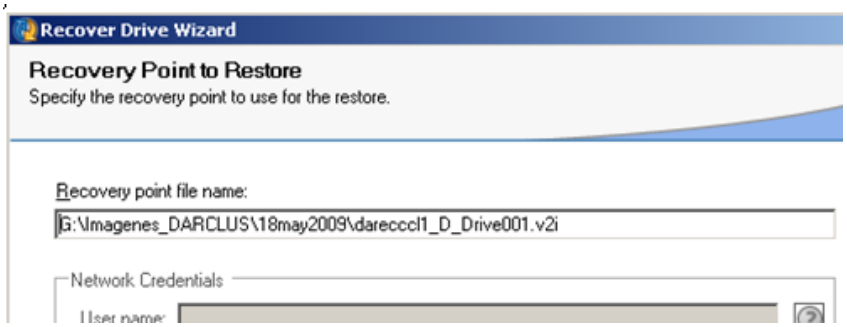


Fig. 4.2.42 Indicador de archivo a restaurar

Seleccionaremos el disco donde restauraremos la imagen, para la unidad ***D*** seleccionaremos el disco ***2***

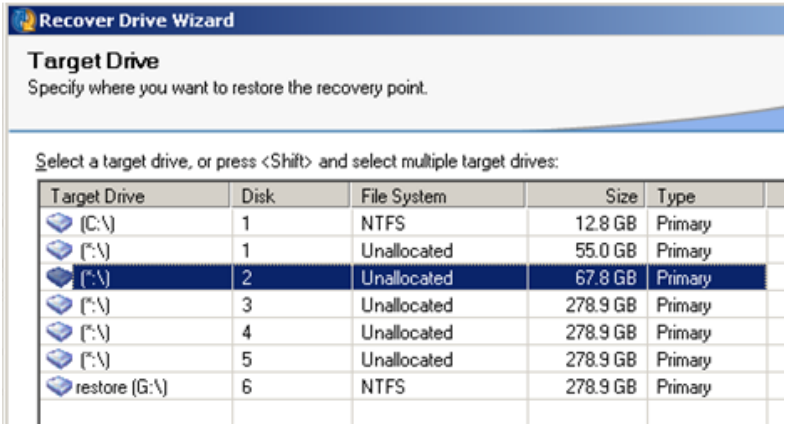


Fig. 4.2.43 Selección de unidad a restaurar

En la opciones seleccionamos ***Verify recovery point before restore***, ***Restore original disk Signature***, en Partitiontype seleccionamos ***Primary Partition*** y en drive letter***D***

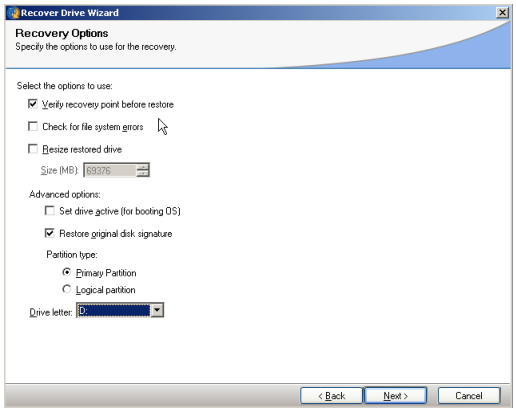


Fig. 4.2.44 Parámetros de restauración

En la pantalla para finalizar la restauración damos un clic en el botón de ***Finish***

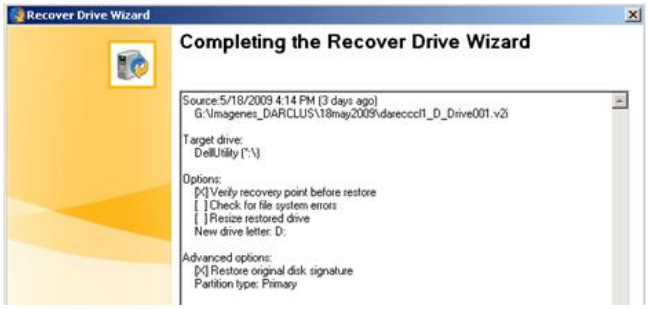


Fig. 4.2.45 Pantalla de confirmación

Comenzará la restauración del **disco local D** el cual tomará varios minutos

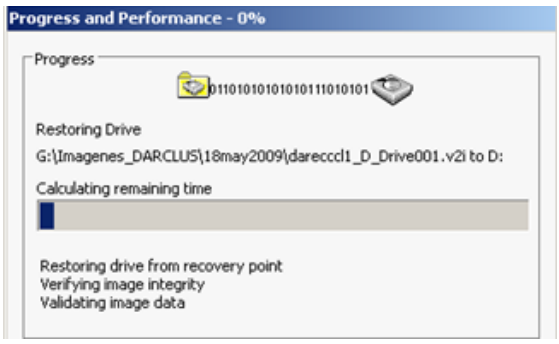


Fig. 4.2.46 Avance de restauración

Al finalizar la restauración se mostrará esta pantalla en la cual daremos un clic en ***Close***

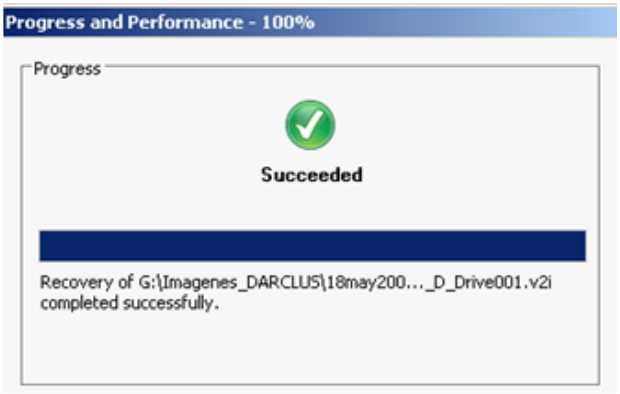


Fig. 4.2.47 Pantalla de finalización

Al dar doble clic en el icono de Mi PC podremos ver que ya existe la unidad restaurada **(D:)** con el nombre de **ORACLE HOME_OFS**

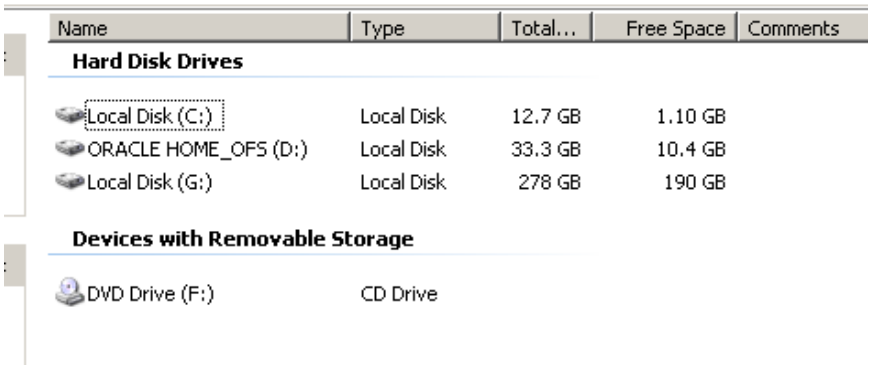


Fig. 4.2.48 Unidad restaurada

Para el resto de las unidades repetimos los pasos anteriores.

Para la unidad ***L*** seleccionaremos el disco ***3***
Podremos ver como al final de la restauración del disco local L aparecerá la unidad **(L:)** con el nombre de **ORIGLOG_ORARCH**

Para la unidad ***S*** seleccionaremos el disco ***5***
Podremos ver como al final de la restauración del disco local S aparecerá la unidad **(S:)** con el nombre de **SAPDATAS**

Para la unidad ***T*** seleccionaremos el disco ***5 que en la columna de target drive aparece como (*.\)***
Podremos ver como al final de la restauración del disco local **T** aparecerá la unidad **(T:)** con el nombre de **MIRROR_BRTOOLS**

Para la unidad ***O*** seleccionaremos el disco ***4***

Podremos ver como al final de la restauración del disco local **O** aparecerá la unidad **(O:)** con el nombre de **USR_SAP**

Quedando al final de la siguiente manera las unidades

| Name | Type | Total... | Free Space | Cor |
|---|---|---|---|---|
| **Hard Disk Drives** | | | | |
| Local Disk (C:) | Local Disk | 12.7 GB | 1.10 GB | |
| ORACLE HOME_OFS (D:) | Local Disk | 33.3 GB | 10.4 GB | |
| Local Disk (G:) | Local Disk | 278 GB | 181 GB | |
| ORIGLOG_ORARCH (L:) | Local Disk | 66.5 GB | 59.6 GB | |
| USR_SAP (O:) | Local Disk | 64.0 GB | 51.6 GB | |
| SAPDATAS (S:) | Local Disk | 199 GB | 95.9 GB | |
| MIRRLOG_BRTOOLS (T:) | Local Disk | 66.5 GB | 64.5 GB | |

Fig. 4.2.49 Unidades restauradas

El **disco local E** no será restaurado mediante imágenes por ser un espacio asignado para memoria virtual y no tener datos, por lo que se creará de la siguiente manera.

Damos un clic con el botón derecho del mouse sobre el icono de **Mi PC** y seleccionamos la opción de ***Manage***

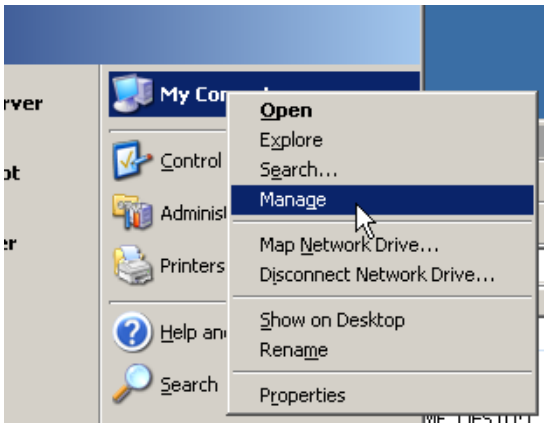


Fig. 4.2.50 Administración de PC

Dentro de la consola de Computer Manager seleccionaremos el area del **DISK 0** que aparece en negro y daremos un clic con el botón derecho seleccionando ***New Partition***

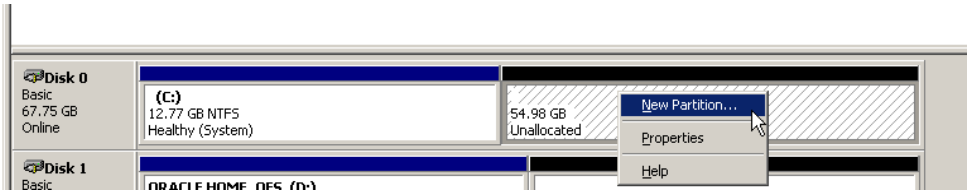


Fig. 4.2.51 Creación de particiones

Daremos clic en el botón de ***Next***


Fig. 4.2.52 Pantalla de inicio de creación de partición

Seleccionaremos la opción de **Primary Partition** y daremos un clic en ***Siguiente***

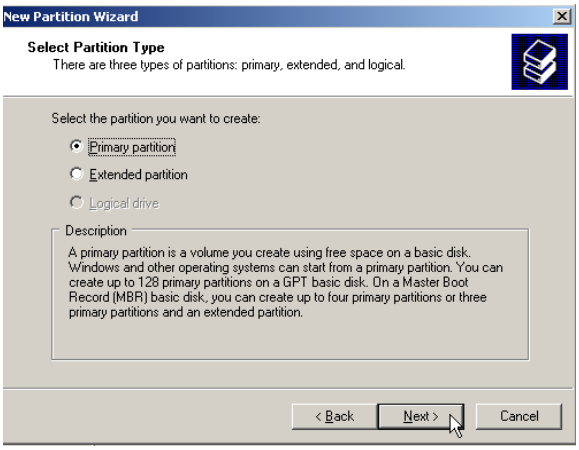


Fig. 4.2.53 Selección de tipo de partición

Establecemos el tamaño de la partición que será de **22092** y damos un clic en el botón de ***Next***

Asignamos la letra **E** y damos ***Next***

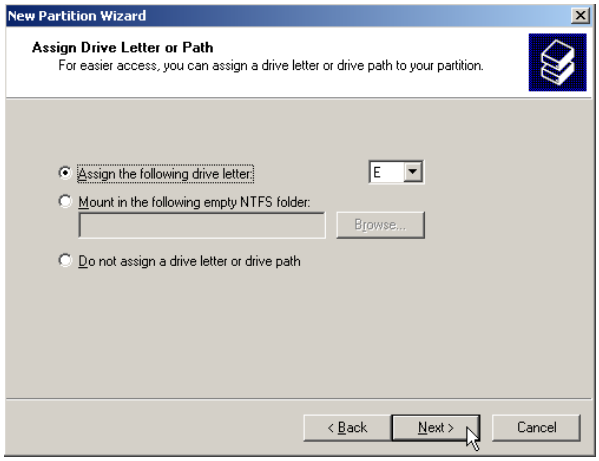


Fig. 4.2.54 Asignación de letra

Formateamos la partición con los siguientes parámetros:

- File system: **NTFS**
- Alocation unit size: **Default**
- Volume label: **Local disk**

Habilitamos la opción de ***Perform a quickformat***y damos un clic en ***Next***

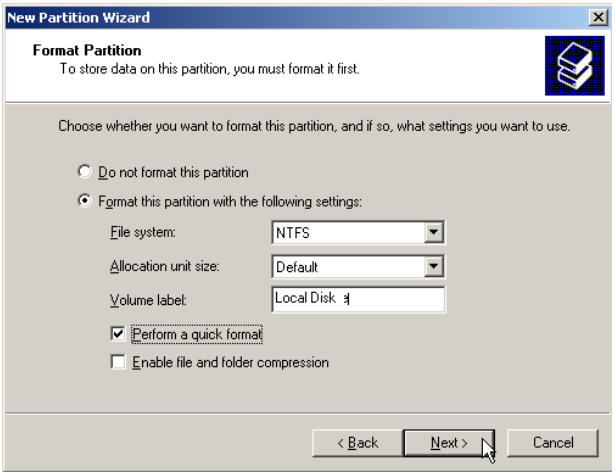


Fig. 4.2.55 Parámetros de partición

La distribución de los discos locales quedará de la siguiente forma y podernos visualizarlo dando un clic con el botón de derecho del mouse sobre ***Mi PC > Administrar > Disk Manager***

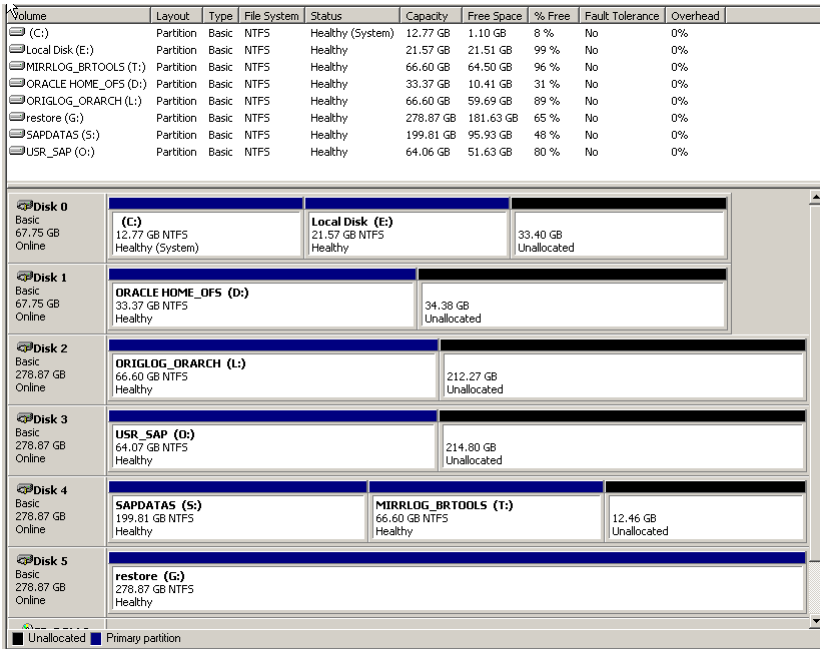


Fig. 4.2.56 Unidades asignadas

En la unidad (G) se crearan dos carpetas para la restauración de la base de datos:

- Data_files
- Redo_logs

### 4.2.3 Etapa 3 Revisión de parametrizacion de Windows, Oracle y SAP

**Paso 1.**

**Parametrizacion de Windows**

Estableceremos la **memoria virtual** necesaria para el funcionamiento de SAP, damos u clic con el botón derecho del mouse sobre el icono de ***Mi PC*** y seleccionamos ***Properties***

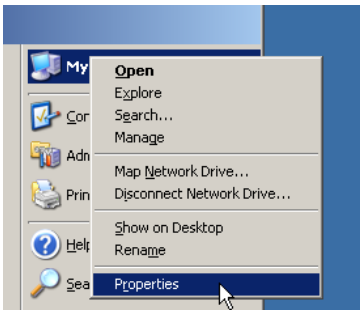


Fig. 4.2.57 Propiedades de Mi PC

En la pantalla de SystemProperties seleccionamos la pestaña de ***Advanced*** y damos un clic en ***Settings***

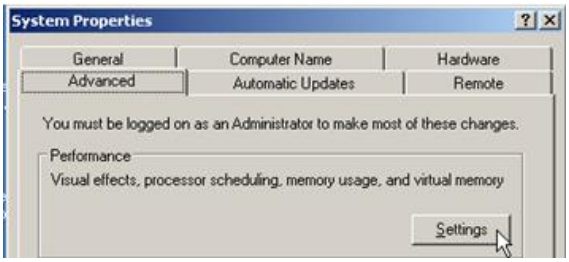


Fig. 4.2.58 Propiedades avazadas

Seleccionamos la pestaña de **Advanced** y damos un clic en ***Change***

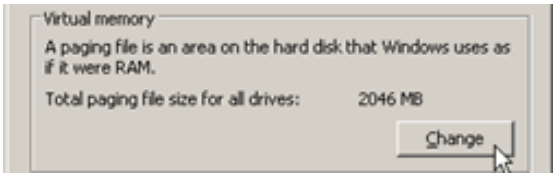


Fig. 4.2.59 Cambio de memoria virtual

Seleccionamos la unidad **D:** y damos un clic en la opción de ***Customsize*** con los siguientes parámetros:

- Initial size (MB) 18762
- Maximum size (MB) 18762

Para la unidad G: y damos un clic en la opción de ***Customsize*** con los siguientes parámetros:

- Initial size (MB) 20480
- Maximum size (MB) 20480

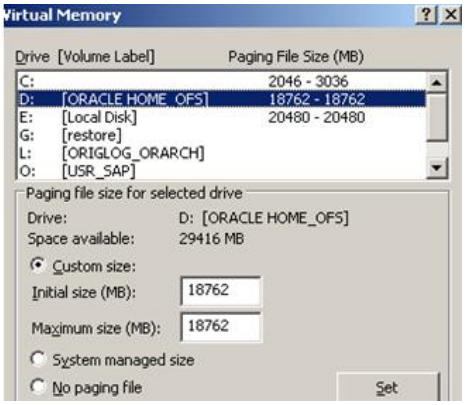


Fig. 4.2.60 Asignación de memoria virtual

Solicitará reiniciar el server para aplicar el cambio damos un clic en el botón de ***Yes***. Con esto terminamos la restauración de las unidades y parametrizacion del servidor.

**Paso 2. Validación de servicios de Oracle**

Antes de iniciar con la restauración de la base de datos de Oracle, cambiaremos el password del usuario de dominio ***ECPADM***, debido a los procesos de restauración empleados por Symantec.

Esto lo realizaremos desde la consola de ***Active Directory User and Computers.*** Localizaremos el usuario de ecpadm y daremos clic con el botón derecho del mouse sobre el usuario y seleccionaremos ***Reset Password***

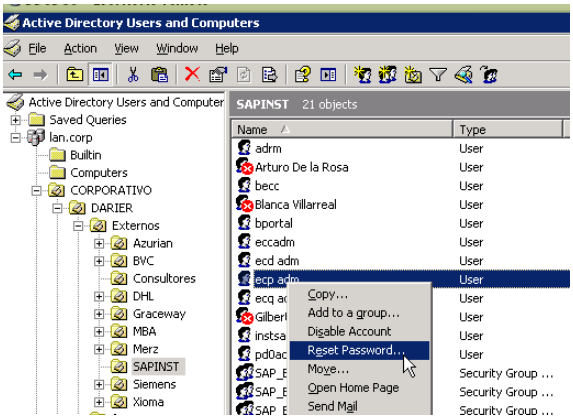


Fig. 4.2.61 Cambio de password

**Paso 3.**

**Cambiar el password a los servicios que utilizan la cuenta corp\ecpadm**

Vamos al botón de Inicio, y del menú desplegado seleccionamos **Services**

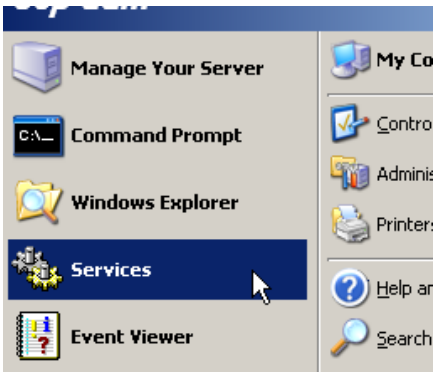


Fig. 4.2.62 Servicios de Windows

En la ventana de servicios, damos clic en el encabezado de la columna **Log on AS,** con esta acción los servicios se ordenaran por la columna **Log on AS** de manera descendente

Damos clic con el botón derecho del mouse sobre el servicio **Oracle MSCS Services**, del submenú desplegado de clic en **Properties**

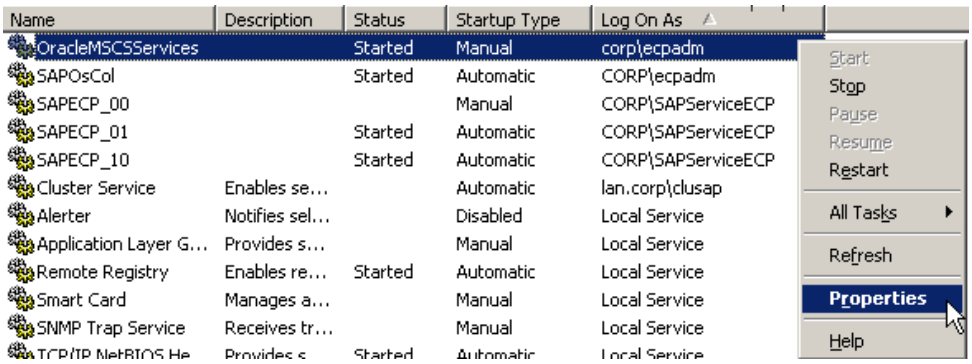


Fig. 4.2.63 Propiedades del servicio

En la ventana de propiedades, de clic en la pestaña **Log On**, después en el cuadro de texto **Password** ingresamos el nuevo password y damos un clic en OK

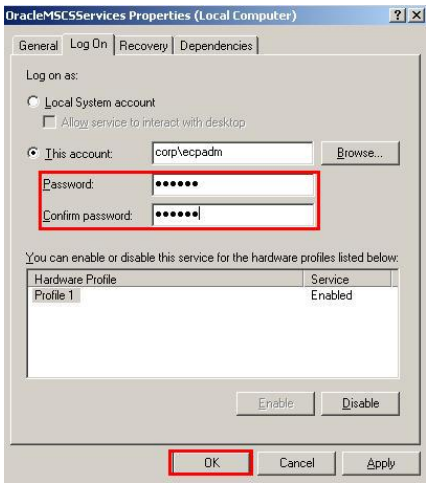


Fig. 4.2.64 Cambio de password en el servicio

Se mostrara el siguiente mensaje, de clic en el botón **OK**

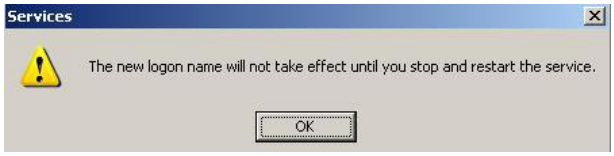


Fig. 4.2.65 Pantalla de notificación

De clic nuevamente con el botón derecho del mouse sobre el servicio **OracleMSCSServices.** Del submenú desplegado de clic en **Stop**

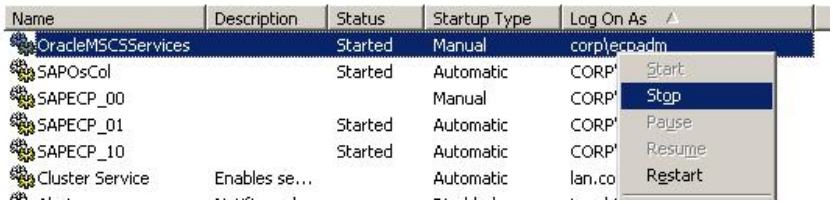


Fig. 4.2.66 Paro de servicio

Cuando termine el proceso de Stop, de clic con el botón derecho del mouse sobre el servicio **OracleMSCSServices,** del submenú desplegado de clic en **Start**

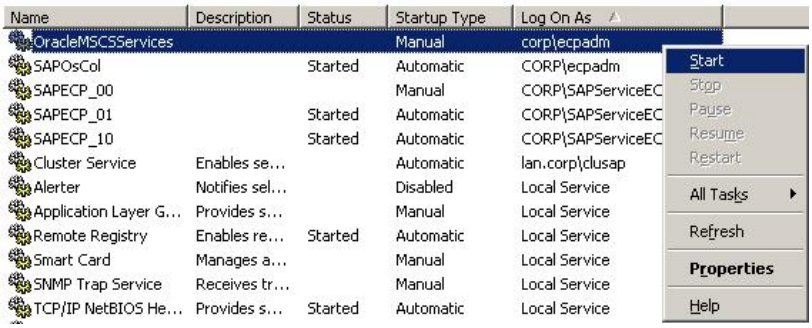


Fig. 4.2.67 inicio de servicio

Realice el mismo procedimiento con el servicio **SAPOscol**

**Paso 4.**

**Iniciar Servicios de Oracle**

Para iniciar los servicios de Oracle realice los siguientes pasos. Abrimos la consola de servicios

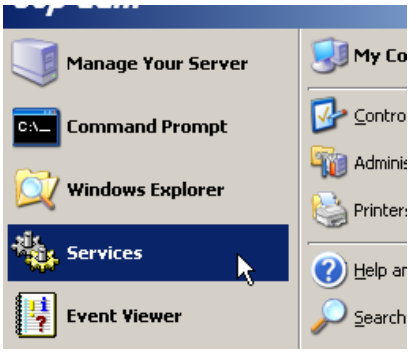


Fig. 12

Una vez desplegada la lista de servicios locales, debemos buscar los tres servicios de Oracle. Seleccione el servicio **OracleECP102TNSListener,** de clic con el botón derecho del mouse, en el submenú que aparece de clic en START

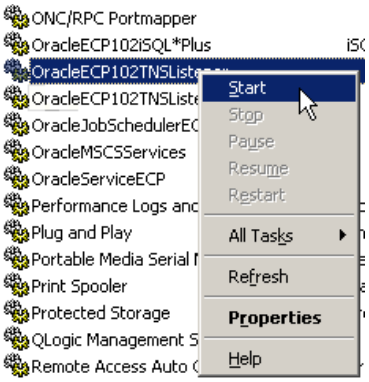


Fig. 4.2.68 Inicio de servicios

Seleccione el servicio **OracleECP102TNSListenerFsloraclegroup,** de clic con el botón derecho del mouse, en el submenú que aparece de clic en START

Seleccione el servicio **OracleServiceECP,** de clic con el botón derecho del mouse, en el submenú que aparece de clic en START

**Paso 5.**

**Verificación de la comunicación con la Base de Datos.**

La prueba de comunicación con la base de datos se realiza desde la línea de comandos. Nos vamos a inicio y damos un clic en CommandPrompt


Fig. 4.2.69 Inicio de símbolo de sistema

Una vez abierta la venta de Prompt ingresar el comando **tnsping ECP** y presione enter


Fig. 4.2.70 Inicio de comando

La comunicación con la base de datos es OK con 30 msec de respuesta

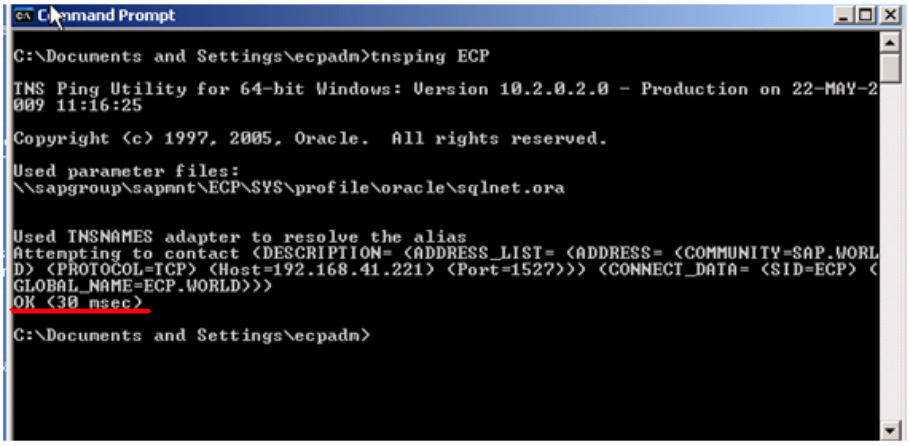


Fig. 4.2.71 Resultado de comando

**Paso 6.**

**Iniciar Oracle**

Para iniciar la base de datos, desde la línea de comando en la que nos encontramos ingresamos la siguiente sentencia **sqlplus / as sysdba** y presione Enter


Fig. 4.2.72 Ejecución de comando

Ingrese el comendo **startup** y presione Enter

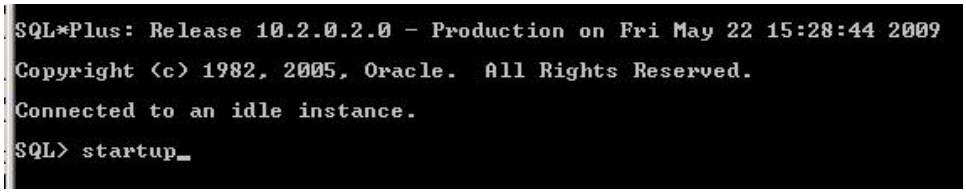


Fig. 4.2.73 Ejecución de comando

Comenzará el proceso de iniciar la instancia, se cargaran las áreas de memoria, los parámetros de inicio, se montara y abrirá la base de datos

**Nota:** Puede ser que oracle llegue a marcar un error, esto es normal y se corregirá con el restore de la base de datos

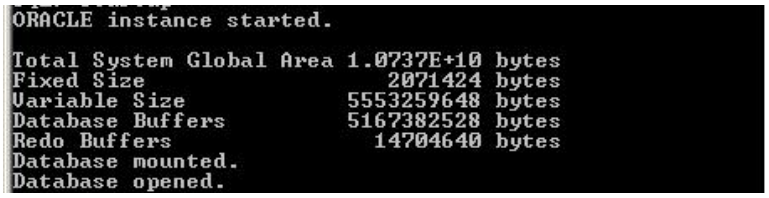


Fig. 4.2.74 Pantalla de notificación

Para salir de oracle ingrese el comando**exit**y presione Enter

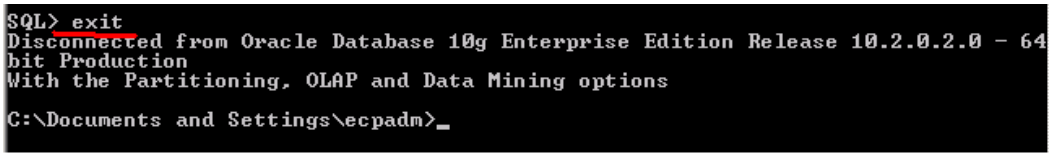


Fig. 4.2.75 Salida de comandos oracle

**Paso 7.**

**Verificar las carpetas compartidas SAPLOC, SAPMNT**

Se debe verificar que las carpetas **SAPLOC** y **SAPMNT** estén compartidas y que cuenten con permisos requeridos

Desde la ventana de comando en la que nos encontramos ingrese el siguiente comando **net sharet** y presione enter

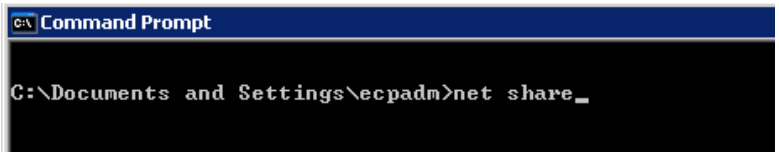


Fig. 4.2.76 Ejecución de comando

Debemos ver las carpetas **SAPLOC** y **SAPMNT** compartidas como se muestra en la imagen

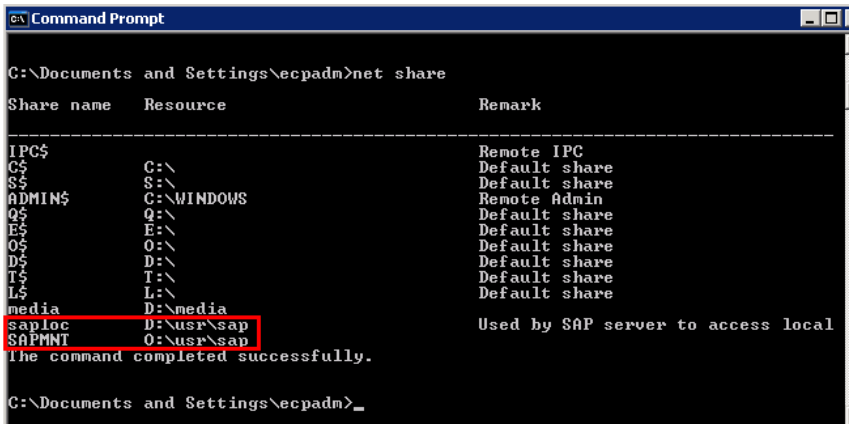


Fig. 4.2.77 Pantalla de verificación

Para ver los permisos debemos ir a la ruta de cada carpeta, navegamos hasta la ruta D:\usr

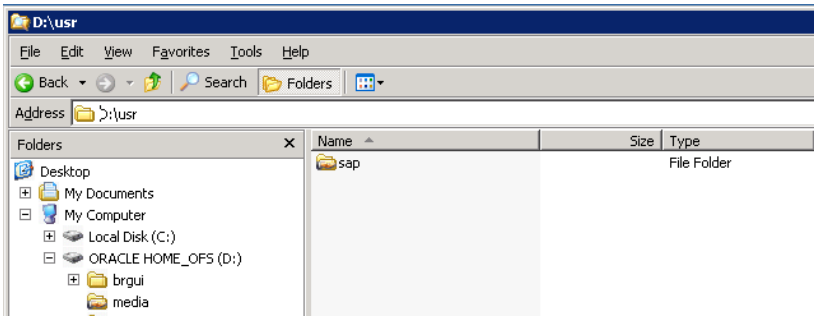


Fig. 4.2.78 Explorador de Windows

Damos un clic con el botón derecho del mouse sobre la carpeta **sap,** del submenú desplegado de clic en **Properties**

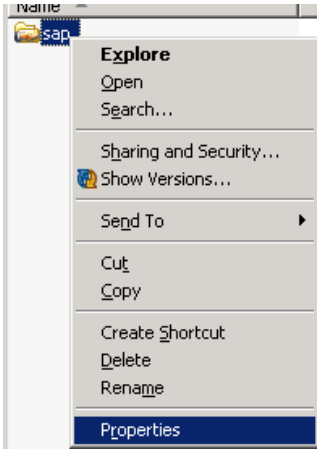


Fig. 4.2.79 Propiedades de carpeta de Windows

Damos un clic en la pestaña **Sharing,** de clic en el botón **Permissions**

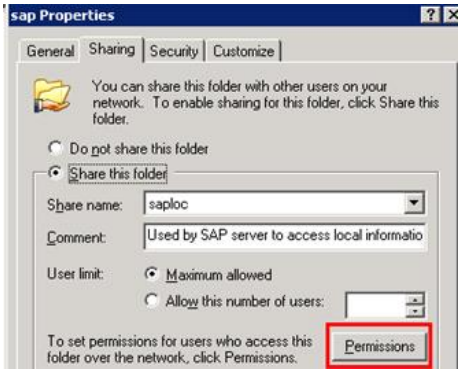


Fig. 4.2.80 Permisos de acceso a carpeta

Debemos ver los usuarios **Administrators(DARECCCL1\Administrators), Everyone,** con privilegios **Full Control,** de clic en el botón **OK**

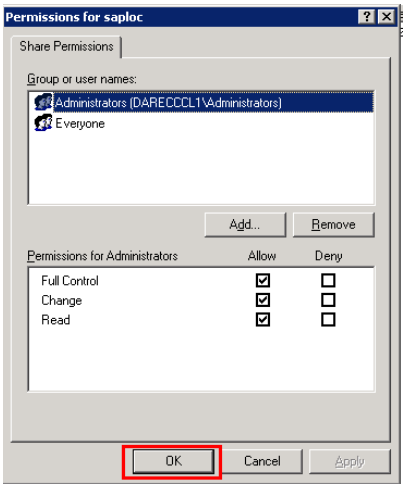


Fig. 4.2.81 Asignación de permisos

Realizamos los mismos pasos con la carpeta compartida **SAPMNT** ubicada en O:\usr

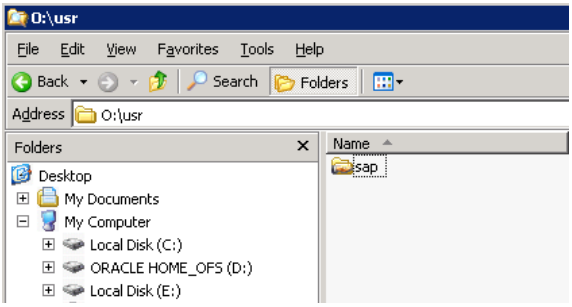


Fig. 4.2.82 Explorador de Windows

Hasta este punto tenemos restaurado:

1. Sistema Operativo
2. Configuración de Unidades
3. SAP
4. Oracle

Con esto es posible pedirle al equipo de validaciones que realice las pruebas de funcionamiento, ya que es posible terminar el Plan de Recuperación de Desastres en este punto.

Si fuera necesario restaurar la base de datos por alguna corrupción, procederemos con la siguiente etapa. **Ver Anexo 2.**

En caso contrario se daría por finalizado la recuperación del sistema SAP productivo en un servidor alterno heterogéneo.

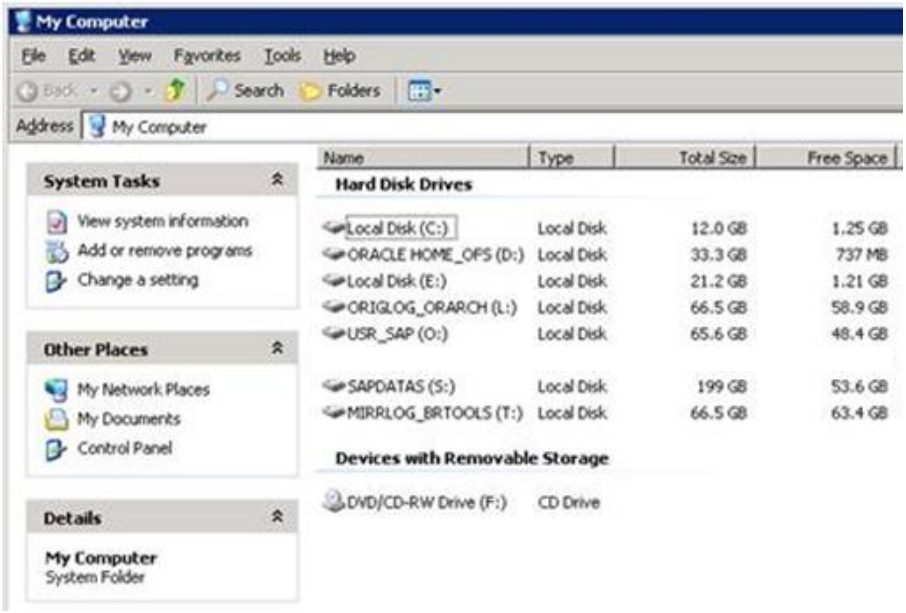


Fig. 4.2.83 Imagen de unidades restauradas

La descripción de cada unidad se muestra a continuación.

***Esquema de disco***

**DARECCL1 Unidades Locales**

| Unidad | Tamaño | Propósito |
|---|---|---|
| C:\ | 12.7GB | Sistema Operativo<br>Page File |
| D:\ | 33.3 GB | \oracle\ECP\102, binarios de Oracle 10g así como OFS (FailSafe)<br>\usr\sap, binarios de SAP de instancias PAS, AAS<br>Page File |
| E:\ | 20.5 GB | Page File |

**DARECCL2 Unidades Locales**

| Unidad | Tamaño | Propósito |
|---|---|---|
| C:\ | 12.7GB | Sistema Operativo<br>Page File |
| D:\ | 33.3 GB | \oracle\ECP\102, binarios de Oracle 10g así como OFS (FailSafe)<br>\usr\sap, binarios de SAP de instancias PAS, AAS<br>Page File |
| E:\ | 20.5 GB | Page File |

**Unidades Compartidas**

| Unidad | Tamaño | Propósito |
|---|---|---|
| L:\ | 66.5 GB | Oracle, origlogs y saparch ( online redo logs y archive logs ) |
| S:\ | 199 GB | Oracle, sapdatas ( datafiles ) |
| T:\ | 65.5 GB | Oracle, mirrlogs y logs de brtools |
| O:\ | 65.5 GB | SAP, binarios y configuración de los servicios centrales |

Fig. 4.2.84 Descripción de unidades restauradas

## 4.3 Pruebas de Funcionalidad

Una vez finalizado el proceso de restauración del sistema SAP en un hardware heterogéneo en una ubicación alterna, el equipo de recuperación estratégica y coordinación (EDEC) realizará las siguientes pruebas.

1. Acceso a SAP mediante el cliente


Fig 4.3.1 Acceso a SAP

2. Generación de transacciones en SAP

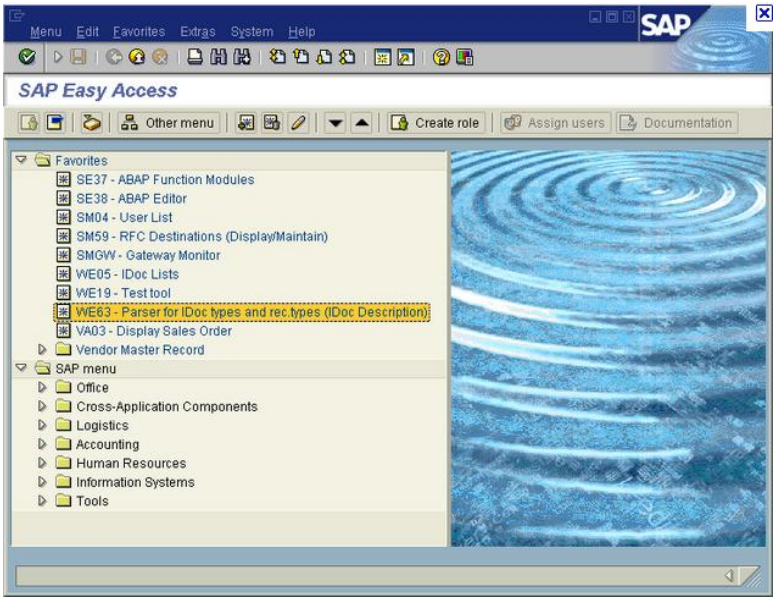


Fig. 4.3.2 Pantalla de inicio del sistema SAP

AL01 SAP Alert Monitor

AL02 Database alert monitor

AL03 Operating system alert monitor

3. Una vez validados los accesos, se pedirá a los KEY USER de cada modulo revisar sus transacciones y validar que la información se encuentre a la fecha y hora que se realizo la transacción

Con estas validaciones podemos dar por finalizado el Plan de Recuperación de Desastres

## 4.4 Formación del Equipo de Recuperación.

La formación del equipo de recuperación tiene como fin determinar y asignar distintas responsabilidades para lograr una exitosa recuperación del entorno ante una emergencia, según el Plan de Recuperación de Desastres Establecido.

### 4.4.1 Roles y Responsabilidades

El equipo de recuperación tiene las siguientes responsabilidades:

i. Definir las medidas preventivas necesarias y factibles de aplicar, a fin de disminuir la probabilidad de ocurrencia de desastres.
ii. Definir, probar, ajustar y mantener actualizado e Plan de Recuperación de Desastres.
iii. Ante un desastre:
    a. Recuperar las prestaciones en el menor tiempo posible y dentro de los plazos máximos establecidos.
    b. Restablecer las condiciones normales que se presentaban antes del desastre
    c. Analizar las causas del desastre y la forma en que se ha producido a fin de emitir un informe y modificar las medidas preventivas y plan de recuperación en función de las conclusiones.

A su vez, el equipo de recuperación está compuesto por sube quipos con distintas obligaciones.

Estos equipos son:

1. **Equipo de dirección estratégica y coordinación (EDEC),** sus responsabilidades son:
    - Dirigir y coordinar las actividades del resto de los equipos que conforman el equipo de recuperación.
    - Realizar las declaraciones de los distintos estados, emergencia, contingencia y restablecimiento
    - Determinar el nivel de desastre producido por una contingencia: total o mayor, parcial, menor.
    - Elaborar los planes de recuperación.
    - Controlar la ejecución de los planes, detectar desvíos y realizar los ajustes de los planes en función a los inconvenientes, problemas y errores hallados durante la aplicación de los mismos.
2. **Equipo de recuperación de hardware (ERH),** sus responsabilidades son:
    - Identificar los elementos del hardware que hayan sido dañados por una contingencia
    - Coordinar con los proveedores de hardware el cumplimiento de los contratos de mantenimiento, garantías y niveles de soporte.
    - Participar en las instalaciones de sistemas operativos que realizan los proveedores
    - Verificar el correcto funcionamiento de los elementos de hardware que hayan sido restaurados o remplazados por proveedores.
3. **Equipo de recuperación de software (ERS)**, las responsabilidades son:
    - Identificar servicios, procesos, bases de datos y aplicaciones que hayan sido afectados por una contingencia.
    - Instalar, configurar y ajustar todo el hardware que haya sido afectado por una contingencia.

4. **Equipo de recuperación de infraestructura (ERC)**, las responsabilidades son:
    - Identificar los elementos de comunicaciones y centros de cómputo que hayan sido afectados por la contingencia.
    - Proveer los respaldos de información necesarios para su uso.
    - Proveer el software necesario para la restauración
5. **Equipo de comunicación a usuarios (ECU)**, las responsabilidades son:
    - Participar en la generación de las comunicaciones oficiales a usuarios ante contingencias, recuperación de prestaciones, demoras incurridas que invaliden o modifiquen lo comunicado anteriormente y el restablecimiento de las condiciones normales.
    - Realizar las comunicaciones a los usuarios internos.

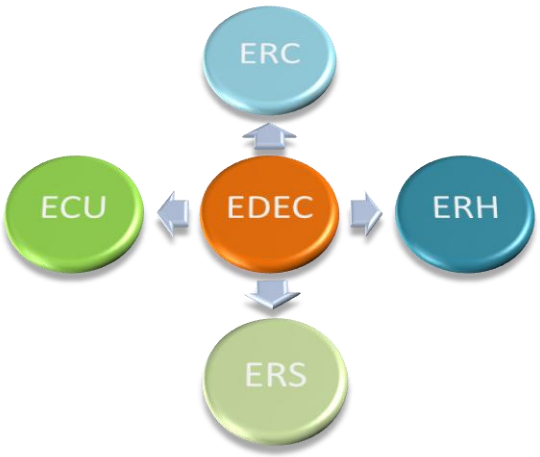


Fig. 4.4.1 Diagrama de Roles

### 4.4.2 Asignación de Roles.

Luego de determinar las características de los equipos de recuperación, se debe designar recursos humanos para cubrir los roles, teniendo en cuenta que una persona no puede formar parte de más de dos equipos.

Para nuestro plan, quedo designado de la siguiente manera:

**EDEC** Jefe de Redes y Comunicaciones

**ERH** Administrador de Redes

**ERS** Administrador SAP

**ERC** Administrador de Comunicaciones

**ECU** Coordinador de Help Desk

# 5. CONCLUSIONES

Teniendo en cuenta la explosión de datos que están experimentando las empresas y la ciega confianza que ponen en sus sistemas de TI a la hora de generar ingresos, cualquier tipo de interrupción implica repercusiones graves, tanto materiales como intangibles.
Los sistemas de Tecnología de la Información (TI) que gestionan el abastecimiento de información empresarial aportan un valor extraordinario pero implican también una vulnerabilidad: si se produce una interrupción en el acceso a los datos cruciales, la empresa sufrirá las consecuencias.

No es difícil imaginar las situaciones que podrían paralizar la estructura informática de una empresa. Ya sea como consecuencia de un fallo en la red de alimentación, una inundación o cualquier otra catástrofe natural, las empresas de todo el mundo cuentan con ejemplos muy recientes que confirman la importancia de una planificación ante desastres. Por muy inverosímil que pueda parecer, hoy en día todas las empresas deben tener presente la probabilidad de un fallo total de sus sistemas de TI en un futuro.

La anticipación de estos sucesos y la planificación de los procesos necesarios para contrarrestar su impacto es hoy en día un requisito imprescindible para el éxito de una empresa.
La preparación de una estrategia de cara a lo inesperado es de lo que se ocupa la planificación de la continuidad de los negocios (Business Continuity Planning, BCP). Una de las subáreas de BCP comprende las medidas preventivas adoptadas por un grupo de TI para garantizar el acceso permanente a los recursos de información, lo que se denomina planificación de recuperación de desastres (Disaster Recovery Planing, DRP)

Las estrategias aplicadas para la protección de datos contra la pérdida como consecuencia de un desastre deben reflejar las prioridades de la empresa. Gastar un millón de pesos en asegurar una recuperación rápida de un servidor de archivos o de impresión puede ser excesivo, pero la inversión de esta misma cantidad de dinero para salvaguardar una aplicación crítica que genera ingresos puede ser justificable.

Pensar en replicación de información en línea en un sitio remoto, estaba fuera de los limites económicos permitidos.

En nuestro caso de estudio, el objetivo planteado por la dirección corporativa, fue asegurar la disponibilidad de la aplicación más importante dentro del negocio con el mínimo de inversión económica posible.

Con la ayuda de software para la creación de imágenes fue posible recuperar el 100% de funcionalidad del sistema SAP Productivo, en un tiempo de 4 hrs. Esta restauración recordemos que fue realizada sobre un hardware heterogéneo, es decir en un hardware de diferentes características que el equipo original.

Con esto se logro cumplir con la recuperación del sistema en un sitio alterno dentro de los parámetros establecidos, y sobre todo con un mínimo de inversión para la ejecución del plan.

Con esta implementación se cubrió con uno de los puntos claves para lograr la validación por SAP de una infraestructura segura.

La importancia de tener un procedimiento escrito, con responsables y con el conocimiento de cómo actuar en caso de una contingencia es parte fundamental de los procesos de un área de tecnología.

Se pudo demostrar que para los tiempos establecidos de recuperación ante una contingencia, la inversión empleada fue de muy bajo costo, y ejecutada con recursos humanos internos.

Y se cumplió con un requisito para poder comenzar con la certificación de Sarbanes Oxley.

# 6. ANEXOS

## 6.1. Anexo 1

La tabla de Matriz de Riesgos fue creada en base a estimaciones en el impacto económico que representaría cada posible amenaza, considerado la mayor afectación posible.

Esta aproximación fue realizada por el Departamento de Administración y Finanzas de la empresa.

Los montos calculados en miles de pesos (miles $) en servidores y aplicaciones no fueron estimados por el área de IT. Solo se proporcionaron los montos de facturas de los equipos involucrados y las horas/hombre estimadas para realizar la recuperación de cada falla.

Se consideró tanto personal interno como personal de consultoras de SAP, para los casos donde involucra una reconfiguración de algún hardware, aplicación o servicio.

El riesgo total fue calculado de la siguiente manera:

Tomaremos como ejemplo de Amenaza: ***Fallas en aire acondicionado***

La probabilidad de ocurrencia se determinó del análisis de un año en incidencias reportadas, de las cuales un 25% se asociaban a fallas en aire acondicionado.

El riesgo total resulta de:

RT= Probabilidad * (Riesgos en servidores ($) + Riesgo en aplicaciones ($))

RT= .25 * ($600 + $200)

RT= 0.25* ($800)

***RT= $ 200***

La efectividad del control se determina después de los controles implementados para cada amenaza, este control en base a porcentaje de efectividad.

Para la mitigación de amenazas, se tomaron las siguientes acciones:

i. Se implementó un segundo sistema de enfriamiento del site de computo
ii. Se implementó un esquema de manteniendo preventivo anual.
iii. Se configuraron monitores de temperatura conectados a la red IP

iv. Se establecieron notificaciones vía email en los equipos que cuentan con sensores internos de temperatura

Por lo que después de los controles implementados la efectividad del control es de .95

El resultado final es:

Riesgo Residual = RT* Efectividad del control (porcentaje no protegido)

Es decir si la efectividad de nuestro control es del .95, el porcentaje no cubierto es de .05

Aplicando al formula

RR= $200 * .05

RR= $10 (en miles de pesos)

## 6.2 Anexo 2

### Restauración de la Base de Datos de Oracle

### Paso 1. Modo NOMOUNT con rman

Este procedimiento fue establecido por el fabricante de la herramienta (Symantec), el cual fue seguido en su totalidad para la ejecución de la restauración.

Antes de realizar el proceso de recuperación de la información debemos poner la Base de Datos en estado nomount y establecer el DBID (ID de la base de datos). Desde la línea de comando en la que nos encontramos ingrese **rman** y presione Enter

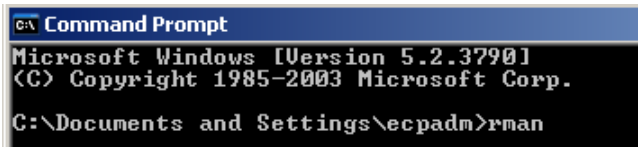


Fig. 6.2.1 Ejecución de comando

Escribimos **connect target sys/oracle@ECP** y presionamos Enter

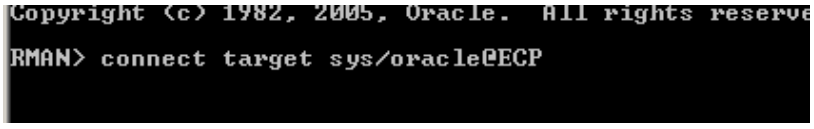


Fig. 6.2.2 Ejecución de comando

Una vez conectado, ingrese el comando **shutdown abort** y presione Enter

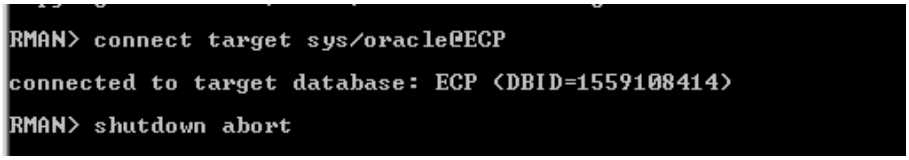


Fig. 6.2.3 Ejecución de comando

Escriba **startup nomount**y presione Enter

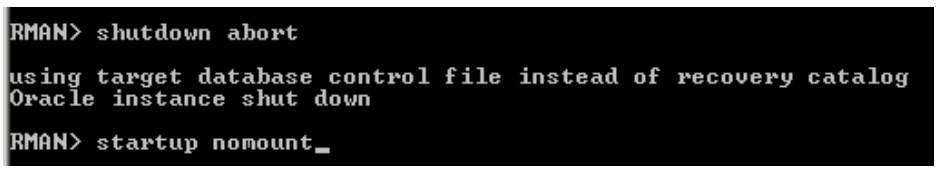


Fig. 6.2.4 Inicio de modo

Cuando rman termine de poner la base de datos en estado **nomount** establezca el IDBD con el siguiente comando: **set dbid 1559108414**

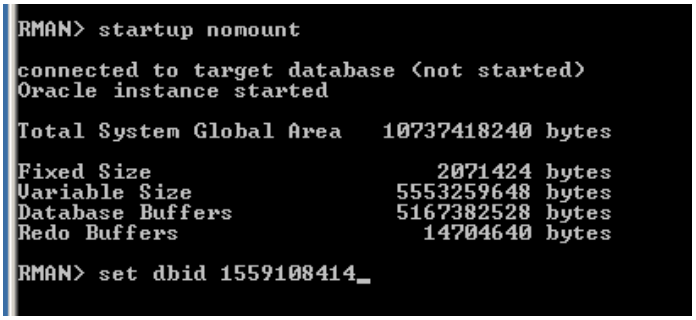


Fig. 6.2.5 Ejecución de comando

Escriba **exit** y presione la tecla Enter para salir de rman

**Paso 2.**

**Restauración de la Base de Datos**

Desde la consola de administracion de Respaldos (DD9STORAGEMX) entramos a la herrameinta de ***Backup Exec 12.5 for Windows Server***


Fig. 6.2.6 inicio de Herramienta de recuperación para base de datos Oracle

Se desplegará la pantalla del sistema

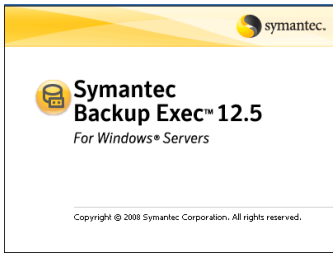


Fig. 6.2.7 Pantalla de inicio de sistema

De ser necesario ejecutaremos los procesos de ***Inventariado y catalogación*** de soportes de respaldos de información. Dentro de la consola de administración de respaldos vamos a la pestaña de ***Dispositivos*** y seleccionaremos la carpeta de ***Respaldos SAP ECCCL1***

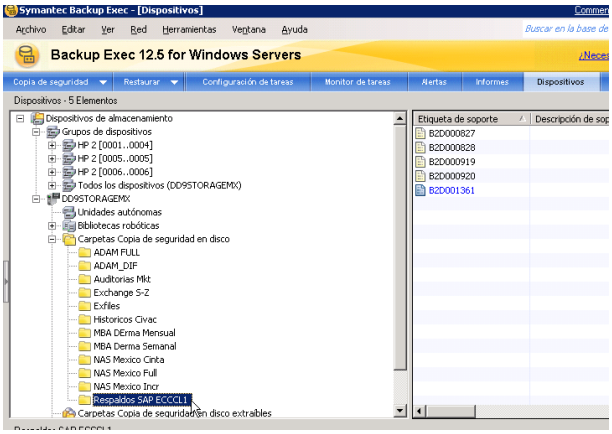


Fig. 6.2.8 Consola de recuperación

Seleccionaremos todos los archivos existentes dentro de la carpeta seleccionada y daremos un clic con el botón derecho del mouse seleccionando la opción de ***Inventariar***

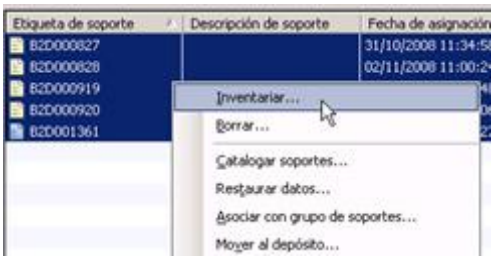


Fig. 6.2.9 Selección de catálogos

En la pantalla siguiente daremos un clic en el botón de ***Ejecutar Ahora***

Seleccionamos la pestaña de ***Monitor de Tareas*** y el panel inferior podremos observar que la tarea se ejecuto correctamente.

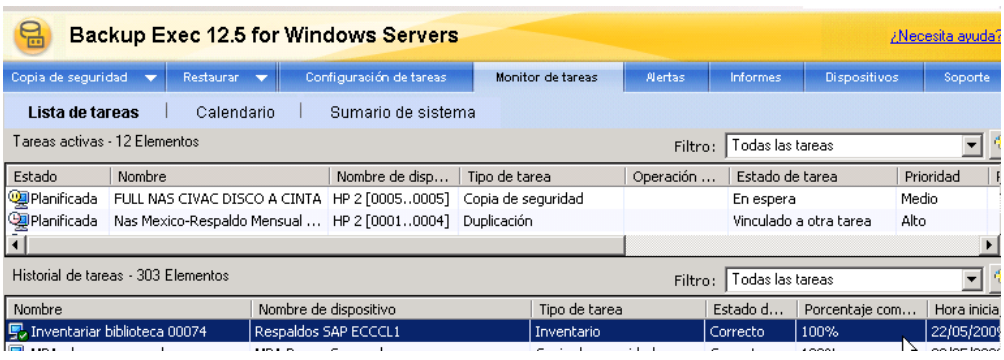


Fig. 6.2.10 Monitor de trabajos

**Catalogación de Soportes**

Seleccionaremos todos los soportes de la carpeta seleccionada y daremos clic con el botón derecho del mouse eligiendo la opción de ***Catalogar Soportes***

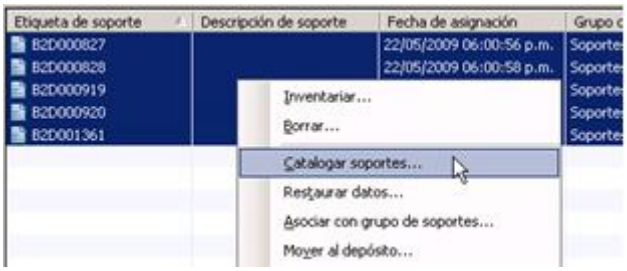


Fig. 6.2.11 Catalogación de soportes

Dependiendo del número de soportes seleccionados aparecerá el mismo número de pantallas como la siguiente en donde daremos un clic en ***EjecutarAhora***

Al término de la catalogación en la pestaña de ***Monitor de Tareas*** podemos revisar la correcta ejecución de los soportes.

| Nombre | Nombre de dispositivo | Tipo de tarea | Estado d... | Porcentaje com... |
|---|---|---|---|---|
| Catalogado 00118 | Respaldos SAP ECCCL1 | Catálogo | Correcto | 100% |
| Catalogado 00117 | Respaldos SAP ECCCL1 | Catálogo | Correcto | 100% |
| Catalogado 00116 | Respaldos SAP ECCCL1 | Catálogo | Correcto | 100% |
| Catalogado 00115 | Respaldos SAP ECCCL1 | Catálogo | Correcto | 100% |
| Catalogado 00113 | Respaldos SAP ECCCL1 | Catálogo | Correcto | 100% |

Fig. 6.2.12 Informe de resultados de tareas

Cambiaremos la cuenta de conexión la sistema de Symanyec BacupExex 12.5 y la homologaremos con el usuario y password de inicio de sesión del servidor restaurado.

Desde la pantalla principal seleccionamos la pestaña de ***Red*** y ***Cuentas deconexión***

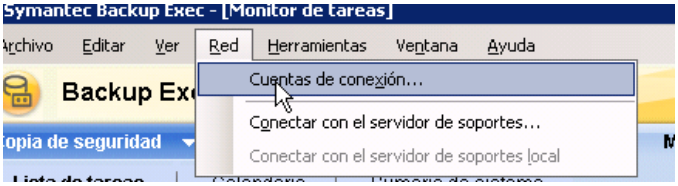


Fig. 6.2.13 Validación de usuario de conexión

Seleccionamos el usuario de ***ecpadm*** y damos un clic en el botón de ***Editar***

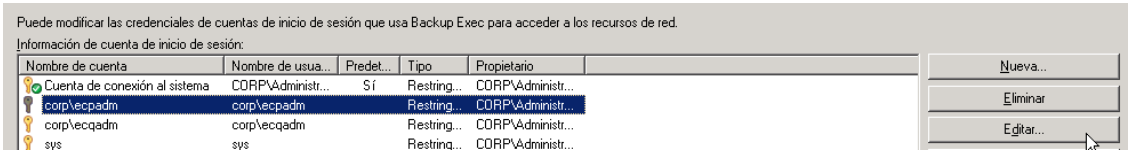


Fig. 6.2.14 Selección de usuario de conexión

Seleccionaremos la opción de ***Cambiar contraseña***

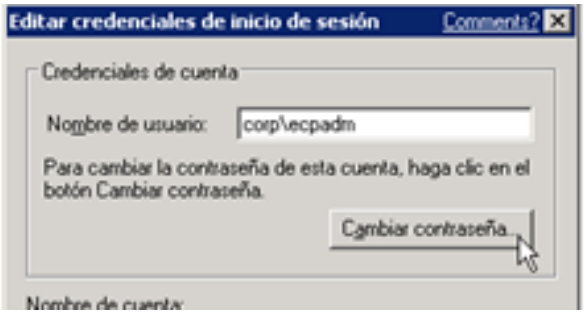


Fig. 6.2.15 Cambio de contraseña

Realizaremos el cambio de password del usuario de conexión de Symantec en el agente instalado en el agente del server restaurado

Damos un clic desde Inicio> All programs > Symantec backup Exec for Windows Server >***Backup Exec Remote Agent Utility***

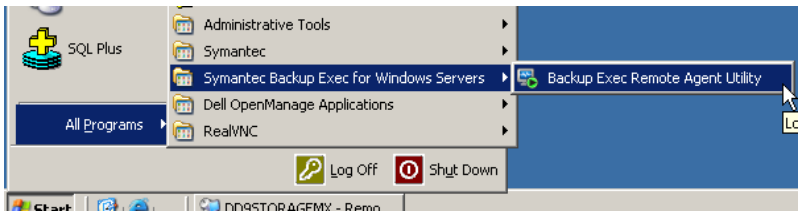


Fig. 6.2.16 Selección de agente

Seleccionamos la pestaña de ***Oracle*** y damos un clic en ***ChangeSettings***

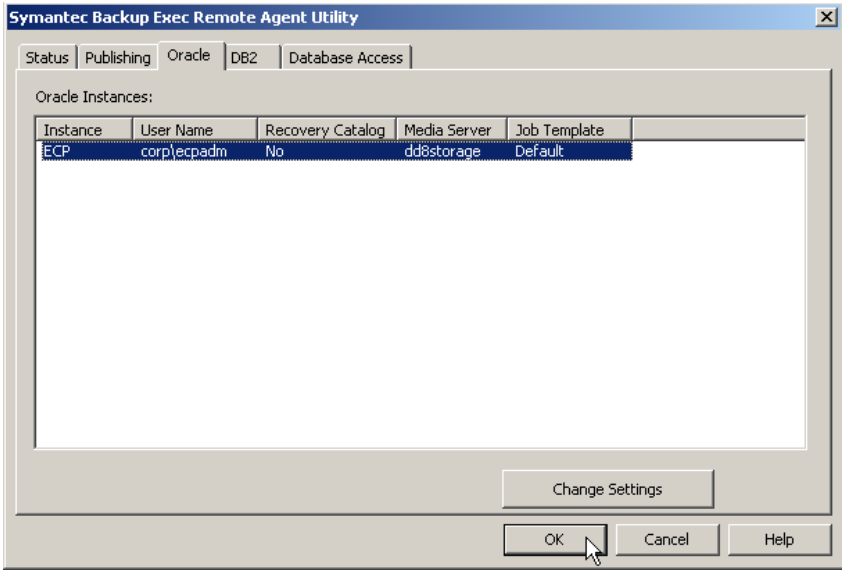


Fig. 6.2.17 Cambio de parametros

Seleccionamos la instancia de ECP y damos un clic en ***Edit***

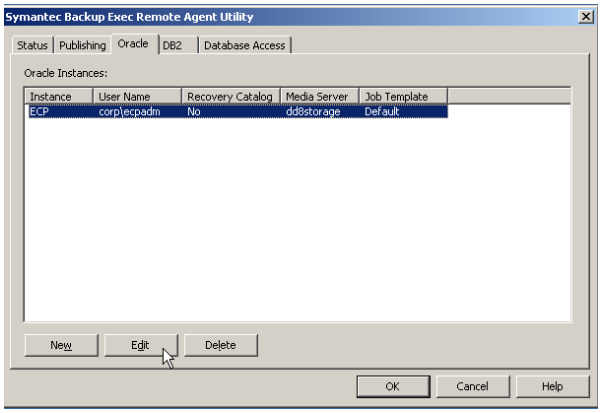


Fig. 6.2.18 Edición de parametros

En la siguiente pantalla verificamos que el usuario sea ***corp\ecpadm*** y damos un clic en ***Changepassword***

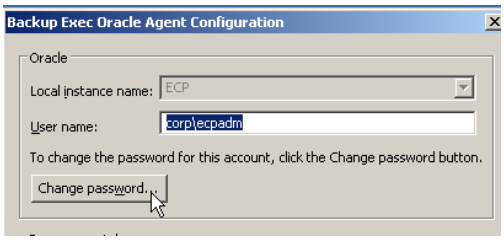


Fig. 6.2.19 Cambio de password

Nos vamos a la pestaña de ***Database Access*** y damos un clic en el botón de ***ChangePassword***

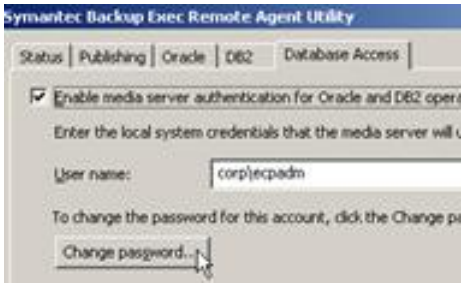


Fig. 6.2.20 Cambio de password

Desde la consola de respaldos (DD9STORAGEMX) seleccionamos la pestaña de ***Restaurar*** damos un clic en ***Nueva tarea de restauración***


Fig. 6.2.21 Nueva tarea de restauración

En dispositivos seleccionamos ***Respaldos SAP ECCCL1***

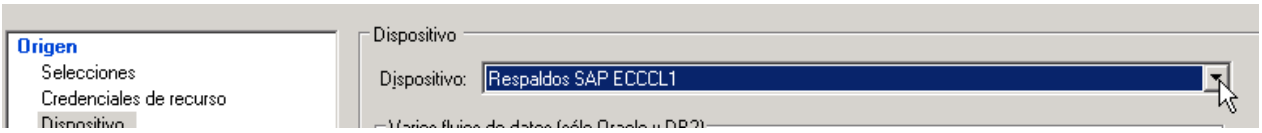


Fig. 6.2.22 Selección de respaldo a restaurar

En ***selecciones*** nos vamos a DARCLUS y seleccionamos el archivo de control más reciente

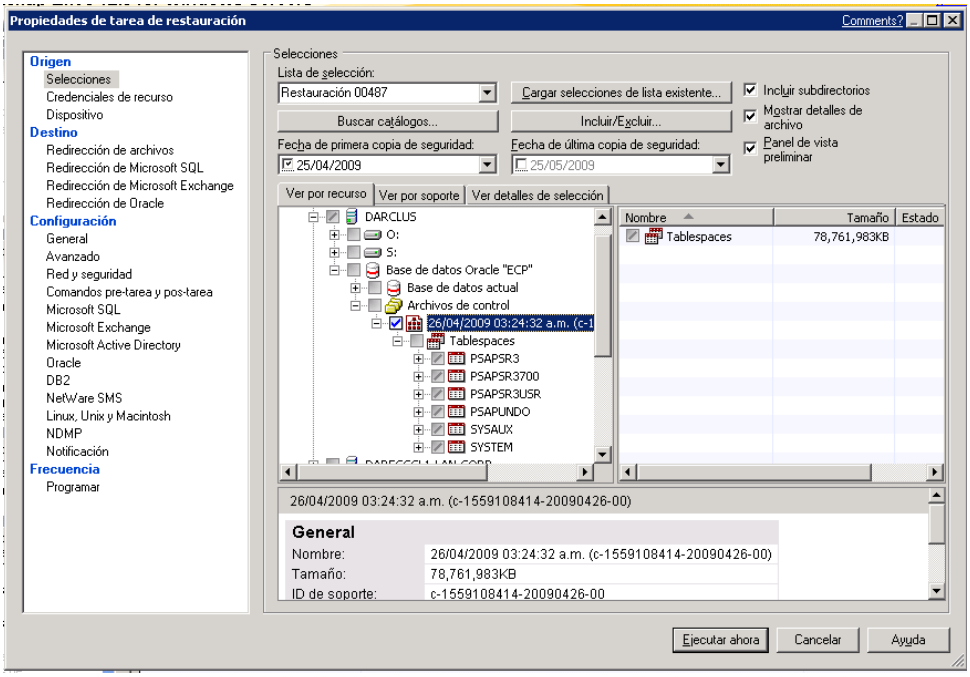


Fig. 6.2.23 Consola de recuperación

En **Destino > Redirección de Oracle** habilitamos la opción de **Redirigir instancias de Oracle**

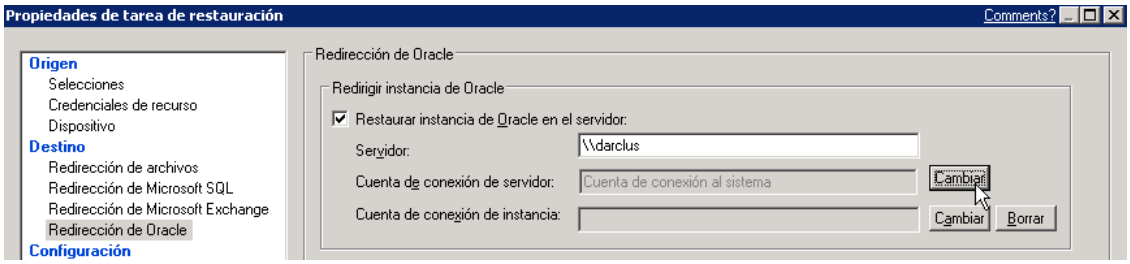


Fig. 6.2.24 Selección de ruta de restauración

Cambiamos la cuenta de conexión al servidor

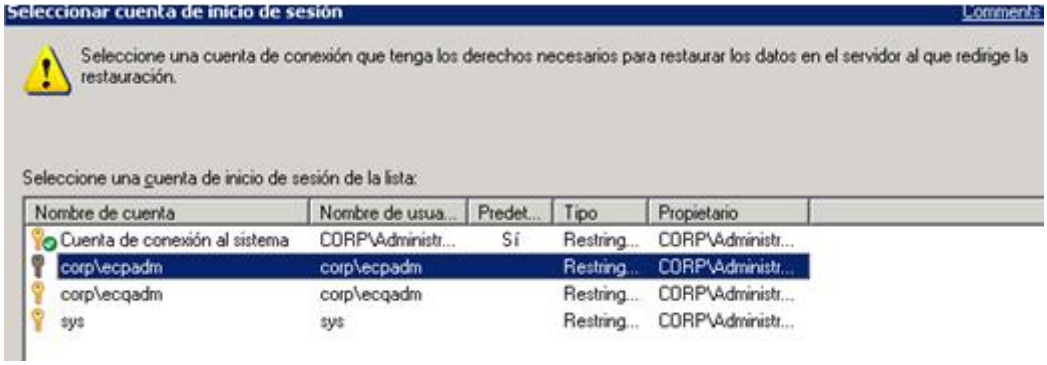


Fig. 6.2.25 Selección de usuario de conexión

Cambiamos la cuenta de conexión a la instancia de Oracle


Fig. 6.2.26 Cambio de instancia de Oracle

Seleccionamos el usuario de**corp\ecpadm**

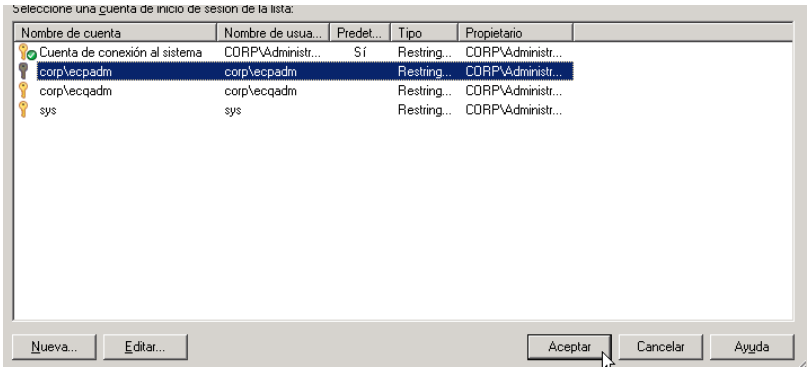


Fig. 6.2.27 Selección de usuario de conexión

Comenzamos con la restauración de la base de datos

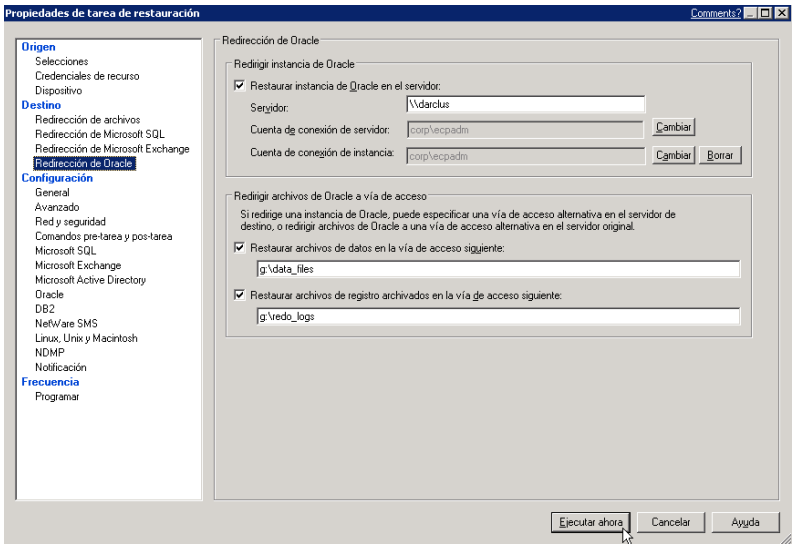


Fig. 6.2.28 Pantalla de inicio de restauración

# 7. GLOSARIO

| | |
|---|---|
| ERP | Enterprice Resource Planining. Un ERP es un sistema de información integral que incorpora los procesos operativos y de negocio. |
| SarbanesOxley | La Ley Sarbanes-Oxley, conocida también como SarOx ó SOA (por sus siglas en inglés SarbanesOxleyAct), es la ley que regula las funciones financieras contables y de auditoria y penaliza en una forma severa, el crimen corporativo y de cuello blanco |
| LOPD | Ley Orgánica de Protección de Datos de España |
| IT | Information technology , Tecnologías de Información |
| RPO | Recovery Point Objective. Expresa la cantidad de datos que una aplicación puede llegar a perder antes de que ello suponga repercusiones negativas para la empresa |
| RTO | Recovery Time Objective, indica cuánto tiempo puede emplear el personal de TI para volver a poner la aplicación en línea después de ocurrir un desastre |
| CEDIS | Centro de distribución |
| SAP | |
| LAN | Local Area Network, Red de área local |
| DBMS | Database management system, sistemas de gestión de bases de datos son un tipo de software muy específico, dedicado a servir de interfaz entre la base de datos, el usuario y las aplicaciones que la utilizan. |
| Kbps | Son las siglas de Kilobits por segundo |
| Mbps | Son las siglas de Megabits por segundo |
| Hertz | |
| Cluster | Conjuntos o conglomerados de computadoras construidos mediante la utilización de hardware comunes y que se comportan como si fuesen una única computadora. |
| TCO | *Total Cost of Ownership,* es el costo total de un producto (por ejemplo, un sistema de información) a lo largo de su ciclo de vida completo. |
| DAS | Direct Attached Storage hace referencia a sistemas de almacenamiento conectados a un host (un PC, portátil o servidor) directamente, sin la existencia de dispositivos de red (como hubs, switchs o routers) entre el dispositivo de almacenamiento y el sistema que hace uso de é |
| SCSI | Small Computers System Interface (Interfaz de Sistema para Pequeñas Computadoras), es una interfaz estándar para la transferencia de datos entre |

distintos dispositivos del bus de la computadora.

| | |
|---|---|
| NAS | Network attached storage es un servidor o disco duro de almacenamiento que viene montado sobre nuestro sistema operativo (Windows o Linux), configurado con la habilidad de aceptar conexiones de red mediante sistemas de archivos |
| RAID | Redundant Array of Independent Disk o conjunto redundante de discos duros independientes que viene a ser como una matriz de discos duros interconectados entre sí y cuya peculiaridad es que se comportan como un único disco es decir, la información se multiplica en cada disco, se graba la misma información en cada uno de ellos, de esta forma si existiese un error físico o mal funcionamiento en uno de ellos el sistema podría continuar funcionando. |
| HBA | Un HBA (Host Bus Adapter) es la tarjeta de interfaz que se conecta a un host una SAN (Storage Area Network) . Es un circuito electrónico y / o adaptador de circuito integrado que ofrece de entrada / salida (E / S) y la conectividad física entre un servidor y un dispositivo de almacenamiento |
| FiberChannel | E una tecnología para transmitir datos entre dispositivos de la computadora a velocidades de datos de hasta 4 Gbps. De canal de fibra está especialmente diseñada para conectar el ordenador servidor de s para dispositivos de almacenamiento compartido y para los controladores de almacenamiento y unidades de interconexión. |
| Hot-pluggable | Conectable en funcionamiento. Permite extraer un componente de un sistema y conectar uno nuevo aunque aún esté encendido y la unidad siga en funcionamiento. Los sistemas redundantes se pueden diseñar para intercambiar unidades de disco, placas de circuito, fuentes de alimentación, CPU o prácticamente cualquier otro elemento que se duplica dentro del equipo. También se denomina "de conexión instantánea". |
| UPS | Sistema de Fuerza Ininterrumpible es un equipo cuya función principal es evitar una interrupción de voltaje en la carga a proteger. |
| NEMA | La Asociación Norteamericana de Manufacturas Eléctricas (NEMA) Es la asociación de comercio más grande en los Estados Unidos, la cual representa los intereses de los fabricantes de la industria eléctrica, y cuyo objetivo es establecer una estandarización |
| DRP | DisasterRecovery Plan, y se refiere a un plan que deben tener todos para recuperarse rápidamente en caso de un desastre informático, y restablecer la operación de la empresa. |
| DNS | DomainNameSystem, Sistema de resolución de nombres. se utiliza para proveer a las computadoras de los usuarios (clientes) un nombre equivalente a las direcciones IP. |

# 8. BIBLIOGRAFIA

Olifer, N. (2009). ***Redes de computadoras. Principios, tecnología y protocolos para el diseño de redes.*** McGraw Hill Interamericana Editores. Primera edición México

Romo Proaño, Marcelo. (2005). ***Informática Básica***. Escuela Politécnica del Ejército. Edición 2005. Ecuador

Microsoft Corporation. (2003). ***Managing a Microsoft Windows Server 2003 Enviroment***. Microsoft Official Course. Edición 2003. Impreso en Colombia

Iseminger, David. (2000). ***Active directory Services for Windows Server. Technical reference***. Primera Ed. 2000 Impreso en USA.

Microsoft Corporation. (2003). ***Manintaining a Microsoft Wndows Server 2003 Envirement***

Microsoft Official Course 2275B. Microsoft 2003. Impreso en Colombia

Achileman, Annie. (2005). ***DELL SAN Management*** Participant Guide 2006.

**Referencias de Internet.**

***Tipos de Respaldos***

http://technet.microsoft.com/en-us/library/cc759141(WS.10).aspx#w2k3tr_back_how_kchg

***Planes de Recuperación de Desastres***

http://www.networksolutionsit.com/?vp=1&ver=1&id=5385&micro2=network

***Software de Recuperación con imágenes***

http://www.symantec.com/es/mx/business/library/article.jsp?aid=rapid_system_recovery

***Características de Windows 2003 server***

http://www.microsoft.com/spain/windowsserver2003

***Especificaciones técnicas del centro de cómputo alterno***

http://www.aduana.gov.ec/archivos/CAE-RE-0030-2010/Anexo%206.%20Diseno%20del%20Centro%20de%20Computo%20Alterno/Especificaciones%20T%C3%A9cnicas%20del%20Centro%20de%20C%C3%B3mputo%20Alterno.pdf

***Guía para la elaboración de planes de recuperación para sistemas de información empresarial y de negocios***

http://www.eumed.net/ce/2009b/jdnr.htm

***Introducción al riesgo informático***

http://www.ccee.edu.uy/ensenian/catcomp/material/riesgo.pdf

***El Análisis de Riesgos Base de un Sistema de Gestión de Seguridad de Información. Caso Magerit***

http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/17-ElAnalisisRiesgosBaseSistemaGestionSeguridadInformacionCasoMagerit.pdf