



**UNIVERSIDAD TÉCNICA DEL NORTE**  
**FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS**  
**CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES**

**TEMA**

“ESTUDIO, ANÁLISIS Y COMPARACIÓN DE TRES HERRAMIENTAS PARA EL SALVAGUARDO DE INFORMACIÓN.”

**APLICATIVO**

“Implementación de una de las Herramientas de Salvaguardo de Información para Sinergy Team Cia. Ltda.”

**Autor:** Edgar Humberto Ortega Pilco

**Director:** ING. XAVIER MAURICIO REA PEÑAFIEL

**Ibarra – Ecuador**

**2012**

# CERTIFICACIÓN

En mi calidad de Director del Trabajo de Grado presentado por el egresado EDGAR HUMBERTO ORTEGA PILCO, para optar por el título de **INGENIERO EN SISTEMAS COMPUTACIONALES**, cuyo tema es **ESTUDIO, ANÁLISIS Y COMPARACIÓN DE TRES HERRAMIENTAS PARA EL SALVAGUARDO DE INFORMACIÓN, CON EL APLICATIVO: IMPLEMENTACIÓN DE UNA DE LAS HERRAMIENTAS DE SALVAGUARDO DE INFORMACIÓN PARA SINERGY TEAM CIA. LTDA.** Considero que el presente trabajo reúne requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del tribunal examinador que se designe.

En la ciudad de Ibarra a los 26 días del mes de octubre del 2011.

.....  
Ing. Xavier Mauricio Rea Peñafiel

**Director de la Tesis**

# CERTIFICACIÓN

Quito, 4 de junio de 2012

Señores  
UNIVERSIDAD TÉCNICA DEL NORTE  
Presente

De mis consideraciones.-

Siendo auspiciantes del proyecto de tesis del Egresado EDGAR HUMBERTO ORTEGA PILCO con CI: 100249363-1 quien desarrolló su trabajo con el tema "ESTUDIO, ANÁLISIS Y COMPARACIÓN DE TRES HERRAMIENTAS PARA EL SALVAGUARDO DE INFORMACIÓN." Con el aplicativo "IMPLEMENTACIÓN DE UNA DE LAS HERRAMIENTAS DE SALVAGUARDO DE INFORMACIÓN PARA SINERGY TEAM CIA. LTDA.", me es grato informar que se han superado con satisfacción las pruebas técnicas y la revisión de cumplimiento de los requerimientos funcionales, por lo que se recibe el proyecto como culminado y realizado por parte del egresado EDGAR HUMBERTO ORTEGA PILCO. Una vez que hemos recibido la capacitación y documentación respectiva, nos comprometemos a continuar utilizando el mencionado aplicativo en beneficio de nuestra empresa/institución.

El egresado EDGAR HUMBERTO ORTEGA PILCO puede hacer uso de este documento para los fines pertinentes en la Universidad Técnica del Norte.

Atentamente,

---

Ing. Víctor Hugo Hinojosa Jaramillo

GERENTE DE IT

SINERGY TEAM CIA. LTDA.



**UNIVERSIDAD TÉCNICA DEL NORTE**  
**CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO**  
**DE INVESTIGACIÓN**  
**A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL**  
**NORTE**

Yo, EDGAR HUMBERTO ORTEGA PILCO con Cédula de Ciudadanía N° 100249363-1, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4,5, y 6, en calidad de autora del Trabajo de Grado denominado **ESTUDIO, ANÁLISIS Y COMPARACIÓN DE TRES HERRAMIENTAS PARA EL SALVAGUARDO DE INFORMACIÓN, CON EL APLICATIVO: IMPLEMENTACIÓN DE UNA DE LAS HERRAMIENTAS DE SALVAGUARDO DE INFORMACIÓN PARA SINERGY TEAM CIA. LTDA.**, que ha sido desarrollado para optar el título de Ingeniero en Sistemas Computacionales en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autor me reservo los derechos morales de la obra antes mencionada, aclarando que el trabajo aquí descrito es de mi autoría y que no ha sido previamente presentado para ningún grado o calificación profesional.

En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la biblioteca de la Universidad Técnica del Norte.

.....

Edgar Humberto Ortega Pilco.

C.I. 100249363-1

Ibarra, a los 16 días del mes de julio del 2012



## UNIVERSIDAD TÉCNICA DEL NORTE

### BIBLIOTECA UNIVERSITARIA

## AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

### 1. IDENTIFICACIÓN DE LA OBRA

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital institucional determina la necesidad de disponer los textos completos de forma digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual ponemos a disposición la siguiente investigación:

DATOS DE CONTACTO	
<b>CEDULA DE IDENTIDAD</b>	100249363-1
<b>APELLIDOS Y NOMBRES</b>	EDGAR HUMBERTO ORTEGA PILCO
<b>DIRECCIÓN</b>	Eloy Alfaro y Granados E14-486
<b>EMAIL</b>	<a href="mailto:eortega@sinergyteam.com.ec">eortega@sinergyteam.com.ec</a>
<b>TELÉFONO FIJO</b>	023341968
<b>TELÉFONO MÓVIL</b>	080253773

DATOS DE LA OBRA	
<b>TÍTULO</b>	"TÍTULO DEL TRABAJO DE GRADO"
<b>AUTOR</b>	EDGAR HUMBERTO ORTEGA PILCO
<b>FECHA</b>	21/05/2012
<b>PROGRAMA</b>	PREGRADO
<b>TÍTULO POR EL QUE</b>	INGENIERÍA EN SISTEMAS COMPUTACIONALES
<b>DIRECTOR</b>	ING. XAVIER MAURICIO REA PEÑAFIEL

### 2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, EDGAR HUMBERTO ORTEGA PILCO, con cedula de identidad Nro. 100249363-1, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y el uso del archivo digital en la biblioteca de la universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión, en concordancia con la Ley de Educación Superior Artículo 144.

.....  
Firma

Nombre: EDGAR HUMBERTO ORTEGA PILCO  
Cédula: 100249363-1

Ibarra a los 16 días del mes de julio del 2012

## Dedicatoria

*Dedico todo mi esfuerzo y trabajo puesto para realizar este proyecto de tesis a mi hija Nathalia por quien cada día, cada paso tiene sentido, testiga silenciosa de mis luchas cotidianas.*

*A mis padres, quienes a lo largo de mi vida han velado por mi bienestar y educación siendo mi apoyo en todo momento, depositando su entera confianza en cada reto que se me presentaba sin dudar ni un solo momento de mi capacidad. Su tenacidad y lucha insaciable han hecho de ellos el gran ejemplo a seguir y destacar, no solo para mí, sino para mis hermanos y familia en general.*

## Agradecimiento

*El cofre en el que se encuentran los más maravillosos tesoros a los que puede acceder el hombre, no se hallan fuera, sino en el más profundo de su mundo interior y hoy iluminado con la luz sagrada que refulge el dorado cáliz del corazón humano quiero expresar mi más fervorosos agradecimientos.*

*A mis hermanos Luis y Maribel por su solidaridad y que con su ejemplo son mi incentivo para seguir adelante cosechando triunfos.*

*A mi Director de Tesis Ing. Mauricio Rea, que con su ejemplo de perseverancia y logros alcanzados, me supo guiar en el arduo trabajo que conlleva la realización de este documento.*

*Y finalmente a la mi querida Universidad y maestros por permitirme ser parte de una generación de triunfadores y personas que ha sabido llevar en alto las enseñanzas y ejemplos otorgados en cada una de las aulas.*

## Índice de Contenidos

CAPITULO 1.....	1
DEFINICIÓN DE MÉTRICAS DEL NEGOCIO.....	1
<b>1.1. INTRODUCCIÓN</b> .....	2
<b>1.2. SITUACIÓN ACTUAL</b> .....	3
<b>1.3. POLÍTICAS DEL NEGOCIO</b> .....	4
<b>1.4. FUNCIONES DEL DEPARTAMENTO DE TI</b> .....	5
<b>1.5. PROCESOS QUE SE REALIZAN A NIVEL DE SERVIDORES</b> .....	5
<b>1.6. EL PROBLEMA</b> .....	8
<b>1.7. OBJETIVOS DEL PROYECTO</b> .....	8
<b>1.7.1. Objetivos Generales</b> .....	8
<b>1.7.2. Objetivos Específicos</b> .....	8
<b>1.8. ESTUDIO DE RIESGOS</b> .....	9
<b>1.8.1. Tecnológico</b> .....	9
<b>1.8.2. Ambiental</b> .....	10
<b>1.8.3. Laboral</b> .....	11
<b>1.8.4. De las Herramientas</b> .....	12
<b>1.8.5. De los Requerimientos</b> .....	13
<b>1.9. VALORACIÓN DE CADA UNO DE LOS RIESGOS</b> .....	14
CAPÍTULO 2.....	15
ESTUDIO DE LAS HERRAMIENTAS DE SALVAGUARDO DE INFORMACIÓN.....	15
<b>2.1. DEFINICIÓN DE SALVAGUARDO DE INFORMACIÓN</b> .....	16
<b>2.2. AMANDA SOURCE BACKUP</b> .....	19
<b>2.2.1. Componentes de Amanda Source Backup</b> .....	20
<b>2.2.2. Características de Amanda Source Backup</b> .....	21
<b>2.2.3. Como Funciona Amanda Source Backup</b> .....	25
<b>2.2.4. Tratamiento de la Información</b> .....	26
<b>2.2.5. Evolución de Amanda Source Backup</b> .....	28
<b>2.2.6. Generación de Material de Entrenamiento</b> .....	30
<b>2.3. TIVOLI STORAGE MANAGER</b> .....	30

2.3.1.	<i>Componentes de Tivoli Storage Manager.</i>	32
2.3.2.	<i>Características de Tivoli Storage Manager.</i>	36
2.3.3.	<i>Como Funciona Tivoli Storage Manager.</i>	40
2.3.4.	<i>Tratamiento de la Información.</i>	44
2.3.5.	<i>Evolución de Tivoli Storage Manager.</i>	46
2.3.6.	<i>Generación de Material de Entrenamiento.</i>	47
2.4.	<b>SYSTEM CENTER DATA PROTECTION MANAGER.</b>	48
2.4.1.	<i>Componentes de System Center Data Protection Manager.</i>	48
2.4.2.	<i>Características de System Center Data Protection Manager.</i>	50
2.4.3.	<i>Como Funciona System Center Data Protection Manager.</i>	54
2.4.4.	<i>Tratamiento de la Información.</i>	58
2.4.5.	<i>Evolución de System Center Data Protection Manager.</i>	62
2.4.6.	<i>Generación de Material de Entrenamiento.</i>	64
CAPÍTULO 3.....		65
ANÁLISIS Y COMPARATIVAS .....		65
3.1.	<b>REQUERIMIENTOS DEL SISTEMA</b> .....	66
3.1.1.	<i>Requerimientos a nivel de Servidor.</i>	66
3.1.2.	<i>Requerimientos a nivel de Respaldos.</i>	72
3.1.3.	<i>Requerimientos a nivel de Conectividad.</i>	73
3.2.	<b>ADMINISTRACIÓN DE RESPALDOS</b> .....	74
3.2.1.	<i>Manejo de Políticas de Respaldo.</i>	74
3.2.2.	<i>Modelo de Respaldos Utilizado.</i>	76
3.2.3.	<i>Flexibilidad de Configuración.</i>	78
3.2.4.	<i>Métodos de Administración.</i>	80
3.3.	<b>Comparativas de las Herramientas</b> .....	83
3.3.1.	<i>Principales diferencias y similitudes.</i>	83
CAPÍTULO 4.....		87
IMPLEMENTACIÓN, ACEPTACIÓN Y PRUEBAS DE LA HERRAMIENTA .....		87
4.1.	<b>ACTIVIDADES BÁSICAS</b> .....	88
4.2.	<b>CONFIGURACIÓN SEGÚN REQUERIMIENTOS DE LA COMPAÑÍA.</b> .....	89
4.2.1.	<b>Instalación de Cliente Linux / Ubuntu / Windows.</b> .....	89
4.2.2.	<b>Instalación de Cliente MYSQL y Microsoft SQL Server.</b> .....	91

<b>4.3. MANTENIMIENTO DE LA HERRAMIENTA.....</b>	<b>94</b>
<b>4.4. PRODUCCIÓN.....</b>	<b>94</b>
CAPÍTULO 5.....	95
CONCLUSIONES Y RECOMENDACIONES.....	95
<b>5.1. CONCLUSIONES .....</b>	<b>96</b>
<b>5.2. RECOMENDACIONES .....</b>	<b>97</b>
<b>5.3. POSIBLES TEMAS.....</b>	<b>98</b>
GLOSARIO.....	99
BIBLIOGRAFÍA Y REFERENCIAS. ....	108
REFERENCIAS GRÁFICAS.....	109
ANEXOS.....	110

## Índice de Figuras.

FIGURA 2.1. ALMACENAMIENTO DE RESPALDOS.....	19
FIGURA 2.2. AMBIENTE DE AMANDA.....	24
FIGURA 2.3. PROCESO DE RESPALDOS .....	27
FIGURA 2.4. DIAGRAMA DE RESPALDOS GERÉRICO .....	31
FIGURA 2.5. PROCESOS DE COPIA DE SEGURIDAD, ARCHIVADO Y MIGRACIÓN.....	43
FIGURA 2.6. EVOLUCIÓN DE TIVOLI STORAGE MANAGER .....	47
FIGURA 2.7. ESTRUCTURA DE DATA PROTECTION MANAGER .....	54
FIGURA 2.8. MÉTODOS DE ALMACENAMIENTO DE DATOS.....	59
FIGURA 2.9. ESQUEMA DE RESPALDOS DE DATA PROTECTION MANAGER.....	61
FIGURA 3.1. MANEJO DE TAPES.....	78
FIGURA 3.2. LINEA DE COMANDOS DE AMANADA SOURCE BACKUP .....	80
FIGURA 3.3. INTERFACE DE ADMINISTRACIÓN AMANDA NETWORK.....	80
FIGURA 3.4. LÍNEA DE COMANDOS DE TSM.....	81
FIGURA 3.5. INTERFACE WEB DE ADMINISTRACIÓN DE TSM .....	81
FIGURA 3.6. INTERFACE GUI DE ADMINISTRACIÓN WINDOWS.....	82
FIGURA 3.7. INTERFACE DE ADMINISTRACIÓN GUI DE DPM.....	82
FIGURA 4.1. CONFIGURACIÓN ARCHIVO DSM.OPT (LINUX).....	90
FIGURA 4.2. CONFIGURACIÓN ARCHIVO DSM.SYS (LINUX).....	90
FIGURA 4.3. CONFIGURACIÓN ARCHIVO DSM.OPT (WINDOWS) .....	90
FIGURA 4.4. INTERFACE GUI DE MSSQL SERVER.....	92
FIGURA 4.5. CONFIGURACIÓN DE CLAVE DE MSSQL. ....	93
FIGURA 4.6. EJEMPLO DE RESPALDO DE MSSQL SERVER.....	93

## Índice de Tablas

TABLA 1.1. ESQUEMA DE RESPALDOS POR SERVIDOR .....	7
TABLA 1.2. RIESGO TECNOLÓGICO .....	9
TABLA 1.3. RIESGO AMBIENTAL .....	10
TABLA 1.4. RIESGO LABORAL.....	11
TABLA 1.5. RIESGO DE LAS HERRAMIENTAS .....	12
TABLA 1.6. RIESGO DE REQUERIMIENTOS .....	13
TABLA 1.7. VALORACIÓN DE RIESGOS .....	14
TABLA 2.1. EVOLUCIÓN DE EQUIPOS INFORMÁTICOS.....	18
TABLA 2.2. COMPARATIVA DE VERSIONES DE AMANDA .....	29
TABLA 2.3. ESQUEMA NORMAL DE RESPALDOS.....	56
TABLA 2.4. ESQUEMA DE RESPALDOS CON LAN BACKUP .....	56
TABLA 2.5. EVOLUCIÓN DE LAS VERSIONES DE DPM.....	62
TABLA 2.6. PRINCIPALES DIFERENCIAS ENTRE VERSIONES DE DPM .....	64
TABLA 3.1. SISTEMAS OPERATIVOS SOPORTADOS POR AMANDA .....	68
TABLA 3.2. SISTEMAS OPERATIVOS SOPORTADOS POR TSM .....	71
TABLA 3.3. SISTEMAS OPERATIVOS SOPORTADOS POR DPM .....	72
TABLA 3.4. CARACTERÍSTICAS DE ALMACENAMIENTO. ....	73
TABLA 3.5. CARACTERÍSTICAS DE CONECTIVIDAD. ....	74
TABLA 3.6. MANEJO DE POLÍTICAS DE RESPALDO. ....	76
TABLA 3.7. FREXIBILIDAD DE CONFIGURACIÓN. ....	80
TABLA 3.8. PRINCIPALES DIFERENCIAS ENTRE HERRAMIENTAS. ....	85
TABLA 4.1. CUMPLIMIENTO DE REQUISITOS DE NEGOCIO. ....	88

## Resumen

Este documento analiza los factores que impulsan la necesidad de Respaldo de Información y los beneficios que éste proceso ofrece. Entre los temas tratados, se incluyen:

- Aspectos del crecimiento de información y la presión resultante en los procesos de “Backup”.
- Tecnologías para realización de “Backups” actuales y su implementación.
- Beneficios de implementar “Backups” y su impacto positivo en el negocio.
- Factores que determinan la eficiencia de un “Backup”.
- Consideraciones específicas de “Backups” en disco.

Finalmente, el documento describirá brevemente las soluciones de “Backup” que se han optimizado para satisfacer las necesidades de “Backups”, los requerimientos de recuperación y los entornos de las aplicaciones.

## Summary

This document examines the factors that driving the need to back up data and the benefits that this process offers. The topics covered include:

- Aspects of the information growth and the resulting pressure in the backup processes.
- The technologies to making current backups and its implementation.
- The benefits of implementing backups and its positive impact on the business.
- The factors that determine the efficiency of a backup.
- The specific considerations to making backups on disk.

Finally, the document will briefly describe the backup solutions that have been optimized to meet the backup needs, the recovery requirements and application environments.

## CAPITULO 1.



## DEFINICIÓN DE MÉTRICAS DEL NEGOCIO.

## 1.1. INTRODUCCIÓN

SINERGY TEAM CIA. LTDA., surge de la necesidad de brindar al cliente una opción dinámica, fresca, altamente tecnológica que ataque las necesidades puntuales del negocio, basándose para esto en nuestros socios tecnológicos, personal del área de TI.

SINERGY TEAM CIA. LTDA., es un asociado de negocios de software, nivel PREMIER de IBM, además de contar con las certificaciones técnicas y comerciales, posee la experiencia necesaria, que permite garantizar el éxito en todos los proyectos que se presenten.

Si bien con la adquisición de los productos IBM, está incluido el soporte técnico directo del Centro de Soporte Latino en Argentina, SINERGY TEAM con el propósito de que los clientes obtengan la mejor optimización de su inversión, proporciona diferentes modalidades de asistencia técnica, las mismas que le permiten al cliente optar por la que más se ajuste a sus necesidades.

Sinergy Team Information Management Solution - Multiplataforma: Solución para optimizar el manejo de la información al interior de la organización, las compañías hoy día requieren mejores tiempos de respuesta y maximizar los recursos de hardware y software, esta solución asegura incrementar en un 30% el rendimiento de su base de datos actual basada en Software IBM. "Sinergy Team Information Management Solution - Multiplataforma" asegura mayor rendimiento y tiempos de respuesta de su sistema de información actual. Esta solución se aplica a plataformas CISC – RISC con sistemas operativos como AIX, HP-UX, Solaris, Windows; que trabajan con IBM Informix Dynamic Server y/o DB2.

Sinergy Team Information Management Solution - Linux: Solución para optimizar el manejo de la información al interior de la organización, las compañías hoy día requieren mejores tiempos de respuesta y maximizar los recursos de hardware y software, esta solución asegura incrementar en un 30% el rendimiento de su base de datos actual basada en Software IBM. "Sinergy Team Information Management Solution - Linux " asegura mayor rendimiento y tiempos de respuesta de su sistema de información actual. Esta solución se aplica a plataformas CISC con sistemas operativos Linux que trabajan con IBM Informix Dynamic Server y/o DB2.

Debido a la experiencia del personal técnico y a la necesidad de mercado, los cursos y talleres especializados que manejan son:

SERVIDORES Y HERRAMIENTAS DE DESARROLLO

SISTEMAS OPERATIVOS

OTROS

Para la capacitación de las soluciones de productos de CONTENT MANAGER, es necesario configurar los cursos de acuerdo a las necesidades del cliente. Para cursos o talleres bajo demanda, se estructurarán de acuerdo con los requerimientos del cliente, brindando flexibilidad tanto en horarios, fechas como lugar.

SINERGY TEAM CIA. LTDA., está en capacidad de brindar asesoría y apoyo en proyectos tecnológicos específicos, gracias al manejo de “know how” e infraestructura. Está en capacidad de garantizar un mejor retorno de inversión, optimizando procesos y recursos de la empresa, logrando la total satisfacción de los clientes. En cuanto a proyectos, luego de analizar la necesidad de los clientes, la empresa está en capacidad de coadyuvar con personal, conceptos o reorganizaciones. Algunos de los proyectos en los que han participado o está participando son: Reorganización de Centros de Cómputo · Desarrollo de módulos especiales · Cooperación en rediseño de sistemas existentes · Outsourcing de servicio de Administración en Centros de Cómputo, etc.

## **1.2. SITUACIÓN ACTUAL**

Sinergy Team Cia. Ltda., tiene como necesidad la acción de generar diariamente respaldos de sus servidores presentes en el Centro de Datos, con respecto a base de datos, correo electrónico, servidores de archivos, por tratarse de un proceso en su mayor parte manual y con intervención humana se está repercutiendo en fallas en los procesos de protección de la información y el tiempo para los mismos se ha visto triplicado en su ejecución y termino correcto, es por esto que se ha visto el requerimiento de automatizar este proceso.

Al no realizar de manera automática estos procesos de aseguramiento de información a ocasionado problemas que afectan en la gestión administrativa y la organización de la ejecución de las tareas de protección de la información, adicionalmente con el aumento de

datos, personal y la creación de nuevas empresas se han generado los siguientes inconvenientes:

- ✓ Olvido en la ejecución de tareas de protección de la información en algunos servidores.
- ✓ Falta de registro de cada tarea realizada.
- ✓ Retraso en tiempos de ejecución programados.
- ✓ Inexistencia de un registro de que información fue salvaguardada.
- ✓ Pérdida de información por daños en equipos o servicios.

Actualmente no se tiene un sistema que facilite de manera óptima la gestión administrativa y efectiva de Protección de la Información de toda la organización, que pueda proporcionar recuperación de información de manera fácil y rápida, ejecución y monitoreo de tareas de protección de información de manera organizada, verificación de la correcta ejecución de dichas tareas, administración centralizada de todos los servidores y ambientes de trabajo presentes en la compañía.

### **1.3. POLÍTICAS DEL NEGOCIO**

SINERGY TEAM CIA. LTDA. Tiene como pilar fundamental el proporcionar a las empresas ecuatorianas la tecnología y las soluciones que se ajusten a sus requerimientos, contando con el recurso humano especializado en las diferentes tecnologías y herramientas que demanda el mercado, apoyado en un amplio portafolio de soluciones empresariales, para proveer servicios altamente competitivos y de calidad.

Gracias a la experiencia que le da su larga trayectoria, certificaciones y cumplimiento de objetivos, IBM la ha calificado como asociado de negocios Nivel Premier.

SINERGY TEAM, con el afán de brindar un amplio portafolio de soluciones, posee alianzas estratégicas de gran valor, basadas en una asistencia permanente y efectiva, que le permite ofrecer a sus clientes productos de reconocida calidad en varias áreas. En cada definición de proyecto de ser necesario se generan nuevas alianzas para poder satisfacer las necesidades del cliente.

#### **1.4. FUNCIONES DEL DEPARTAMENTO DE TI**

Las funciones definidas para el departamento de TI (Ingenieros de Soporte), están definidas de la siguiente manera:

- ✓ Verificar los estados de todos y cada uno de los servidores presentes en la compañía.
- ✓ Chequear respaldos realizados en la noche y parte de la madrugada de cada uno de los servidores.
- ✓ Generar el listado de las tareas realizadas en los servidores.
- ✓ Si se presenta un error en los respaldos, agendar una hora de bajo impacto para los usuarios, para poder realizar las tareas que no se realizaron en horas de la noche manualmente.
- ✓ Si no es factible realizar las tareas de respaldo en el horario normal de trabajo tendrá que realizarlo el técnico de turno en horas no laborables.
- ✓ Realizar chequeos constantes sobre tareas pendientes en los clientes.
- ✓ Completar la lista de clientes con los cuales hay que comunicarse.
- ✓ Reportar a su Jefe inmediato por tareas a realizar fuera del cronograma del día.
- ✓ Generar al fin del día cronograma para el siguiente día y si se lo realiza fuera de la oficina informar a todo el departamento de TI.

#### **1.5. PROCESOS QUE SE REALIZAN A NIVEL DE SERVIDORES**

Se describe a continuación las tareas que se realizan a nivel de servidores

Servidor de Correo (SRVMAIL).

- ✓ Ejecución de Respaldo a través del script (bkp\_incr\_mail.sh) diariamente a las 22:00 (Respaldo Incremental).
- ✓ Compresión del respaldo generado.
- ✓ Copiar respaldo a disco externo y borrado del respaldo origen.
- ✓ Ejecución de Respaldo a través del script (bkp\_full\_mail.sh) mensualmente a las 22:00 todos los 30's de cada mes (Respaldo completo).
- ✓ Se utiliza comandos propios de Exchange para poder generar respaldos de las bases GDB.

Servidor de Archivos (FILESERVER).

- ✓ Ejecución de Respaldo a través del script (bkp\_incr\_file.cmd) diariamente a las 00:00 (Respaldo Incremental).
- ✓ Compresión del respaldo generado.
- ✓ Copiar respaldo a disco externo y borrado del respaldo origen.
- ✓ Ejecución de Respaldo a través del script (bkp\_full\_file.cmd) mensualmente a las 00:00 todos los 30's de cada mes (Respaldo completo).
- ✓ Se respalda todo el directorio denominado FILESERVER, donde se encuentran todos los archivos y directorios pertenecientes a la compañía.

Servidor de Contabilidad (CONAST).

- ✓ Ejecución de Respaldo a través del script (bkp\_full\_conta.cmd) diariamente a las 02:00 (Respaldo completo).
- ✓ Compresión del respaldo generado.
- ✓ Copiar respaldo a disco externo y borrado del respaldo origen.
- ✓ Se realiza un respaldo del archivo GDB, base de datos del sistema de Contabilidad.

Servidor de CRM (SRVSUGAR).

- ✓ Ejecución de Respaldo a través del script (bkp\_incr\_crm.sh) diariamente a las 04:00 (Respaldo Incremental).
- ✓ Copiar respaldo a disco externo y borrado del respaldo origen.
- ✓ Ejecución de Respaldo a través del script (bkp\_full\_crm.sh) mensualmente a las 04:00 todos los 30's de cada mes (Respaldo Completo).
- ✓ Los respaldos se realizan de la base de datos de MYSQL, utilizando comandos propios del mismo motor.

Servidor de Untangle (FIREWALL).

- ✓ Bajada del Servicio y motor de Untangle.
- ✓ Ejecución de Respaldo a través del script (bkp\_full\_firewall.sh) diariamente a las 04:30 (Respaldo Completo).
- ✓ Compresión del respaldo generado.
- ✓ Copiar respaldo a disco externo y borrado del respaldo origen.
- ✓ Subida del Servicio y motor de Untangle.

- ✓ Se realiza el respaldo de la información desde la línea de comandos del sistema operativo conjuntamente con los de la herramienta.

Servidor de Aranda Soft (SRVARANDA).

- ✓ Ejecución de Respaldo a través del script (bkp\_incr\_aranda.cmd) diariamente a las 05:30 (Respaldo Incremental).
- ✓ Compresión del respaldo generado.
- ✓ Copiar respaldo a disco externo y borrado del respaldo origen.
- ✓ Ejecución de Respaldo a través del script (bkp\_full\_aranda.cmd) mensualmente a las 05:30 todos los 30's de cada mes (Respaldo Completo).
- ✓ Se realiza el respaldo de las bases ArandaDB, keys, etc., de la base de datos Microsoft SQL 2005 Standard.

SRVMAIL	COMPLETO	30 de Cada Mes	22:00	MICROSOFT EXCHANGE	40GB
	INCREMENTAL	Diariamente	22:00		
FILESERVER	COMPLETO	30 de Cada Mes	00:00	SISTEMA DE ARCHIVOS LINUX	2TB
	INCREMENTAL	Diariamente	00:00		
CONTAST	COMPLETO	Diariamente	02:00	BASE DE DATOS INTERBASE	200MB
SRVSUGAR	COMPLETO	30 de Cada Mes	04:00	BASE DE DATOS MYSQL	2GB
	INCREMENTAL	Diariamente	04:00		
FIREWALL	COMPLETO	Diariamente	04:30	SISTEMA DE ARCHIVOS DEBIAN	45GB
SRVARANDA	COMPLETO	30 de Cada Mes	05:30	MICROSOFT SQL 2005 STANDARD	4GB
	INCREMENTAL	Diariamente	05:30		

Tabla 1.1. Esquema de Respaldos por Servidor  
Fuente. Personal

Para nuestro caso, luego del informe de manejo y utilización de espacio otorgado por el personal de Sinergy Team, se procede a definir las características del servidor para albergar dicha información.

- ✓ Una servidor IBM X3580 M3 de Rack, Quad Core de 3,6HG, con 16GB en memoria RAM, tarjeta de red dual port, dos discos de 7200 RPM de 146GB SAS en RAID 1 y cuatro discos de 15000 RPM de 2TB SATA en RAID 5.

## **1.6. EL PROBLEMA**

Sinergy Team Cia. Ltda. Ofrece servicios de consultoría, implementaciones, soporte, venta de Software, Hardware y Capacitación de talento humano utilizando para ello el apoyo de tecnología como son servidores de aplicaciones, correo, base de datos y de archivos pero no cuenta con un sistema dinámico, confiable, fácil de administrar y modificar para el salvaguardo de información de toda su infraestructura informática. Por lo tanto todo el data center se encuentran de cierta manera aislado de las tareas de salvaguardo de información.

La falta de un sistema confiable de información, planificación y administración de salvaguardo de la información, así como la no existencia de una herramienta centralizada de monitoreo y verificación de actividades ha llegado a convertirse en un punto crítico incluso afectando a los clientes tanto internos como externos que es el principal foco de atención para la compañía, es primordial contar con un sistema de administración que permita identificar de manera ágil posibles inconvenientes que se produzcan con los servidores referente a salvaguardo de la información, calendarización para la realización de los mismos, registro detallado de que información es la que se está manejando, información tanto para fallos como para tareas completadas correctamente, acceso rápido a la información en caso de necesitarla sin restricción de sistema operativo.

## **1.7. OBJETIVOS DEL PROYECTO**

### **1.7.1. Objetivos Generales.**

- ✓ Estudio, Análisis y Comparación de tres herramientas para el salvaguardo de información.

### **1.7.2. Objetivos Específicos.**

- ✓ Crear calendarios diarios para la ejecución de tareas de protección de información.
- ✓ Generar un registro periódico sobre las actividades que se vienen realizando en cada uno de los servidores ya sea de fallas, errores o tareas cumplidas exitosamente.
- ✓ Permitir a los administradores del sistema de respaldos, visualizar eventos generados por las actividades de los servidores y estado del propio sistema.

- ✓ Permitir que la administración de la herramienta sea accesible desde la red interna a través de un acceso web y si lo solicita la Compañía poder acceder a la misma vía internet.
- ✓ Mejorar la forma de generar las tareas actuales de protección de información y la capacidad de generar más políticas de respaldos, si el caso lo amerita de manera fácil y rápida.
- ✓ Realizar las respectivas pruebas y dejar en funcionamiento para Sinergy Team.
- ✓ Generar material de entrenamiento por cada herramienta para que sea objeto de estudio dentro de la Facultad de Ingeniería en Ciencias Aplicadas.

### **1.7.3. De Estudio**

- ✓ Estudiar las herramientas más conocidas, para salvaguardo de información tanto de uso libre como propietarias.
- ✓ Analizar las ventajas y desventajas que existen al usar herramientas de aseguramiento de información.
- ✓ Estudiar y analizar los diferentes sistemas operativos soportados por las herramientas.
- ✓ Identificar la mejor opción en software de salvaguardo de la información para cumplir con los requerimientos y necesidades de la compañía.
- ✓ Estudiar y aplicar técnicas de retención de información, optimización de “backups” y “archives”.

## **1.8. ESTUDIO DE RIESGOS**

Un riesgo es una amenaza para el proyecto y para la empresa, es algo que puede ocurrir en la ejecución de un proyecto, que lo afecta de forma significativa.

El análisis de riesgos tiene su razón de ser ya que para el correcto desarrollo del proyecto y aplicar el mismo se debe considerar factores tanto internos como externos, los mismos que deben tener un límite de tolerancia donde poder moverse sin necesidad de llegar a cambios significativos en todo el proyecto en general.

Al poder delimitar los riesgos que se podrían presentar en el proyecto se reduce los mismos, en cada hito marcado del proyecto se realizará un análisis de metas propuestas, obtenidas y

retrasadas, las mismas que luego de ser objeto de estudio se determina qué tipo de inconveniente se suscitó para que exista un retraso principalmente en el proyecto.

Los riesgos que se pueden presentar dentro de nuestro análisis son los siguientes:

### 1.8.1. Tecnológico.

RIESGO	PROBABILIDAD	EFECTO/ IMPACTO	ESTRATEGIA
No se posee un canal dedicado (VLAN, o LAN), para respaldos.	Moderada	Moderada	Optimizar las programaciones respaldos para que se ejecuten fuera de horarios laborales.
El hardware necesario para el desarrollo del proyecto no está disponible.	Alta	Alto	Implementación por prioridad, iniciando con los servidores críticos de la empresa.
Adquisición de nuevos servidores, para realizar nuevas tareas en la empresa.	Alta	Moderado	Solicitar una identificación de prioridad si serán tomados en cuenta en el proyecto o no.
Las configuraciones por equipo tomarán más tiempo del planeado.	Moderada	Moderado	Terminar lo antes posible para solventar los retrasos.
No se dispone de un Servidor en el cual poder implementar el software de respaldos.	Alta	Alta	Realizar pruebas dentro de un ambiente virtualizado hasta solventar el tema.
No se puede definir que herramienta se implementará.	Alta	Alto	Realizar más estudios para definir la herramienta a implementar.
Las versiones utilizadas por las herramientas son remplazadas por nuevas y con nuevas características.	Baja	Bajo	Implementar nuevas versiones y estudiar las nuevas características.
Cambio de Servidores ya sea de versiones o de sistemas operativos instalados	Moderada	Bajo	Definir las actualizaciones a utilizar de las herramientas para poder ser compatibles con los nuevos cambios.
Base de Datos utilizada por las diferentes herramientas de respaldos, no soporta toda la información de la empresa.	Alta	Moderado	Diferenciar que herramientas pueden tener este inconveniente y remplazarla.
La cantidad de información presente en la empresa sobrepasa los límites asignados de espacio para respaldos y toman demasiado tiempo en ser respaldados.	Alta	Alta	Estudia el porcentaje de holgura para poder tener estas variables adecuadas para mediano y largo tiempo.

Tabla 1.2. Riesgo Tecnológico  
Fuente. Personal

### 1.8.2. Ambiental.

RIESGO	PROBABILIDAD	EFEECTO/ IMPACTO	ESTRATEGIA
Consumo excesivo de recursos energéticos en la implementación del proyecto.	Baja	Bajo	Generación de equipos virtuales de prueba antes de la implementación definitiva.
Uso excesivo de material de oficina, papel, impresiones, etc.	Baja	Bajo	Elaboración y diseños del proyecto digital, proyecto final imprimible.
Cambio de equipos, mal manejo de dichos equipos.	Baja	Bajo	Reutilizar partes y piezas, reciclando de ser posible el sobrante o realizando un buen manejo del desecho.
Control inexistente de emanación de estática de los equipos a ser utilizados.	Baja	Bajo	Crear un data center seguro y tomando en cuenta las medidas de seguridad recomendadas.
Control de Ruido, equipos excesivamente ruidosos.	Baja	Bajo	Crear un data center seguro y tomando en cuenta las medidas de seguridad recomendadas.
Posibilidad de incendio por sobre calentamiento de los equipos.	Moderada	Moderado	Crear un data center seguro y tomando en cuenta las medidas de seguridad recomendadas.
Instalaciones eléctricas defectuosas que aumenten el consumo de energía o puedan ocasionar accidentes.	Moderada	Moderado	Chequeo periódico de las instalaciones eléctricas para precautelar su correcto funcionamiento.

**Tabla 1.3. Riesgo Ambiental**  
Fuente. Personal

### 1.8.3. Laboral.

RIESGO	PROBABILIDAD	EFECTO/ IMPACTO	ESTRATEGIA
No se dispone del personal con el conocimiento necesario para el manejo de las herramientas.	Moderado	Alto	Capacitaciones constantes durante todo el proceso de implementación.
Ausencia por enfermedad del personal que apoya en el desarrollo del proyecto.	Alto	Alto	Entrevistas detalladas optimizando tiempo y requisitos.
Falta de motivación y de entusiasmo en el personal a cargo de proporcionar información para el desarrollo del proyecto.	Alto	Alto	Generar motivación a través de dar a conocer las ventajas y ayuda que dará la correcta implementación de la herramienta.
Falta de compromiso en la ejecución de tareas de verificación del proyecto.	Alto	Alto	Crear un listado de tareas con un único responsable por el cumplimiento de ellas.
Información no precisa o faltante sobre todo el nivel de respaldos necesarios.	Alto	Alto	Establecer varias reuniones de trabajo, con cada uno de los implicados en el manejo de servidores.
Falta de conocimiento de que servidores y datos se deben respaldar.	Alto	Alto	Establecer informes diarios por el lapso de 15 días, para registrar el funcionamiento de la Empresa.
Inexistencia de procesos de respaldos	Bajo	Bajo	Análisis de cada uno de procesos de los servidores y establecer las tareas de respaldo.
Falta de personal dedicado para el manejo y administración de la herramienta.	Alto	Alto	Definición de roles para los empleados y poder tener varios administradores y operadores, con el personal disponible.
Personal con experiencia abandona la Empresa.	Alta	Medio	Generación de documentación sobre el manejo de toda la infraestructura

**Tabla 1.4. Riesgo Laboral**  
Fuente. Personal

#### 1.8.4. De las Herramientas.

RIESGO	PROBABILIDAD	EFECTO/ IMPACTO	ESTRATEGIA
La o las herramientas dejan de ser soportadas por el fabricante.	Bajo	Alto	Verificar con el fabricante los documentos (roadmap) para conocer el tiempo que tendrá soporte las versiones seleccionadas de las herramientas.
No existe soporte para poder realizar consultas o reporte de errores en problemas encontrados.	Moderado	Moderado	Identificar herramientas exactas con soporte y documentación para poder solventar este detalle.
Cambio de versiones de las elegidas en un inicio.	Moderado	Moderado	Verificar características nuevas y analizar si son aplicables y estables.
No soportan los sistemas operativos y/o aplicativos presentes en la empresa.	Bajo	Alto	Realizar un estudio y análisis previo de las bondades de cada herramienta.
La herramienta es muy compleja y causa problemas su administración.	Moderado	Moderado	Fortalecer conocimientos mediante el uso de manuales y documentos de implementación de las herramientas.
La herramienta no soporta la carga transaccional derivada del proceso de salvaguardo de información.	Moderado	Alto	Análisis de las características y rendimiento de las herramientas.
La herramienta tiene un límite de crecimiento tanto para los servidores que se pueden configurar como para la cantidad de información que se puede administrar.	Moderado	Alto	Acorde a las especificaciones se puede determinar si la herramienta es apta para el negocio.
El costo de adquisición de licencias sobrepasa el presupuesto establecido.	Alto	Alto	Realizar adquisiciones paulatinas de ser el caso, solicitar opciones de financiamiento.
No existe información o documentos que puedan ayudar en el proceso de instalación y configuración de las herramientas.	Alto	Alto	Identificar herramientas exactas con soporte y documentación para poder solventar este detalle.

Tabla 1.5. Riesgo de las Herramientas  
Fuente. Personal

### 1.8.5. De los Requerimientos.

RIESGO	PROBABILIDAD	EFECTO/ IMPACTO	ESTRATEGIA
Habr� m�s cambios de requerimientos de los esperados.	Moderada	Bajo	Verificar la factibilidad de los nuevos requerimientos y aplicarlos de ser el caso.
El tama�o del Proyecto se ha Subestimado	Alta	Alto	Acoplar los requerimientos nuevos paso a paso.
La planificaci�n no incluye las tareas necesarias para solventar las necesidades de respaldos.	Moderada	Moderado	Aumentar detalles de generaciones de respaldos para solventar las necesidades.
Las planificaciones autom�ticas de respaldos generan colisiones y fallas entre s�.	Bajo	Bajo	Luego de la implementaci�n se contempla un periodo de revisi�n y correcci�n de 30 d�as para eliminar estos detalles.
Los periodos de retenci�n de informaci�n hacen que crezcan los respaldos de manera exponencial.	Bajo	Bajo	El an�lisis de requerimientos conjuntamente con las mejores pr�cticas de configuraci�n solventa este problema.
El n�mero de versiones que se est�n manteniendo no est� direccionado a cada tarea que realizan los servidores.	Bajo	Bajo	El an�lisis de requerimientos conjuntamente con las mejores pr�cticas de configuraci�n solventa este problema.
Los servidores que est�n tomados en cuenta para respaldos, cambian de aplicaci�n y/o cambian de sistema operativo.	Moderado	Moderado	Se verifica si las aplicaciones y sistemas operativos son soportadas de serlo se proceder a configurarlas.
El espacio especificado para la instalaci�n de la herramienta de salvaguardo de informaci�n, es demasiado peque�o.	Moderado	Moderado	La estad�stica de crecimiento puede indicarnos el tama�o a asignar de espacio por herramienta acorde tambi�n a requerimientos del fabricante.
Pol�ticas de respaldo a�n no definidas, para ser aplicadas por cada servidor o por cada grupo de servidores presentes en la empresa y que se proceder� a generar respaldos.	Moderado	Moderado	En la definici�n del proyecto se toma en cuenta esta informaci�n la misma que puede cambiar y ajustarse en el transcurso del tiempo.

Tabla 1.6. Riesgo de Requerimientos  
Fuente. Personal

## 1.9. VALORACIÓN DE CADA UNO DE LOS RIESGOS.

TIPO DE RIESGO	IDENTIFICADOR POTENCIAL
TECNOLÓGICO	Numero de problemas tecnológicos reportados, numero de entregas retrasadas de hardware y/o software.
AMBIENTAL	Contaminación por ruido, desperdicios o por uso excesivo de energía.
LABORAL	Malas relaciones para con el equipo de trabajo, disponibilidad de nuevo empleo.
HERRAMIENTAS	Mala elección de herramientas, características inferiores a los requerimientos que necesita la empresa.
REQUERIMIENTOS	Levantamiento de requerimientos, no acorde con las necesidades de la empresa, definiciones faltantes para salvaguardar la información.

Tabla 1.7. Valoración de Riesgos  
Fuente. Personal

La tecnología para este caso seleccionada es “Abuelo, padre e hijo”, ya que por necesidades de la empresa y las programaciones establecidas se necesitan respaldos completos y diferenciales.

La otra configuración aplicable es conocida como “Incremental Forever”, donde se ejecutan en el lapso de un año hasta tres respaldos completos y los siguientes respaldos serán incrementales.

## 1.10. SOLUCIONES Y BENEFICIOS QUE SE LOGRA CON LA IMPLEMENTACIÓN DE LA HERRAMIENTA

Mediante el estudio e implementación de una herramienta que pueda manejar y optimizar los respaldos de la infraestructura presentada se puede obtener lo siguiente:

- ✓ Creación de tareas calendarizadas, adicionando un log de registro por cada una de ellas.
- ✓ Control de respaldos que se realizan o no, dentro de un informe desde la herramienta.
- ✓ Administración centralizada de respaldos.
- ✓ Creación de políticas, que afecten a todos o cada uno de los servidores.
- ✓ Manejo de versionamiento para cada respaldo.
- ✓ Políticas de Migración automática para utilizar diferentes medios de almacenamiento.
- ✓ Posibilidad de escalamiento conjuntamente con el cliente y su infraestructura.
- ✓ Capacidad de conectividad nativa con los servidores para generar respaldos “ON-LINE”
- ✓ Manejo de unidades de cintas.
- ✓ Monitoreo de medios de almacenamiento para identificar falta de espacio.
- ✓ Capacidad de encriptar los datos de ser necesario.
- ✓ Recuperación rápida ante desastres.

## CAPÍTULO 2.



## ESTUDIO DE LAS HERRAMIENTAS DE SALVAGUARDO DE INFORMACIÓN

## **2.1. DEFINICIÓN DE SALVAGUARDO DE INFORMACIÓN**

La definición de Salvaguardo tiene que ver con defender o proteger a una persona o cosa, las autoridades deben salvaguardar los derechos de los ciudadanos, salvaguardar defender, proteger información, realizar una copia de seguridad, en este caso tomamos como punto de partida la información, el concepto de proteger viene al caso ya que con el uso de estas herramientas lo que se intenta realizar es proteger, defender la información perteneciente a los servidores de la organización, tales como Servidores de Archivos, Servidores de Correo, Servidores de Aplicaciones, etc.

Hoy en día el manejo de información se ha visto como una prioridad más que en épocas pasadas ya que la era de la tecnología ha crecido de manera exponencial, los servidores de hace unos 10 años atrás manejaban información a razón de Megabits o incluso en empresas bastante grandes llegaban a los Gigas de información, hoy por hoy ese tamaño se ha visto triplicado, lo que ha dado como resultado la aparición de nuevas tecnologías de almacenamiento como son las unidades de tape LTO 3, LTO4 y por el momento LTO5, medios de almacenamiento llamados “Storage” que pueden albergar Teras de información con esto se ha solventado en gran medida las necesidades del cliente.

Como los sistemas de computadora central estaban haciendo la transición de las máquinas colosales a los sistemas más personalizado y controlable, los administradores de TI carecían de la capacidad para administrar los entornos complicados. En estas "anticuadas" veces, los administradores de sistemas que dedicar un tiempo fuera de las horas y los fines de semana para ejecutar los programas de copia de seguridad. En el nuevo mundo en red, los administradores de TI necesitan para reducir significativamente la ventana de copia de seguridad de datos que requieren comenzaron a multiplicarse más rápido que nunca.

Los aplicativos y aplicaciones que constituyen una parte del “Core del Negocio”, de igual manera en su evolución requieren muchos más requerimientos de hardware, ya sea de velocidad de procesamiento o de almacenamiento.

En tal virtud siguiendo la línea de evolución de la información se necesita herramientas capaces de manejar tanto el volumen de información como los medios donde serán

almacenados, cumplir con normas o políticas internas de las diferentes organizaciones o regulaciones del gobierno.

A principios de 1993, sólo había cincuenta servidores web que operan en todo el mundo. Con la explosión de la World Wide Web, ese número aumentó a más de 30 veces en el curso de 18 meses, sin dejar de acelerar la actualidad a un ritmo que es virtualmente imposible de rastrear. Hoy en día el poder de las tecnologías de Internet, junto con la proliferación de dispositivos de comunicación, permite a las personas conectarse con prácticamente cualquier persona, a cualquier hora - con poco o ningún costo. Una idea que parecía incomprendible para la mayoría de nosotros hace diez años.

Para tener una idea de la industria del almacenamiento que existía en la década de 1990, hay que considerar que la red de área de almacenamiento (SAN) no se había inventado. La mayoría de las empresas se basaron en mainframes, mientras que, hoy en día, las redes son construidas sobre servidores escalables basados en Intel con Windows, Unix o Linux son mucho más frecuentes. Las empresas estaban empezando a enfrentarse con el hecho de que la información importante a sus negocios ya no se almacena de forma centralizada, sino que se distribuye a los sistemas que no estaban bajo el control central. Cada año durante la última década, la empresa media ha duplicado la cantidad de almacenamiento que requiere, y de acuerdo con Firma de analistas Gartner, el software de copia de seguridad fue el de software empresarial más comprados el año pasado.

NOMBRE	FECHA	CARACTERÍSTICAS	RESPALDOS
<b>1ra. Generación</b>	1940 - 1958	Funcionaban por medio de tubos al vacío. Utilizaban programas escritos en lenguaje de bajo nivel. Su velocidad de procesamiento se medía en milisegundos. Producir un millón de cálculos costaba \$200.00 Dólares.	Inexistentes.
<b>2da. Generación</b>	1959 - 1965	Su velocidad de procesamiento se calculaba en microsegundos. Sus Programas se escribían en lenguaje simbólico. Su capacidad de almacenamiento interno oscilaba entre 16,000 y 18,000 caracteres	Inexistentes.
<b>3ra. Generación</b>	1965 - 1970	Requerían menos energía eléctrica Su velocidad de procesamiento se	Respaldos dedicados utilizando el mismo

		media en nanosegundos. Utilizaban un método de organización que permitía que el usuario acceda a la información directamente en cualquier momento.	equipo y manteniéndolos como tipo espejo del mismo.
<b>4ta. Generación</b>	1971 - 1981	Dispositivos de entrada/salida extremadamente rápidos. Requerimientos de electricidad muy bajos. Velocidad de cálculo en picosegundos.	Aparecen los primeros indicios de utilización discos magnéticos.
<b>5ta. Generación</b>	1982 - 1989	Conectividad entre computadoras. Surgimiento de la PC como se conoce hoy en día. El almacenamiento se lo realiza en discos magnéticos.	Respaldos realizados a discos magnéticos, siendo no tan confiables y no siempre disponibles.
<b>6ta. Generación</b>	1990 - Hoy	Cuentan con arquitectura paralelo/vectorial. Capacidad de realizar más de un millón de operaciones aritméticas. Almacenamiento en discos rígidos. Comunicación vía internet.	Uso de herramientas especializadas para respaldos y que pueden utilizar el hardware disponible.

**Tabla 2.1. Evolución de Equipos Informáticos**  
Fuente: Propia

De estas circunstancias cada organización toma en cuenta cuán crítico es respaldar o no su información y si después de una pérdida grave de información está en la capacidad de solventar la continuidad del negocio.

Tres son las principales áreas o conceptos para el almacenamiento: el back-up (almacenamiento de corto-tiempo), archiving (almacenamiento de largo tiempo) y disaster recovery. Entre el backup y el archiving ubicamos al almacenamiento near-line el cual se usa, en entornos NAS (Network Attached Storage) y SAN (Storage Area NetWork).

Backup significa hacer copias de archivos almacenados originalmente en discos rígidos. El backup es necesario para recuperar archivos perdido o dañados o para recuperar un sistema que ha caído. Los archivos que se almacenan para backup son redundantes y no están hechos como copias sobre las que se está trabajando.

Archiving significa copiar uno o más archivos sobre el CD/DVD/Cinta, para almacenar por un largo período de tiempo, ya sean por cuestiones legales o para hacer espacio en el disco.

Disaster recovery significa recuperar desde una situación en la que el sistema está fuera de servicio. Se requiere entonces el backup guardado off-site a partir del cual puede recuperarse gran parte y hasta todo el sistema

Un backup total debería siempre guardarse en un lugar seguro (off-site).

Con un backup diferencial, se almacenan los datos modificados después del último backup total realizado. (Se almacena el documento en su versión original y el documento modificado)

Con el backup incremental, se almacenan todos los datos modificados desde el último backup total, diferencial o incremental (se almacenan sólo los datos modificados desde el último backup). El backup incremental es más veloz pero la recuperación de datos desde una serie de backups incrementales será más lenta.

En tal caso se pone en consideración el estudio de las siguientes herramientas.



Figura 2.1. Almacenamiento de Respaldos  
Fuente: [Web 1]

## 2.2. AMANDA SOURCE BACKUP

Amanda Source Backup "Archivador de Disco de Red Automatizado Avanzado de Maryland" (Advanced Maryland Automated Network Disk Archiver), es una solución robusta y completa de respaldo y recuperación de código abierto. Con Amanda Source usted puede crear un servidor de respaldo para respaldar múltiples servidores de Linux, Windows, Solaris y MAC OS en cintas magnéticas, discos duros o storage clouds.

Amanda fue escrito originalmente por James da Silva del Departamento de Ciencias de Computación de la Universidad de Maryland en 1992. El objetivo era crear un sistema capaz de hacer copias de seguridad de múltiples clientes en una única máquina servidora de copias de

seguridad. Es una utilidad de dominio público. Es tan avanzado como lo puede ser una utilidad gratuita de copias de seguridad, y cuenta con un gran número de usuarios.

Se usa para hacer copias de seguridad (backups). Amanda permite establecer un único servidor de copias de seguridad (server Linux) para salvaguardar datos de múltiples máquinas en un mismo dispositivo de copia. Amanda puede usar diferentes programas para realizar las copias, tales como programas de copia comerciales o el simple GNUtar y puede hacer copias de un gran número de estaciones clientes corriendo múltiples versiones de Unix. Las versiones más recientes de Amanda también pueden usar Samba para hacer copias de máquinas Windows (95/98/NT/2000/XP/VISTA/7) en el servidor.

Es decir, Amanda permite salvaguardar de forma automatizada la información importante de la red, ya esté ubicada en el servidor central, o en los clientes Windows/Unix.

### **2.2.1. Componentes de Amanda Source Backup.**

Los componentes de Amanda Source Backup para proceder con la implementación son los que se detallan a continuación:

- ✓ GNU tar 1.12 o superior (<http://www.gnu.org>)  
La versión GNU del programa "tar" con capacidades para realizar copias parciales y omitir los ficheros seleccionados. Este es uno de los programas clientes de realización de copias que Amanda sabe utilizar.
- ✓ Samba 1.9.18p10 o superior (<http://www.samba.org>, y la "Traducción del Manual de Samba", en S.O.B.L.)  
Samba es una implementación del protocolo "System Message Block" (SMB) usado por los sistemas basados en Windows para el acceso a ficheros. Contiene una herramienta, "smbclient", que Amanda puede usar para realizar copias a través de Samba.
- ✓ Perl 5.004 o superior (<http://www.perl.org>)  
Perl es un lenguaje de programación tipo script, orientado a la administración de sistema y la manipulación de textos. Es usado por una serie de herramientas de informes de Amanda y por algunos intercambiadores de cintas.

- ✓ GNU readline 2.2.1 o superior (<http://www.gnu.org>)  
La librería "GNU readline" puede ser incorporada para su uso por programas interactivos, para proporcionar históricos de línea de comando y para edición. Se crea en la herramienta de restauración de Amanda "amrecover", si está disponible.
- ✓ GNU awk 3.0.3 o superior (<http://www.gnu.org>)  
La versión GNU del lenguaje de programación "awk" contiene una versión común a plataformas y algunas características adicionales.
- ✓ Gnuplot 3.5 o superior (<ftp://ftp.dartmouth.edu/pub/gnuplot/>)  
Esta librería "gnuplot" (que no tiene nada que ver con las herramientas GNU) es un paquete gráfico de impresión. Se usa por la herramienta opcionalmente para estadísticas de Amanda "amplot".

Se debe asegurar de buscar en el directorio de parches de Amanda y de mirar en la sección de parches de la página web, para posibles necesidades de actualizaciones de estos paquetes. Las versiones de Samba anteriores a la 2.0.3, en particular, deben ser parchadas para que funcionen correctamente con Amanda. Sin estos parches, las copias de seguridad parecerán que se están realizando correctamente, pero las imágenes resultantes estarán corruptas.

Cuando Amanda es configurada, las localizaciones de software adicional usado en los clientes, tales como GNU tar y Samba, se incorporan a los programas de Amanda, de forma que el software adicional debe ser instalado en el mismo sitio donde se encuentra instalada Amanda y en todos los clientes.

### **2.2.2. Características de Amanda Source Backup.**

- ✓ Amanda simplifica la vida de un administrador del sistema que pueden fácilmente configurar un único servidor de copia de seguridad de varios clientes en red a una cinta o un disco basado en sistema de almacenamiento.
- ✓ Amanda está bien documentado y se puede configurar muy rápidamente.

- ✓ Amanda ofrece la capacidad única de escribir copias de seguridad en cinta y disco al mismo tiempo. Los mismos datos podrían estar disponibles en línea para recuperaciones rápidas de un disco y fuera de sitio para recuperación de desastres y retención a largo plazo.
- ✓ Dado que Amanda no usa drivers propietarios de dispositivos, un dispositivo con el apoyo de un sistema operativo funciona bien con Amanda. El administrador del sistema no tendrá problemas al actualizar Amanda.
- ✓ Amanda utiliza volcado nativo y/o utilidades GNU tar. Dado que no existen formatos propietarios, en caso de emergencia, los datos podrían ser recuperados con las utilidades de nativos, independientemente de si Amanda está instalada o no.
- ✓ Amanda es muy seguro. Cifrado en el cliente garantiza la seguridad de los datos en tránsito y cifrado en el servidor de copia de seguridad garantiza la seguridad de los datos en reposo, por ejemplo, en una cinta o en una nube. Amanda soporta hasta 4096 bits con claves de criptografía de clave pública, así como encriptación 256-bit AES.
- ✓ Un único programador optimiza el nivel de seguridad para los diferentes clientes de tal manera que el tiempo de copia de seguridad total es de aproximadamente el mismo para cada ejecución de copia de seguridad. Amanda libera a los administradores de sistemas de tener que adivinar el tipo de cambio de datos en sus entornos.
- ✓ Amanda es estable y robusta, ya que el código es de alta calidad.
- ✓ El Proyecto Open Source Amanda tiene una gran comunidad y productividad que crece día a día.
- ✓ AMANDA se ha diseñado para manejar gran cantidad de clientes y datos, y aun así es razonablemente simple de instalar y mantener. Se escala bien, así que

pequeñas configuraciones, aún el caso de un sólo equipo, son posibles. El código es portable a un gran número de plataformas Unix.

- ✓ AMANDA proporciona sus propios protocolos de red sobre TCP y UDP. No usa, por ejemplo, rsh o rdump/rmt. Cada programa cliente de copia de seguridad es instruido para grabar a la salida estándar, donde AMANDA recoge y transmite los datos copiados al servidor de cintas. Esto permite a AMANDA insertar compresión y encriptación y además mantener un catálogo de la imagen para su posterior recuperación.
- ✓ AMANDA soporta usar más de una cinta en una misma ejecución, pero no divide una imagen de copia entre varias cintas. Esto significa que no soporta imágenes de copias mayores que el tamaño de una cinta. AMANDA actualmente inicia una nueva cinta por cada ejecución y no proporciona un mecanismo para añadir una nueva ejecución a la misma cinta como la ejecución previa, lo cual puede ser un problema en las pequeñas configuraciones.
- ✓ AMANDA soporta una amplia variedad de dispositivos de cinta. Usa operaciones básicas a través del subsistema de E/S normal del sistema operativo y una simple definición de características. Los nuevos dispositivos son muy fáciles de incorporar. Varios cambiadores de cintas, apiladores, y robots están soportados para proporcionar una operatividad 'sin manos'. El interfaz del cambiador es externo a AMANDA y está bien documentado, así que se pueden añadir cargadores no soportados sin mucho esfuerzo.
- ✓ Tanto el cliente como el servidor pueden hacer compresión por software, o bien se puede usar la compresión por hardware. En la parte del cliente, la compresión por software reduce el tráfico de red. Por la parte del servidor, se reduce la carga de CPU de cliente. Si Kerberos está disponible, los clientes pueden usarlo para autenticación y las copias se pueden encriptar. Sin Kerberos, se usa la autenticación desde el fichero .amandahosts (similar a .rhosts), o bien AMANDA puede ser configurado para usar .rhosts (aunque rsh/rlogin/rexec no es usado). AMANDA trabaja bien con herramientas de seguridad como los TCP Wrappers y los cortafuegos, o firewalls. Como se usa software estándar para generar imágenes

de copias y compresión por software, sólo las herramientas típicas como mt, dd, y gunzip/uncompress son necesarias para recuperar una imagen de una copia desde la cinta si AMANDA no está disponible. Cuando el software de AMANDA está disponible, éste localiza qué cintas son necesarias y encuentra las imágenes en las cintas.

- ✓ AMANDA está preparado para funcionar en modo desatendido, como por ejemplo en forma de tarea nocturna desde cron. Las máquinas clientes que no se encuentran disponibles o están apagadas son anotadas y saltadas. Errores en las cintas provocan que AMANDA pase a modo degradado, donde las copias se siguen realizando, pero sólo en los discos de almacenamiento. Pueden pasarse luego a cinta manualmente cuando se resuelva el problema.
- ✓ AMANDA tiene opciones de configuración para controlar casi todos los aspectos de la operación de copia, y proporciona varios métodos de programación de tareas.

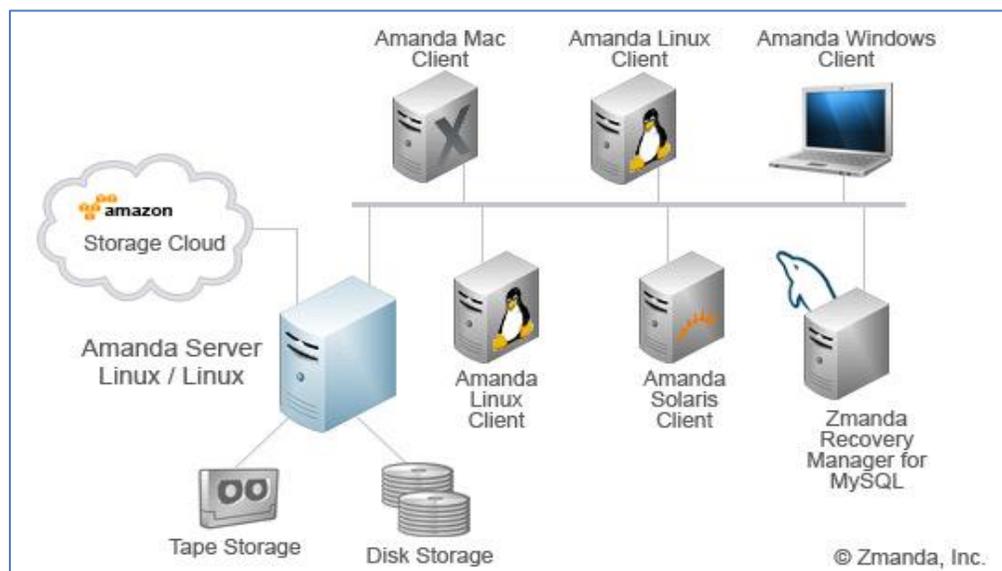


Figura 2.2. Ambiente de Amanda

Fuente: [Web 2]

### 2.2.3. *Como Funciona Amanda Source Backup.*

AMANDA fue diseñada en la filosofía de la introducción de unidades de cinta de gran capacidad, tales como las ExaByte de 8mm y las DAT de 4mm. Con estos dispositivos y el incremento de las estaciones de trabajo personales ya no tiene sentido hacer copias de seguridad individuales de cada máquina en dispositivos separados. La coordinación de los accesos y el proporcionar entendimiento con el hardware de cintas supuso un gran coste y esfuerzo. Una solución típica a este problema era sacar al cliente del host de cintas y copiar las áreas una a una a través de la red. Pero esto normalmente no lo soportaba el dispositivo de cintas, y se traducía en una caída del rendimiento.

La idea de AMANDA es usar un 'disco de almacenamiento' en el servidor de cintas, hacer varias copias en paralelo hacia ficheros en el disco de almacenamiento y tener a un proceso independiente tomando datos hacia el disco de almacenamiento. Como la mayoría de las copias son partes pequeñas del total, incluso una cantidad modesta de espacio en el disco de almacenamiento puede proporcionar un flujo casi óptimo de imágenes del proceso de copia hacia la cinta.

AMANDA también se aproxima a las copias programadas. Un dump cycle o ciclo de copia se define para cada área para controlar el tiempo máximo entre copias completas. AMANDA toma esa información, estadísticas sobre rendimientos de copias anteriores, y estima el tamaño de las copias para decidir qué nivel de copia usar. Esto se aleja de la estética tradicional. Por ejemplo es viernes, así que se realiza un copia completa del directorio /usr en el cliente A y permite a AMANDA balancear las copias, así que el total del tiempo de ejecución es aproximadamente constante de un día a otro.

Imaginemos la siguiente situación: somos los administradores de una red de 30 puestos, todos ellos clientes Windows de un servidor Linux. Los clientes Windows almacenan sus documentos importantes en la carpeta "Mis Documentos", y no quieren la responsabilidad de tener que hacer copias de seguridad de su información. Esa red de 30 puestos está servida por una máquina Linux que, entre otras muchas cosas, les da salida a Internet, correo interno/externo, acceso a ficheros de la empresa ubicados en el servidor Linux desde las máquinas windows (a través de Samba), etc. Esa máquina Linux dispone de una unidad de cinta, con suficiente espacio para almacenar tanto los

contenidos del servidor como los de las carpetas "Mis Documentos" de los clientes. Pues bien, con Amanda se puede programar la copia de toda esa información. Además, se puede automatizar, añadiendo una simple orden en el crontab del servidor.

AMANDA usa un sistema de gestión de cintas simple y lo protege de la sobre escritura de cintas que todavía tienen imágenes de copias válidas, así como de cintas no localizadas en la configuración. Las imágenes pueden ser sobrescritas cuando un cliente está apagado durante un período de tiempo largo o si no se localizan suficientes cintas, pero sólo después de que AMANDA haya enviado varios avisos.

AMANDA también puede ser programada para que no reutilice determinadas cintas. Se puede usar un programa de validación antes de cada ejecución para detectar posibles problemas durante las horas de trabajo, cuando estos son fáciles de corregir.

Un reporte de actividad es enviado vía e-mail tras cada ejecución. AMANDA puede también enviar un reporte a una impresora y generar etiquetas para las cintas. No existe un interfaz gráfico. Para la administración, sólo hay que editar un simple fichero de texto, así que esto no es un problema. Por razones de seguridad, AMANDA no soporta recuperación de datos por parte de cualquier usuario. Hay una utilidad tipo ftp de restauración para que los administradores (root) hagan búsquedas en línea por los catálogos y recuperen información.

#### ***2.2.4. Tratamiento de la Información***

Una configuración típica realiza copias completas periódicas con copias parciales entre medio. También hay soporte para:

- ✓ Archivado Periódico de Copias, tales como pasar copias completas a un sitio secundario desde el sitio principal.
  
- ✓ Copias sólo incrementales, donde las copias completas se realizan fuera de AMANDA, tales como áreas muy activas que deben ser tomadas fuera de línea, o copias no completas para áreas que pueden ser recuperadas desde dispositivos comerciales.

- ✓ Hacer siempre copias completas, tales como áreas de bases de datos que cambian completamente entre cada ejecución, o áreas críticas que son más sencillas de manejar durante una emergencia si están en una operación de restauración simple.

Es sencillo soportar múltiples configuraciones en el mismo servidor de cintas, tales como configuraciones periódicas de almacenamiento al lado de una configuración diaria normal. Se pueden ejecutar múltiples configuraciones simultáneamente en el mismo servidor de cintas si hay múltiples unidades de cinta.



Figura 2.3. Proceso de Respaldos

Fuente: [Web 3]

La programación de copias completas se deja normalmente a cargo de AMANDA. Estas se reparten a lo largo del ciclo de copia para compensar la cantidad de información copiada en cada ejecución. Es importante mantener registros de dónde están las imágenes de las copias para cada área (lo cual AMANDA hace automáticamente), ya que no están en una específica, predecible, cinta (p.e., la cinta del Viernes no siempre tiene una copia completa de /usr para el cliente A). El nivel de copia parcial también queda para AMANDA. Se mantiene información histórica de los niveles anteriores, y el nivel de copia se incrementa automáticamente cuando se realiza una copia de un tamaño suficiente.

### 2.2.5. Evolución de Amanda Source Backup.

Característica	Comunidad	Empresarial
Centralizado de copias de seguridad completas e incrementales	Y	Y
Linux y UNIX de apoyo	Y	Y
Windows Server y soporte de escritorio	Y	Y
Mac OS X Soporte	Y	Y
Inteligente Backup Scheduler	Y	Y
Copia de seguridad en disco (NAS, SAN, iSCSI, Cloud Storage, “Solo Versión Network”)	Y	Y
Copia de seguridad para unidades de cinta, bibliotecas de cintas y VTL	Y	Y
Bóveda y de disco a disco a cinta (D2D2T)	Y	Y
Formatos abiertos para el archivado a largo plazo	Y	Y
Cifrado y compresión de los archivos de copia de seguridad	Y	Y
Certificación de Security Enhanced Linux (SELinux)	N	Y
Live Backup de Oracle	N	Y
Live Backup de SQL Server, Exchange y SharePoint	N	Y
Seguridad de las imágenes en vivo de máquinas virtuales VMware base	N	Y
NDMP basada copias de seguridad de dispositivos NAS	N	Y
Consola de administración web	N	Y
Copia de seguridad de informes	N	Y
Administración basada en roles	N	Y
Guiada por un asistente de instalación	N	Y
Replication Server Backup (DR a un sitio remoto)	N	Y

<b>Apoyo a la Producción 24x7</b>	N	Y
<b>Servicios Profesionales y Formación</b>	N	Y

Tabla 2.2. Comparativa de Versiones de Amanda

Fuente: Propia

En adición a las mejoras y depuración de errores constantemente realizada por el equipo de desarrollo de AMANDA, tres cambios principales se encuentran en varios estados de desarrollo:

- ✓ Un nuevo almacén de seguridad interior hará más sencillo a los desarrolladores añadir otros métodos de seguridad, tales como SSH (<ftp://ftp.cs.hut.fi/pub/ssh/>) y SSL (Secure Socket Layer).
- ✓ Otro proyecto mayor es la redefinición de cómo AMANDA ejecuta el programa de copia del cliente. Esto actualmente se realiza con un programa comercial, GNU tar o SAMBA tar. El nuevo mecanismo permitirá el uso de programas arbitrarios como cpio, star, y también otros sistemas de copias de seguridad.

También añade pasos opcionales pre y post copia, que pueden ser usados para bloqueos/desbloqueos, e instantáneas de datos rápidamente cambiados tales como bases de datos o el registro de Windows.

El tercer mayor proyecto es una redefinición del subsistema de salida para soportar dispositivos distintos a cintas, tales como CD-ROM, ficheros locales, ficheros remotos vía herramientas como rcp y ftp, cintas remotas, etc.

También podrá dividir imágenes de copias entre dispositivos, manejar al mismo tiempo y de forma simultánea dispositivos de diferentes tipos, tales como grabar a múltiples cintas o a una cinta y un CD-ROM, y manejar la grabación de copias de imágenes a múltiples dispositivos, tales como una cinta, para mantener un sitio, y un CD-ROM o una cinta duplicada para archivado.

En adición, el formato de salida será mejorado para incluir un fichero-1 y un fichero-n. La idea es poner herramientas de recuperación de emergencia en el fichero-1 (el primer fichero en la salida) que puedan ser recuperados fácilmente con programas como estándar del sistema como tar, y entonces usar estas herramientas para recuperar el

resto de la información. El área del fichero-n es el último fichero en la salida y puede contener elementos como la base de datos de AMANDA.

#### **2.2.6. Generación de Material de Entrenamiento.**

**Revisar Anexo A**

### **2.3. TIVOLI STORAGE MANAGER.**

Tivoli Storage Manager (TSM), o más recientemente llamado IBM Tivoli Storage Manager (ITSM) es un software centralizado y basado en políticas que permite la administración de los recursos de almacenamiento.

TSM surge de una necesidad para el DataSave de estaciones de trabajo (WDSF) del proyecto realizado en el Almaden Research Center de IBM en 1990. Propósito original WDSF era una copia de seguridad de PC / DOS, OS / 2, AIX y los datos de estación de trabajo en una MVS (y más tarde VM / CMS) del servidor.

La base de datos de TSM v5.5 tiene un límite de arquitectura de aproximadamente 530GB de espacio de base de datos y 13GB de espacio de registro. Aunque la base de datos de Tivoli Storage Manager utiliza muchas de las mismas tecnologías subyacentes como DB2 de IBM, tiene un motor SQL (aunque para el acceso de lectura solamente), y soporta el acceso a través de ODBC, que utiliza una base de datos personalizada a través de la versión 5.5. A partir de Tivoli Storage Manager 6.1, lanzado en mayo de 2009, TSM utiliza una instancia de DB2 como base de datos. Esto elimina los límites de la arquitectura anterior.

Este software es parte de la serie IBM TotalStorage y no tiene relación con Tivoli Framework. Previamente se conocía como ADSTAR Distributed Storage Manager (ADSM).

ADSTAR (almacenamiento y recuperación automatizada de documentos) era el nombre de la división de hardware de almacenamiento de IBM en 1992. ADSTAR fue vendida a Tivoli Systems, Inc. , pero más tarde fue comprado por el Tivoli de IBM. ADSTAR es conocida principalmente por sus tareas de “*BACKUP*” y “*RESTORE*” del producto llamado Administrador de ADSTAR Distributed Storage .

Gestión ADSTAR Distributed Storage (ADSM) es un término colectivo para la familia de IBM de alta gama de software que ayuda a un cliente gestionar los dispositivos de almacenamiento (por ejemplo, centrales de almacenamiento, unidades de disco de PC, y las unidades Zip) que se encuentran diseminados por la empresa.

ADSM ayuda a las empresas medianas y grandes a generar de forma automática copias de seguridad de la información empresarial en todos los dispositivos de almacenamiento en toda la empresa. ADSM software trabaja con una variedad de formatos de base de datos, incluyendo las realizadas por los competidores de IBM.

La premisa básica detrás de ADSM es permitir a los clientes ver y gestionar el almacenamiento como un esfuerzo único y global. La idea es permitir a los clientes una copia de seguridad de nivel empresarial, en lugar de tener que guardar todos los datos que residen en todos los equipos, redes y otras máquinas a través de una empresa en cada lugar.

IBM ya no distribuye el software ADSM. En su lugar, IBM y su filial de Tivoli comercializa Tivoli Storage Manager como el sucesor ADSM.

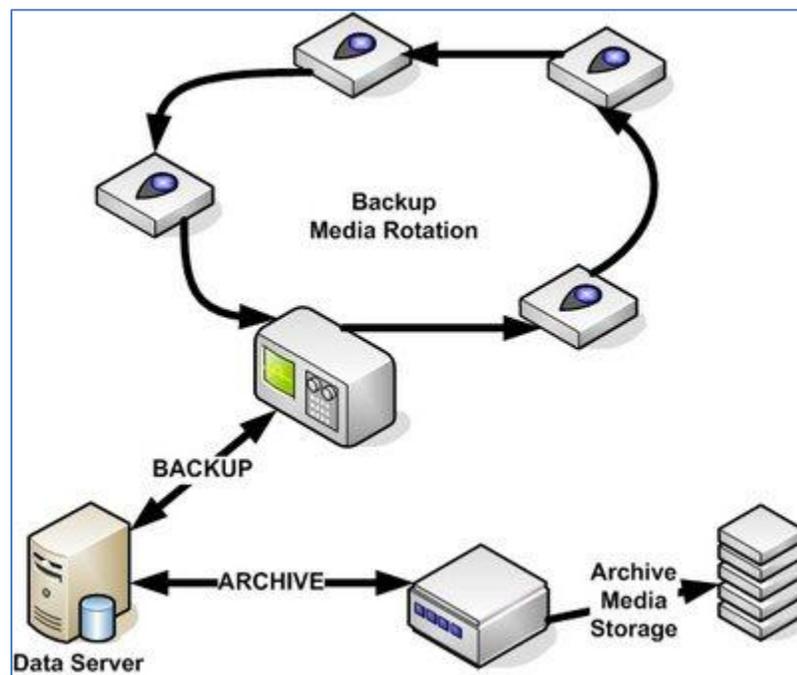


Figura 2.4. Diagrama de Respaldos Genérico

Fuente: [Web 4]

### 2.3.1. Componentes de Tivoli Storage Manager.

Tivoli Storage Manager como un sistema se compone de varios componentes diferentes. Los principales componentes de Tivoli Storage Manager incluyen:

✓ Programa servidor.

El programa servidor proporciona servicios de copia de seguridad, de archivado y de gestión de espacio a los clientes. En la red de la empresa puede establecer varios servidores para equilibrar los recursos de almacenamiento, de procesador y de red.

✓ Interfaz de administración.

La interfaz de administración permite a los administradores controlar y supervisar las actividades del servidor, definir políticas de gestión para clientes y configurar planificaciones para proporcionar servicios a clientes de forma periódica. Las interfaces de administración disponibles incluyen un cliente de administración de línea de comandos y una interfaz de navegador Web denominada Centro de administración. Tivoli Storage Manager permite gestionar y controlar varios servidores desde una única interfaz que se ejecuta en un navegador Web.

✓ Base de datos y anotaciones de recuperación

El servidor de Tivoli Storage Manager utiliza una base de datos para realizar un seguimiento de información sobre el almacenamiento del servidor, los clientes, los datos de los clientes, la política y las planificaciones. El servidor utiliza las anotaciones de recuperación como cuaderno de apuntes para la base de datos y registra la información sobre las acciones del cliente y del servidor mientras éstas se están llevando a cabo.

✓ Almacenamiento del servidor

El servidor puede grabar datos en unidades de disco duro, matrices de disco y subsistemas, unidades de cintas autónomas, bibliotecas de cintas y otras formas de almacenamiento de acceso aleatorio y secuencial. Los medios que utiliza el servidor se agrupan en *agrupaciones de almacenamiento*. Los dispositivos de

almacenamiento pueden conectarse directamente al servidor o conectarse a través de la red de área local (LAN) o de la red de área de almacenamiento (SAN).

✓ Nodos cliente

Un nodo cliente puede ser una estación de trabajo, un PC, un servidor de archivos, un servidor de archivos NAS (almacenamiento conectado a red) o incluso otro servidor de Tivoli Storage Manager. El nodo cliente tiene software del cliente de IBM Tivoli Storage Manager instalado (excepto para servidores de archivos NAS que utilicen NDMP). Un nodo cliente se inscribe en el servidor.

✓ Cliente de copia de seguridad/archivado

El cliente de copia de seguridad/archivado permite a los usuarios mantener versiones de copia de seguridad de los archivos, que pueden restaurar si los archivos originales se pierden o se dañan. Los usuarios también pueden archivar copias para almacenarlas a largo plazo y recuperar las copias archivadas cuando sea necesario. Los propios usuarios o administradores pueden inscribir las estaciones de trabajo y los servidores de archivos como nodos cliente en un servidor de Tivoli Storage Manager.

El agente de almacenamiento es un componente opcional que también puede instalarse en un sistema que es un nodo cliente. El agente de almacenamiento permite el traspaso de datos fuera de la LAN para operaciones de cliente y se admite en varios sistemas operativos.

✓ Servidor de archivos de almacenamiento conectado a red (utilizando NDMP)

El servidor puede emplear el protocolo de gestión de datos de red (NDMP) para realizar operaciones de copia de seguridad y restauración de sistemas de archivos almacenados en un servidor de archivos NAS (almacenamiento conectado a red). La copia de seguridad de los datos de un servidor de archivos NAS se realiza en una biblioteca de cintas. No es necesario que haya instalado ningún software de Tivoli Storage Manager en el servidor de archivos NAS. También se puede realizar la copia de seguridad de un servidor de archivos NAS a través de la LAN en un servidor de Tivoli Storage Manager. Consulte el Capítulo 7. Utilizar NDMP

para operaciones con servidores de archivos NAS para obtener más información al respecto, incluidos los servidores de archivos NAS permitidos.

✓ Cliente de aplicación

Los clientes de aplicación permiten llevar a cabo copias de seguridad en activo de los datos en aplicaciones como por ejemplo, los programas de base de datos. Una vez que el programa de aplicación inicia una copia de seguridad o restauración, el cliente de aplicación actúa como la interfaz para Tivoli Storage Manager. A continuación, el servidor de Tivoli Storage Manager aplica sus funciones de gestión de almacenamiento a los datos. El cliente de aplicación puede realizar sus funciones mientras los usuarios trabajan con las mínimas interrupciones posibles.

Los productos siguientes proporcionan clientes de aplicación para el uso con el servidor de Tivoli Storage Manager:

- ✓ Tivoli Storage Manager para servidores de aplicaciones.
- ✓ Tivoli Storage Manager para bases de datos.
- ✓ Tivoli Storage Manager para ERP.
- ✓ Tivoli Storage Manager para correo.

También está disponible Tivoli Storage Manager para hardware, que se ejecuta con el cliente de copia de seguridad/archivado y la API para ayudar a eliminar los efectos sobre el rendimiento relacionados con la copia de seguridad.

✓ Interfaz de programación de aplicaciones (API)

La API permite mejorar las aplicaciones existentes para utilizar los servicios de copia de seguridad, archivado, restauración y recuperación que Tivoli Storage Manager proporciona. Los clientes de API de Tivoli Storage Manager pueden inscribirse como nodos cliente en un servidor de Tivoli Storage Manager.

✓ Tivoli Storage Manager para la gestión de espacio

Tivoli Storage Manager para la gestión de espacio proporciona servicios de gestión de espacio para estaciones de trabajo en determinadas plataformas. La función de gestión de espacio es básicamente una versión de archivado más automatizada. Tivoli Storage Manager para la gestión de espacio migra

automáticamente los archivos menos utilizados al almacenamiento del servidor; de este modo, se libera espacio en la estación de trabajo. Los archivos migrados también se denominan *archivos bajo gestión de espacio*.

Los usuarios pueden recuperar automáticamente los archivos bajo gestión de espacio simplemente accediendo a ellos del modo habitual desde la estación de trabajo. Tivoli Storage Manager para la gestión de espacio también se denomina cliente de gestión de espacio o cliente de gestión de almacenamiento jerárquico (HSM).

✓ Agentes de almacenamiento

El agente de almacenamiento es un componente opcional que puede instalarse en un sistema que también es un nodo cliente. El agente de almacenamiento permite el traspaso de datos fuera de la LAN para operaciones de cliente.

El agente de almacenamiento está disponible para el uso con clientes de copia de seguridad/archivado y clientes de aplicación en diversos sistemas operativos. El producto Tivoli Storage Manager para redes de área de almacenamiento incluye el agente de almacenamiento.

Los programas cliente, como por ejemplo, el cliente de copia de seguridad/archivado y el cliente de HSM (gestor de espacio) se instalan en sistemas conectados a través de una LAN y se inscriben como nodos cliente. Desde esos nodos cliente, los usuarios pueden hacer copias de seguridad, archivar o migrar archivos al servidor.

En los apartados siguientes se presentan los conceptos fundamentales y se facilita información acerca de IBM Tivoli Storage Manager. En estos apartados se describe cómo gestiona Tivoli Storage Manager los archivos de cliente en función de la información proporcionada en las políticas definidas por el administrador y cómo gestiona los dispositivos y los medios según la información proporcionada en los objetos de almacenamiento de Tivoli Storage Manager definidos por el administrador.

### 2.3.2. *Características de Tivoli Storage Manager.*

IBM Tivoli Storage Manager (TSM) de la familia de Tivoli ofrece una amplia gama de características de apoyo a la protección automatizada centralizada de datos que puede ayudar a reducir los riesgos asociados con la pérdida de datos al tiempo que ayuda a administrar los costos, reducir la complejidad y encaminar el cumplimiento de la retención de datos sobre la regulación de requisitos de la empresa.

✓ Almacenamiento y la nube

Servicios en la nube dependen en gran medida de mantener los datos y las aplicaciones que están manejando en todo momento, y para restablecer las operaciones rápidamente tras cualquier tipo de desastre, garantizando al mismo tiempo la utilización óptima y el rendimiento de los recursos de almacenamiento en la nube.

✓ Protección de aplicaciones

Protege los datos de aplicaciones críticas del negocio para una amplia variedad de bases de datos, programas de correo, soluciones ERP y servidores de aplicaciones, asegurando la integridad y fiabilidad de los datos.

✓ Backup y Recuperación

Proteger los datos mediante el almacenamiento de copias de seguridad en el almacenamiento en línea y fuera de las instalaciones, y emplea múltiples técnicas inteligentes para hacer copias de seguridad de datos.

✓ Continuidad del Negocio de Nivel de Servicio de Protección

Las empresas necesitan alta disponibilidad de datos y la rápida recuperación de un tiempo de inactividad con el fin de mantener su competitividad.

✓ Reducción de datos

Las empresas necesitan alta disponibilidad de datos y la rápida recuperación de tiempo de inactividad con el fin de mantener su competitividad.

- ✓ Prepararse para una catástrofe  
Crea un plan de recuperación de desastres que contiene los pasos detallados de recuperación y scripts, equipo para recuperar los activos más críticos de su empresa.
- ✓ Virtualización del almacenamiento  
Se busca reducir la complejidad y los costos de administrar de almacenamiento basado en SAN.
- ✓ Administrador de “Archives”  
Guardar copias de datos activa o inactiva por un período de tiempo especificado en el almacenamiento fuera de línea. Ideal para almacenamiento a largo según los requisitos de plazos reglamentarios o de contabilidad.
- ✓ Protección de los datos de oficinas remotas.  
Afrontar los retos de proteger y recuperar datos importantes en las oficinas remotas y sucursales, de forma rápida, automática y de forma rentable.
- ✓ Gestión de Almacenamiento de Recursos  
Herramientas de gestión de almacenamiento de los recursos puede ayudar a los clientes a reducir la complejidad de la gestión de sus entornos de almacenamiento mediante la centralización, simplificación y automatización de las tareas de almacenamiento.
- ✓ Gestión Unificada de recuperación  
IBM ofrece la posibilidad única de manejar todas las complejidades de la protección de datos en toda la empresa distribuida a partir de una interfaz de administración única.
- ✓ Automatiza, supervisa y controla la programación de trabajo en toda su infraestructura de TI y se integra con su ERP, CRM y soluciones de comercio electrónico.
- ✓ Agrupaciones de Almacenamiento de Datos Activos.  
Permite optimizar el acceso a las versiones de restauraciones activas optimizando la rapidez. Las versiones activas del grupo de almacenamiento se pueden generar en el momento o después de que la copia de seguridad se haya completado.

- ✓ **Compatibilidad con Active Directory**  
Establece la no-supresión (reanimación) de objetos del Active Directory.
- ✓ **Centro de Administración / Interfaz de Administración de Usuario**  
Interfaces web para gestionar uno o varios servidores de Tivoli Storage Manager,
- ✓ **Backup Sets (rápida restauración o “archives” al instante)**  
Ofrece la posibilidad de crear un conjunto de copia de seguridad que consolida los archivos de un cliente en un conjunto de medios de comunicación que es portátil y puede ser directamente legibles por el sistema de los clientes para una rápida restauración de archivos, sin necesidad del uso de LAN (sin red) dichas operaciones de restauración
- ✓ **Bare Machine Restore (Bare Metal Restore)**  
Restaura el sistema operativo de Windows, Sun <sup>TM</sup>, Linux, AIX y HP, a un punto en el tiempo
- ✓ **Checksum**  
Añade una capa adicional de verificación de datos entre el servidor de TSM y el cliente se recomienda ejecutar en entornos de hardware inestable.
- ✓ **Grupos de colocación**  
Toma una agrupación de clientes e individualmente sus datos para poder especificar si los datos deben residir en su propia cinta o un conjunto de cintas.
- ✓ **Compresión**  
Los clientes pueden elegir que sus datos sean comprimidos antes de ser enviados al servidor de Tivoli Storage Manager para ayudar a conservar el ancho de banda
- ✓ **Deduplicación**  
La deduplicación de datos reduce la cantidad de datos enviados a través de la red hacia el servidor de TSM. Post-proceso de respaldo, el objetivo de deduplicación de datos es reducir la capacidad necesaria de disco en las agrupaciones de almacenamiento.

- ✓ Disaster Recovery Manager (DRM)  
Crea un plan de recuperación ante desastres y facilita el seguimiento de los volúmenes fuera de sitio. El plan contiene los pasos detallados de recuperación y scripts automatizados equipo.
  
- ✓ Cifrado  
Permite que los archivos de copia de seguridad o archivado puedan ser encriptados antes de ser enviados al servidor de Tivoli Storage Manager, también ofrece soporte a nivel de dispositivo cifrado gestionado por TSM.
  
- ✓ Configuración y Administración de Políticas de Respaldo según Requerimientos de las empresas.  
La configuración de Tivoli Storage Manager permite que la información de políticas de respaldo se definan una vez en la configuración del servidor de Tivoli Storage Manager y después se propagan a cualquier número de servidores gestionados por TSM.
  
- ✓ VMware Consolidated Backup (VCB)  
Consolidated Backup es una solución de copia de seguridad de ESX Server + SAN. Utiliza un solo agente en el servidor proxy en lugar de un agente en cada máquina virtual. Gestiona los datos de copia de seguridad de máquinas virtuales como si hubiera sido respaldado por un cliente de Tivoli Storage Manager instalado en la máquina. Ofrece respaldos de virtuales tanto a nivel de archivos y copias de seguridad como a nivel de imagen.
  
- ✓ Restauración de buzones de correo a nivel de ítem.  
Proporciona la recuperación individual de buzones a nivel de elementos de Microsoft Exchange.
  
- ✓ Copia de seguridad de archivos abiertos.  
Permite la copia de seguridad de archivos que se están siendo utilizados.
  
- ✓ Interface SQL Server.  
Compatibilidad con las consultas SQL contra la base de datos del servidor de TSM.

- ✓ Clientes basados en web y una interface de administración.  
Interfaz simple y amigable que reduce el tiempo de búsquedas y puede aumentar la productividad.

### **2.3.3. *Como Funciona Tivoli Storage Manager.***

Las funciones administrativas se acceden a través de la herramienta de línea de comandos de IBM, a través de WebSphere Portal de IBM, la aplicación conocida como la "Administración Central", o a través de ODBC Console. También hay clientes de terceros API de administración, por ejemplo TSMManager.

TSM utiliza dos agentes de propósito especial. El primero es el agente de almacenamiento fuera de la LAN. Esta es una función limitada del servidor de Tivoli Storage Manager que se configura como un cliente de la librería de cintas y los usos de servidor a servidor de comunicaciones para coordinar el uso de los recursos de almacenamiento que están configurados para TSM, pero que también se presentan para el agente de almacenamiento. Por lo general, "LAN free" y "Server free backup" se instala en el cliente específico. Un ejemplo sería la de conectar a través de InfiniBand entre dos chasis BladeCenter, donde uno tiene conectado la SAN a la cinta, y el otro no. Esto podría pasar por alto un limitado ancho de banda Ethernet sin tener que mover la instancia del servidor TSM.

Las políticas de Tivoli Storage Manager son reglas que rigen la forma en que se almacenan y se gestionan los datos de los clientes. Las reglas incluyen dónde se almacenan los datos inicialmente, el número de versiones de copia de seguridad que se conservan, el tiempo de almacenamiento de las copias archivadas, etc. Se pueden tener varias políticas y asignarlas según convenga a clientes determinados o incluso a archivos determinados.

La política asigna una ubicación en el almacenamiento del servidor donde los datos se almacenan inicialmente. El almacenamiento del servidor está dividido en agrupaciones de almacenamiento que son grupos de volúmenes de almacenamiento. El almacenamiento del servidor puede incluir volúmenes de disco duro y de cinta.

Al instalar Tivoli Storage Manager, se dispone de una política predeterminada que puede utilizar.

Los clientes utilizan Tivoli Storage Manager para almacenar datos con una de las finalidades siguientes:

#### Copia de seguridad y restauración

El proceso de copia de seguridad copia los datos de las estaciones de trabajo cliente en el almacenamiento del servidor para garantizar que no se pierdan los datos que se cambian habitualmente. El servidor conserva las versiones de un archivo según la política y sustituye las versiones anteriores del servidor por versiones más recientes. La política especifica el número de versiones y el período de retención de las mismas. Un cliente puede restaurar la versión más reciente de un archivo o versiones anteriores.

#### Archivado y recuperación

El proceso de archivado, copia los datos de las estaciones de trabajo cliente en el almacenamiento del servidor para conservarlos durante largos períodos de tiempo. Este proceso, si se desea, puede suprimir las copias archivadas de las estaciones de trabajo cliente. El servidor conserva las copias archivadas en función de la política establecida durante un período de retención de copia archivada. Un cliente puede recuperar una copia archivada de un archivo.

#### Archivado instantáneo y recuperación rápida

El *archivado instantáneo* es la creación de un conjunto completo de archivos de copia de seguridad de un cliente. El conjunto de archivos se denomina *juego de copias de seguridad*. Un juego de copias de seguridad se crea en el servidor a partir de los archivos de copia de seguridad más recientes que ya se han almacenado en el almacenamiento del servidor del cliente. La política para el juego de copias de seguridad consta del tiempo de retención que se selecciona al crear el juego de copias de seguridad.

Es posible copiar un juego de copias de seguridad en medios portátiles compatibles, que, a continuación, pueden llevarse directamente al cliente para que se pueda

recuperar rápidamente sin utilizar ninguna red y sin tener que comunicarse con el servidor de Tivoli Storage Manager.

#### Migración y recuperación

La *migración* es una función del programa Tivoli Storage Manager para la gestión de espacio que libera espacio del almacenamiento del cliente copiando archivos de las estaciones de trabajo en el almacenamiento del servidor. En el cliente, el programa Tivoli Storage Manager para la gestión de espacio sustituye el archivo original por un archivo apéndice que hace referencia al archivo original ubicado en el almacenamiento del servidor. Los archivos se recuperan para las estaciones de trabajo cuando es necesario.

Este proceso se denomina también gestión de almacenamiento jerárquico (HSM). Una vez configurado, el proceso es transparente para los usuarios. Los archivos se migran y recuperan de forma automática.

La política determina cuándo debe considerarse la migración automática de los archivos. En los sistemas UNIX o Linux que admiten el programa Tivoli Storage Manager para la gestión de espacio, las políticas determinan si deben realizarse copias de seguridad de los archivos antes de realizar la migración de los mismos. La gestión de espacio también se integra con la copia de seguridad. Si el archivo del que debe realizarse una copia de seguridad ya se ha migrado al almacenamiento del servidor, la copia de seguridad del archivo se realizará en el almacenamiento del servidor.

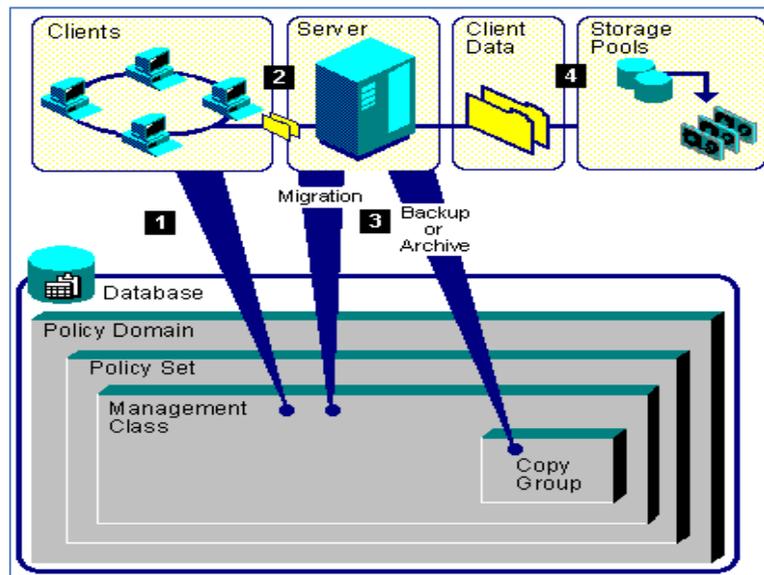


Figura 2.5. Proceso de Copia de Seguridad, Archivado y migración  
Fuente. [Web 5]

Los pasos del proceso son los siguientes:

- Un cliente inicia una operación de copia de seguridad, archivado o migración. El archivo implicado en la operación está vinculado con una clase de gestión. La clase de gestión es la clase predeterminada o una clase especificada para el archivo en las opciones de cliente (lista de inclusión/exclusión del cliente).
- Si el archivo es un candidato para la copia de seguridad, archivado o migración según la información de la clase de gestión, el cliente envía el archivo y la información del archivo al servidor.
- El servidor comprueba la clase de gestión vinculada al archivo para determinar el *destino*, el nombre de la agrupación de almacenamiento de Tivoli Storage Manager donde el servidor almacena inicialmente el archivo. Para las copias de seguridad de archivos y copias archivadas, los destinos se asignan en los grupos de copia de seguridad y copia archivada, que están en las clases de gestión. Para los archivos bajo gestión de espacio, los destinos se asignan en la clase de gestión propiamente dicha. La agrupación de almacenamiento puede ser un grupo de volúmenes de disco, de cinta u ópticos.

- El servidor almacena el archivo en la agrupación de almacenamiento identificada como destino de almacenamiento. El servidor de Tivoli Storage Manager guarda información en su base de datos sobre cada archivo que migra, archiva o del que hace una copia de seguridad. Si configura el almacenamiento del servidor en una jerarquía, Tivoli Storage Manager puede migrar posteriormente el archivo a una agrupación de almacenamiento distinta de la agrupación en que dicho archivo estaba almacenado inicialmente. Por ejemplo, puede establecer el almacenamiento del servidor de modo que Tivoli Storage Manager migre los archivos de una agrupación de almacenamiento de disco a volúmenes de cinta en una agrupación de almacenamiento de cinta.

#### ***2.3.4. Tratamiento de la Información.***

Los archivos permanecen en el almacenamiento del servidor hasta que caducan y se produce el proceso de caducidad, o hasta que se suprimen del almacenamiento del servidor. Un archivo caduca según los criterios que se configuran en la política. Por ejemplo, los criterios incluyen el número de versiones permitidas para un archivo y el número de días que han transcurrido desde la supresión de un archivo del sistema de archivos del cliente. Si la protección de retención está activada, un objeto archivado no puede suprimirse accidentalmente.

El cliente de Tivoli Storage Manager normalmente envía los datos al servidor a través de la LAN. A continuación, el servidor transfiere los datos a un dispositivo conectado al servidor. Sin embargo, con la llegada del almacenamiento conectado a red y de SAN, Tivoli Storage Manager ofrece opciones que permiten minimizar el uso de la LAN y de los recursos informáticos tanto del cliente como del servidor.

El traspaso de datos fuera de la LAN permite agentes de almacenamiento que se instalan en los nodos cliente para traspasar datos al servidor sin enviarlos a través de la LAN

### Consolidación de datos de copia de seguridad para clientes

Al agrupar los datos de copia de seguridad para un cliente, puede minimizar el número de montajes de medios necesarios para la recuperación del cliente. El servidor ofrece métodos para realizarlo:

#### Proximidad

El servidor puede mantener los archivos de cada uno de los clientes en un número mínimo de volúmenes dentro de una agrupación de almacenamiento. Puesto que los archivos de clientes están consolidados, al mantener los archivos una cierta proximidad, para restaurarlos se necesitan menos montajes de medios. No obstante, la copia de seguridad de archivos de clientes diferentes requiere más montajes.

#### Agrupaciones de datos activos

Las agrupaciones de datos activos son agrupaciones de almacenamiento que sólo contienen las versiones activas de los datos de copia de seguridad del cliente. Los datos de copia archivada y los datos migrados mediante clientes de gestión de almacenamiento jerárquico (HSM) no están permitidos en las agrupaciones de datos activos.

Las agrupaciones de datos activos se pueden asociar a tres tipos de dispositivos: discos de acceso secuencial (FILE), medios extraíbles (de cintas u ópticos) o volúmenes de acceso secuencial en otro servidor de Tivoli Storage Manager. Existen tres tipos de agrupaciones de datos activos, cada uno de ellos con ventajas claras. Por ejemplo, una agrupación de datos activos asociada a un disco de acceso secuencial es ideal para restauraciones de datos de cliente rápidas, ya que no es preciso montar las cintas y el servidor no tiene que posicionar archivos inactivos anteriores.

#### Creación de juegos de copias de seguridad

Puede crear un juego de copias de seguridad para cada uno de los clientes de copia de seguridad/archivado. Un juego de copias de seguridad contiene todos los archivos de copia de seguridad activos que existen actualmente para dicho cliente en el almacenamiento del servidor. El proceso también se denomina archivado instantáneo.

El juego de copias de seguridad es portátil y se mantiene durante el tiempo que se especifique. La creación del juego de copias de seguridad requiere más medios puesto que se trata de una copia adicional a las copias de seguridad que ya están almacenadas.

Traspaso de datos para un nodo cliente

Puede consolidar datos para un nodo cliente mediante el traspaso de datos dentro del almacenamiento del servidor. Puede traspasarlos a una agrupación de almacenamiento diferente o a otros volúmenes de la misma agrupación de almacenamiento.

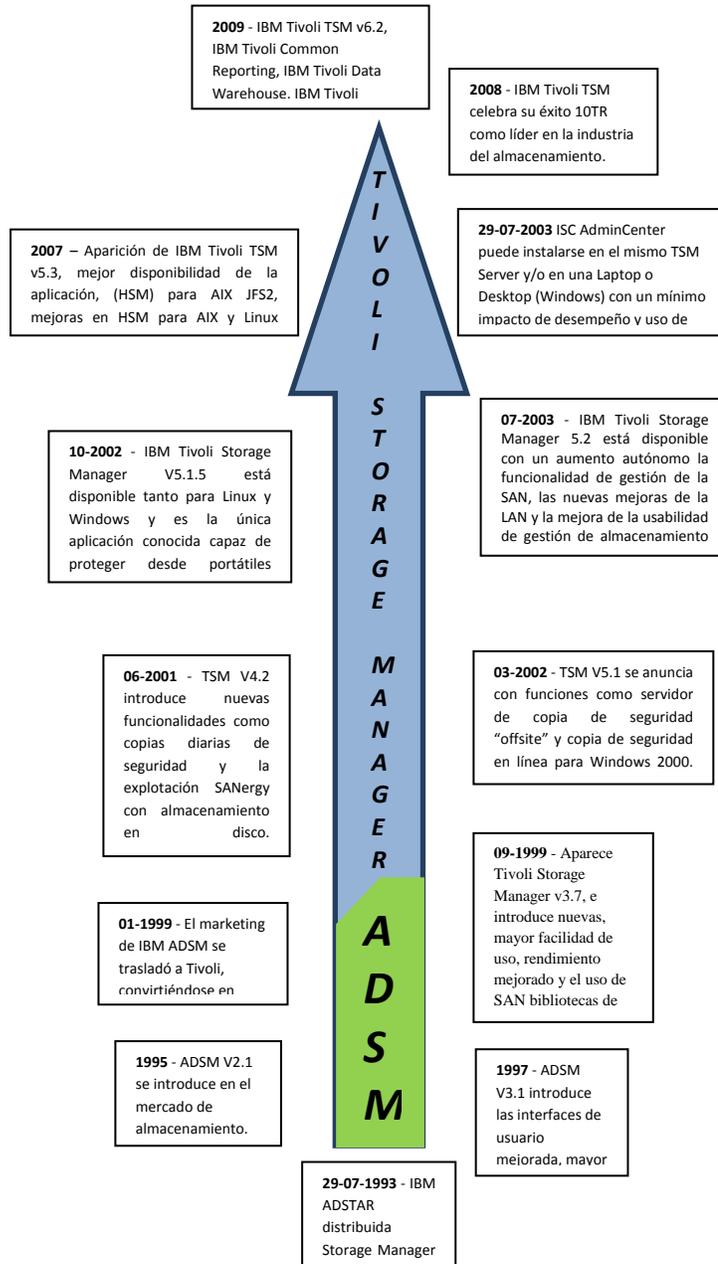
### **2.3.5. Evolución de Tivoli Storage Manager.**

TSMManager ofrece reemplazar funcionalidades de IBM Tivoli Storage Manager como:

- ✓ Integrated Solutions Console (ISC) Admin Center, componente de IBM WebSphere, aludiendo que IBM Tivoli Storage Manager sobrecarga el uso de CPU y Memoria.
  
- ✓ Disaster Recovery Module (DRM), componente de la versión IBM Tivoli Storage Manager Extended Edition, aludiendo que este componente no se incluye en la versión TSM (Basic).
  
- ✓ IBM Tivoli Storage Manager Extended Edition incluye el Disaster Recovery Module. Generalmente, esta es la versión que se comercializa y ofrece a los clientes por el valor que aporta y por la robustez de la arquitectura de respaldos. IBM Tivoli Storage Manager (Basic) no incluye el DRM, sin embargo, se le hace patente al cliente cuando esto es así. Raras ocasiones se ofrece la versión "Basic".

TSMManager es un producto (appliance) desarrollado y vendido por Tivoli Associates, Inc. y las funcionalidades que ofrece ya están incluidas desde las versiones IBM Tivoli Storage Manager EE v5.4, v5.5, e incluso en la más reciente v6.1 con mejoras substanciales en cuando a uso de recursos, espacio en disco y mejoras al desempeño, entre otras.

IBM Tivoli Storage Manager tiene ya más de 15 años en el mercado y cada nueva versión, integración de sus productos y soluciones implican un desarrollo robusto ofreciendo los más altos estándares de la industria de tecnologías de la información



**Tabla 2.6. Evolución de TSM**  
Fuente. Personal

**2.3.6. Generación de Material de Entrenamiento.**

**Anexo B**

## **2.4. SYSTEM CENTER DATA PROTECTION MANAGER.**

Data Protection Manager 2010 forma parte de la familia de productos de administración de System Center de Microsoft. Proporciona una protección de datos unificada para servidores de Windows como SQL Server, Exchange, SharePoint, Virtualización y servidores de archivos y también para equipos de escritorio y equipos portátiles de Windows. DPM está diseñado como la mejor solución de su clase en las áreas de copias de seguridad y recuperación para los entornos de Windows de Microsoft. DPM proporciona la mejor protección y los escenarios más compatibles de recuperación de su entorno de Windows desde disco, cinta o la nube. Los clientes de Windows de cualquier tamaño pueden confiar en Microsoft para que les proporcione una solución de protección escalable y manejable que es rentable, segura y fiable.

Para la recuperación de los datos, System Center Data Protection Manager (DPM) crea puntos de recuperación (versiones anteriores) de los datos protegidos. Puede buscar en los puntos de recuperación de cada réplica para encontrar, seleccionar y recuperar las versiones anteriores de los datos protegidos.

Anteriormente conocido como Servidor de Protección de Datos, DPM es la primera entrada de Microsoft en el mundo de copias de seguridad continua / recuperación de información. También se utiliza la tecnología de “Microsoft Shadow Copy” para copias de seguridad continuas.

Data Protection Manager 2006 fue lanzado el 27 de septiembre 2005 en las decisiones de almacenamiento en Nueva York. La versión actual, Data Protection Manager 2010, apoya la protección de servidores de archivos Windows, Exchange Server, Microsoft SQL Server, SharePoint, Microsoft Virtual Server y Bare Metal Restore (BMR).

### **2.4.1. Componentes de System Center Data Protection Manager.**

System Center Data Protection Manager (DPM) 2010 requiere una instancia de SQL Server 2008 Service Pack 1 para la base de datos de DPM. Durante la instalación, puede elegir que el programa de instalación de DPM instale SQL Server en el servidor DPM, o puede especificar una instancia remota de SQL Server para su uso con DPM.

Utilizando una instancia remota de SQL Server requiere que los archivos de soporte DPM estén instalados en el equipo remoto.

Dependiendo del sistema operativo que utilice, hay cambios que deben aplicarse antes de instalar DPM.

DPM instala automáticamente verifica la existencia de los siguientes componentes para poder llevar a cabo la instalación de DPM, de no existir los mismo procede a instalarlos.

- ✓ .Net Framework 3.5 con Service Pack 1 (SP1) o posterior.
- ✓ Microsoft Visual C ++ 2008 Redistributable.
- ✓ Windows PowerShell 2.0.
- ✓ Windows Installer 4.5 o posterior.
- ✓ Microsoft Application Error Reporting.
- ✓ Consola de Administración de DPM.
- ✓ Agentes para Microsoft Windows 2008 SP1.
- ✓ Agentes para Microsoft Virtual Server 2005 R2
- ✓ Agentes para Windows Server 2008 con Hyper-V
- ✓ Agentes para Windows Server 2008 R2 con Hyper-V
- ✓ Agentes para Hyper-V Server 2008 y 2008 R2

#### **2.4.2. Características de System Center Data Protection Manager.**

- ✓ Protección para clientes de Windows, en línea o sin conexión, con asistentes de fácil uso para establecer programaciones de protección, retención y alerta. Un solo servidor de DPM puede proteger más de 1000 clientes Windows al mismo tiempo, los usuarios finales pueden recuperar sus propios datos utilizando Windows Explorer o Microsoft Office.
- ✓ Protección de plataformas de Microsoft Virtualization, incluyendo configuraciones de Migración actualizada de Hyper-V / Volúmenes compartidos de clúster (CSV). DPM puede recuperar también elementos de archivo único desde copias de seguridad de VM basado en host.
- ✓ Protección mejorada para SQL Server, ampliando a más de 2.000 bases de datos por cada servidor de DPM y ofreciendo protección automática para nuevas bases de datos por cada instancia de SQL. Los administradores de bases de datos pueden recuperar sus propias bases de datos mediante una utilidad de recuperación automática para SQL Server.
- ✓ Protección mejorada para Exchange Server, ampliando a más de 40TB de correo electrónico y compatibilidad con Exchange 2010 Database Availability Groups (DAG), así como con CCR/SCR en Exchange 2007.
- ✓ Protección mejorada para SharePoint sin el requisito de una granja de servidores de recuperación con SharePoint 2010 y ampliando las granjas hasta los 25TB con más de un millón de elementos. Las nuevas bases de datos de contenidos están ahora protegidas automáticamente sin la intervención de un administrador.
- ✓ DPM 2010 está verdaderamente preparado para la empresa, ampliando a más de 100 servidores con más de 80TB por cada servidor de DPM e incluye nuevas características de expansión automática, reparación automática y protección automática para convertirse en una solución completa y fiable de protección y recuperación.

- ✓ DPM 2010 ofrece soporte integrado para Exchange y las configuraciones avanzadas de clúster de SQL, corta las ventanas de backup SQL sin necesidad de compresión, así como avanzadas opciones de protección de datos de SharePoint.
- ✓ Las aplicaciones generan cero pérdida de información en el proceso de restauración de la información.
- ✓ DPM 2010 permite la recuperación sin pérdidas de Exchange, SQL y servidores de SharePoint, sin necesidad de replicación constante sincronización, perfecta integración de restauración en un punto en el tiempo de bases de datos con los registros de las aplicaciones existentes.
- ✓ Las copias de seguridad están basadas en host de servidor virtual.
- ✓ DPM 2010 incluye soporte para copias de seguridad basado en host de los clientes de Windows Virtual Server. El uso de un único host basado en DPM 2010 para proporcionar copias de seguridad de agente de aplicación coherente de todas y todos los huéspedes que residen en un host. DPM 2010 puede proteger cualquier sistema operativo o aplicación a través de este mecanismo, siempre y cuando se ejecutan en un servidor Windows.
- ✓ Recuperar archivos en minutos en lugar de horas.
- ✓ La recuperación de archivos típicos de cintas lleva horas y pueden ser costosas. Un centro de datos mediano típico puede tener de 10 a 20 horas o más para recuperaciones por mes. DPM 2010 permite recuperaciones en minutos, lo cual se transforma en ahorro de dinero para el negocio y en ahorro de tiempo para los administradores de TI. Además, una recuperación más rápida de información mantiene a los trabajadores productivos, ya que pasan menos tiempo de inactividad en espera de sus archivos a recuperar.
- ✓ Eliminar la ventana de copia de seguridad de sus servidores de producción.

- ✓ Crecimiento masivo de las capacidades de almacenamiento, se ha incrementado el tiempo necesario para servidores de archivos de copia de seguridad. Las empresas también se enfrentan a la exigencia de 24 / 7 el tiempo de actividad y la dificultad para encontrar un tiempo sin interrupciones para realizar una copia de seguridad. Debido a DPM 2010 sólo se mueve los cambios a nivel de bytes de los servidores de archivos de los que se realiza copias de seguridad, que elimina de manera efectiva el tiempo de inactividad necesario para respaldar sus servidores de archivos. Los clientes nunca tienen que planificar para tales "ventanas de copia de seguridad".
- ✓ Permiten a los usuarios realizar su propia recuperación.
- ✓ Procesos de recuperación y copia de seguridad generalmente implican varios administradores, cada uno con una experiencia única, añadiendo al coste de gestión de datos total de propiedad. Las corporaciones gastan en conjunto miles de millones de dólares al año en recuperación de datos perdidos. DPM 2010 resuelve estos problemas al permitir la recuperación de usuario auto-servicio, que le permite acceder y recuperar los archivos directamente en Microsoft Windows (versiones de XP hasta Windows 7) y Microsoft Office (versiones 2007 y 2010) aplicaciones sin intervención del administrador, lo que reduce los costos y aumentar la productividad del administrador.
- ✓ Los medios de comunicación se integran de manera perfecta.
- ✓ DPM 2010 cuenta con una perfecta integración entre el disco y cinta. Esto incluye una interfaz de usuario inteligente de manejo, para poder quitar del operador de la necesidad de administrar por separado en disco y cinta, una experiencia integral de restauración de discos y cintas, y una rica funcionalidad de gestión de los medios de comunicación.
- ✓ Eficiencia del almacenamiento
- ✓ Tecnología de filtro patentado reduce el volumen de copias de seguridad completas hasta en un 90 por ciento de las organizaciones típicas, el ahorro de espacio en

disco y reduce el tiempo de copia de seguridad completa de horas a minutos. Utilización de VSS para instantáneas de los servidores lo cual reduce el volumen necesario en disco.

- ✓ Quitar las cintas de las sucursales y Centralización de copias de seguridad en el centro de datos.
- ✓ La forma principal de proteger a los servidores remotos es que el personal de la sucursal realice copias de seguridad en medios extraíbles, como son los cartuchos o cintas de datos, y luego manualmente trasportarlos a una instalación de almacenamiento fuera del sitio. Restaurar la información de una cinta dentro de esta configuración puede ser costoso y lento. DPM despliega agentes en los servidores de archivos remotos para enviar dicha configuración donde se almacenará los respaldos en una central de datos por ende será más seguro el proceso de respaldado y será manejado por un administrador de TI.
- ✓ Ofrece una funcionalidad avanzada a bajo costo.
- ✓ Debido a DPM 2010 es parte del Windows Server System, que contiene herramientas que ya están en el software de servidor, como Microsoft Management Console (MMC) y el Explorador de Windows. Los administradores de TI ya están familiarizados con estas herramientas, lo que reduce los costes de formación. Junto con la funcionalidad se incluye informes completos, DPM 2010 también puede cargar todos sus informes y alertas a la consola de Microsoft Operations Manager.
- ✓ Protección y recuperación para servidores de Exchange.
- ✓ DPM 2010 protege intercambio de bases de datos de servidores cada 15 minutos.
- ✓ Protección y recuperación de Sharepoint.
- ✓ DPM 2010 proporciona la mejor clase de protección y recuperación para Microsoft Office SharePoint Technologies.

- ✓ Protección y recuperación para Microsoft SQL Server.
- ✓ DPM 2010 protege las bases de datos SQL Server cada 15 minutos, y se puede restaurar no sólo a cada una de las marcas de 15 minutos, sino también le permiten recuperarse a cualquier punto de la transacción, o incluso a la última transacción la cual fue comprometida después de un corte de energía.
- ✓ Protección para Hyper-V y Virtual Hosts Invitados.
- ✓ Incluyendo soporte para los escenarios de migración en vivo con volúmenes compartidos de clúster (CSV) y la restauración de máquinas virtuales para alternar hosts Hyper-V.
- ✓ DPM 2010 extiende la protección para ordenadores portátiles y no solo para PC's de escritorios fijos.

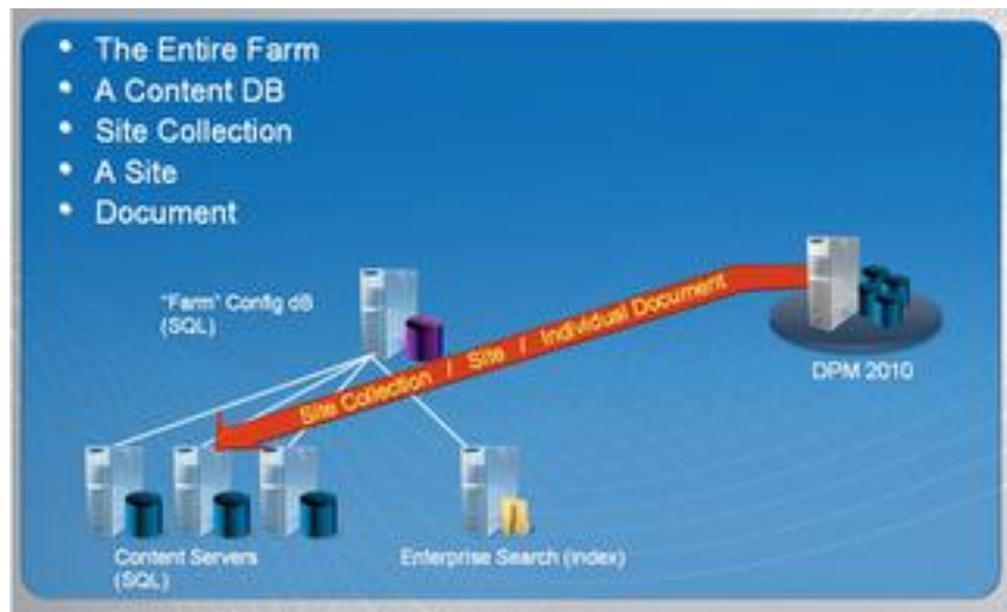


Figura 2.7. Estructura de Data Protection Manager.

Fuente. [Web 7]

#### 2.4.3. Como Funciona System Center Data Protection Manager.

En DPM, use el Asistente para recuperación para realizar la recuperación de datos. Cuando recupera datos, puede utilizar la configuración predeterminada o bien

modificar las opciones de recuperación para especificar la manera de restaurar la copia de seguridad y la ubicación. Para minimizar el tiempo necesario para las operaciones de recuperación y disminuir el tamaño de los datos que se van a transferir, DPM usa la compresión en el cable en todas las operaciones de recuperación.

El uso de direcciones de red para la copia de seguridad utilizando Data Protection Manager 2010 (DPM) le permite configurar una dirección de red de respaldo para asegurar que las copias de seguridad de DPM no reduzcan la velocidad de la red primaria. La dirección de red de copia de seguridad se crea cuando se pone adaptadores de red por separado en el servidor DPM y los servidores protegidos se conectan a través de una LAN independiente. Como resultado, el tráfico de datos de copia de seguridad no afecta a la red primaria.

Usted puede configurar la dirección de la red de copia de seguridad mediante DPM 2010 Management Shell (PowerShell) cmdlets.

Antes de que usted pueda configurar una dirección de red de copia de seguridad, es necesario:

- ✓ Asegúrese de que la resolución de nombres este activa y que tanto el servidor de DPM como el servidor del cual se realizará la copia de seguridad se puede conectar sin problema.
- ✓ Configurar la subred de copia de seguridad y su máscara correspondiente utilizando el complemento BackupNetworkAddress.

**Nota:** La subred debe cubrir todo el rango de direcciones de red para el servidor DPM y los servidores que se deseen proteger.

- ✓ Reinicie el agente de DPM en el servidor de DPM y los ordenadores protegidos. Puede suceder que las tareas en curso fallen sino se realiza esta acción. Después de un reinicio, tenga cuidado con las alertas, y realice las acciones recomendadas, si es necesario.

### Ejemplo:

En este ejemplo se detalla el proceso de creación de una dirección de red de copia de seguridad de un servidor DPM para proteger otro servidor. Todos los nombres y direcciones son hipotéticos y sólo como ejemplo.

La configuración de copia de seguridad existente consiste en la protección de dpm.xycom ps.xycom. Nombre de búsqueda con "nslookup" en cualquier servidor devuelve las direcciones IP siguientes (es decir, cada dirección IP es visible para cada nodo):

**Nota:** La búsqueda de nombres se debe realizar en los FQDN, por ejemplo, "ps.xycom nslookup".

Servidor	NIC Address
Servidor DPM (dpm.x.y.com)	10.10.12.89
Equipo protegido (ps.x.y.com)	10.10.12.90

**Tabla 2.3. Esquema Normal de Respaldos**  
Fuente. Propia

Ahora, para configurar una red de copia de seguridad, otra tarjeta de red se agrega a cada uno de los servidores y conectado a otra red como 192.168.1.0/24 con una máscara de subred 255.255.255.0 respectivamente. Cuando la red y tarjetas de red se configuran, la búsqueda del nombre con "nslookup" devuelve dos direcciones por servidor como se indica a continuación.

Servidor	NIC Address Primaria	NIC Address de Backup
Servidor DPM	10.10.12.89	192.168.1.23
Equipo protegido	10.10.12.90	192.168.1.24

**Tabla 2.4. Esquema de Respaldos con LAN Backup**  
Fuente. Propia

Se recomienda que se compruebe si el servidor DPM es capaz de hacer ping a la dirección del equipo protegido de la red de copia de seguridad (192.168.1.24). Del mismo modo, el equipo protegido debe ser capaz de hacer ping a la dirección de red de copia de seguridad del servidor DPM (192.168.1.23).

**Nota:** Complemento BackupNetworkAddress le permite configurar más de una red de respaldo. También puede utilizar la red como una red primaria de reserva durante se genera el uso de la red de respaldo. En el ejemplo anterior, la red secundaria también podría haber sido añadido con SequenceNumber 2. Como resultado, si la red secundaria se elimina y la búsqueda de nombres de servidores ya no devuelve las direcciones 192.168.1.0/24, DPM puede comenzar automáticamente con la copia de seguridad a través de la red principal registrada también para la copia de seguridad de datos

#### Cómo recuperar datos

- ✓ En la Consola de administrador DPM, haga clic en Recuperación en la barra de navegación.
- ✓ Examine o busque los datos que desee recuperar y selecciónelos en el panel de resultados.
- ✓ Los puntos de recuperación disponibles se indican en negrita en el calendario de la sección de puntos de recuperación. Seleccione las fechas en negrita de los puntos de recuperación que desee recuperar.
- ✓ En el panel Elemento recuperable, seleccione el elemento que desee recuperar.
- ✓ En el panel Acciones, seleccione una acción de recuperación: Recuperar o Mostrar todos los puntos de recuperación. DPM iniciará el Asistente para recuperación.
- ✓ Revise las selecciones de recuperación y haga clic en Siguiente.
- ✓ Especifique el tipo de recuperación que desee realizar y haga clic en Siguiente.
- ✓ Especifique las opciones de recuperación y haga clic en Siguiente.
- ✓ Revise la configuración de recuperación y haga clic en Recuperar.

La pérdida de datos es un evento indeseable, incluso desastroso, para cualquier organización. El administrador de protección de datos (DPM) ayuda a mitigar este tipo de pérdidas, proporcionándole características de búsqueda y navegación que le ayudan a encontrar los datos que necesita recuperar. Una vez encontrados los datos, puede recuperar la versión encontrada o mostrar una lista de todas las versiones disponibles para seleccionar la versión específica que se va a recuperar. Estos datos pueden ser archivos, aplicaciones o datos de equipos que ejecutan SQL Server, Windows SharePoint Services o Exchange Server. Además, DPM es compatible con la protección y recuperación de equipos de escritorio y servidores virtuales.

Sólo se tardan unos minutos en encontrar datos, seleccionar una versión y empezar un trabajo de recuperación o una colección de recuperación (múltiples trabajos). En función del tamaño de los datos que se recuperan, el trabajo puede tardar entre menos de un minuto y varias horas. Puede comprobar el estado de los trabajos de recuperación en el área de tareas Supervisión.

#### ***2.4.4. Tratamiento de la Información.***

Con DPM de protección de datos, puede utilizar almacenamiento en disco, cinta, o ambos.

Almacenamiento basado en disco, también llamado *D2D*, de "disco a disco", es un tipo de copia de seguridad en que los datos de un ordenador se almacenan en el disco duro de otro equipo. Esto contrasta con el método tradicional de hacer copias de seguridad de un ordenador a un medio de almacenamiento tales como cintas, también llamado *D2T*, para "disco a cinta." Para protección adicional, los dos métodos se pueden combinar en un disco a disco a cinta (*D2D2T*) de configuración que ofrece los beneficios de una rápida recuperación basada en disco de almacenamiento en el corto plazo y basados en cinta, almacenamiento de archivos para los datos críticos en el largo plazo. La siguiente ilustración muestra los métodos de almacenamiento de tres.

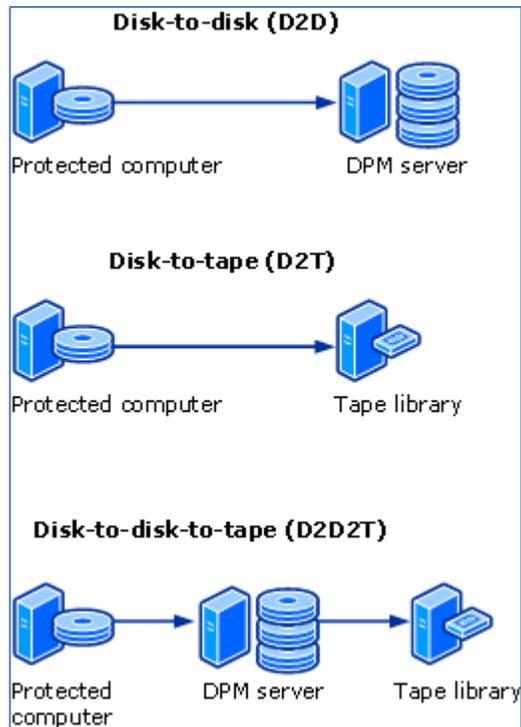


Figura 2.8. Métodos de almacenamiento de datos  
Fuente. [Web 8]

Para determinar qué método de almacenamiento se acopla para su uso, debe tener en cuenta la importancia relativa de los requisitos de protección de su organización.

*Cantidad de datos que su organización puede.* Teniendo en cuenta este tema, podemos decir que no todos los datos son igualmente valiosos. Las organizaciones deben evaluar el impacto de la pérdida contra los costos de la protección.

*¿Cómo recuperar rápidamente los datos que deben estar disponibles?* La recuperación de datos críticos para las operaciones en curso suele ser más urgente que los datos de rutina. Por otro lado, las organizaciones deben identificar los servidores que proporcionan servicios esenciales durante las horas de trabajo que no debe ser interrumpida por las operaciones de recuperación.

*El tiempo que su organización debe mantener los datos.* Almacenamiento a largo plazo podría ser necesario para las operaciones comerciales, en función del tipo y contenido de los datos. Una organización también puede estar sujeta a los requisitos

legales para la retención de datos, tales como la Ley gubernamental y las políticas internas de Retención de Datos.

**¿Cuánto de su organización puede gastar en protección de datos?** Al considerar la cantidad a invertir en la protección de datos, las organizaciones deben incluir el costo del hardware y los medios de comunicación, así como los gastos de personal de administración, gestión y apoyo.

Puede usar DPM para hacer copias de seguridad de discos y cintas, que le da la flexibilidad para crearlo de manera centralizada, estrategias de copia de seguridad detallada que dan lugar a la protección de datos eficiente y económica. Cuando usted necesita restaurar un único archivo o un servidor entero, la recuperación es rápida y simple: identificar los datos, y DPM localiza los datos y la recupera.

### ***Protección basada en disco y recuperación***

Una de las ventajas de la protección de datos basada en disco es el ahorro de tiempo posible. En cambio en el uso de cinta interviene los tiempos de preparación, puesto de trabajo, la carga de la cinta, el posicionamiento de la cinta hasta el punto de partida correcto. La facilidad de usar un disco alienta el envío de datos adicionales con más frecuencia, lo que reduce el impacto en el equipo protegido y los recursos de red.

La recuperación de datos con protección basada en disco es más fiable que la de sistemas basados en cinta. Las unidades de disco suelen tener un tiempo mucho mayor para presentar fallos.

Recuperación de datos desde el disco es más rápida y más fácil que la recuperación de la cinta. La recuperación de datos desde el disco es una simple cuestión de navegar a través de las versiones anteriores de los datos en el servidor DPM y la copia de versiones seleccionadas directamente a la computadora protegida. A la recuperación de archivos típico de la cinta lleva horas y puede ser costoso, y los administradores en un centro de mediano tamaño por lo general se puede esperar para llevar a cabo 10 a 20 horas o más de estas recuperaciones de cada mes.

Mediante DPM y protección de datos basada en disco, los datos se pueden sincronizar con la frecuencia de cada 15 minutos y se mantendrá por 448 días.

Basado en cinta un backup y archive

La cinta magnética y otros medios similares de almacenamiento ofrecen una forma barata y portátil de protección de información.

En DPM, puede grabar los datos de una computadora directamente a la cinta (D2T). También puede grabar los datos de la réplica en disco (D2D2T). La ventaja de crear su copia de seguridad a largo plazo en la cinta y la réplica en disco es que la operación de copia de seguridad puede ocurrir en cualquier momento sin ningún impacto en la computadora protegida.

Además, un plan de recuperación de desastres completa incluye el almacenamiento fuera del sitio de información crítica que usted quiere proteger y tener la capacidad de recuperar los mismos, en caso de que su centro fuese dañado o destruido. La cinta es un medio popular y conveniente para el almacenamiento fuera del sitio.

Los datos se pueden copiar en la cinta con la frecuencia diaria de protección a corto plazo, y se puede mantener hasta 99 años lo que se conoce como protección a largo plazo.

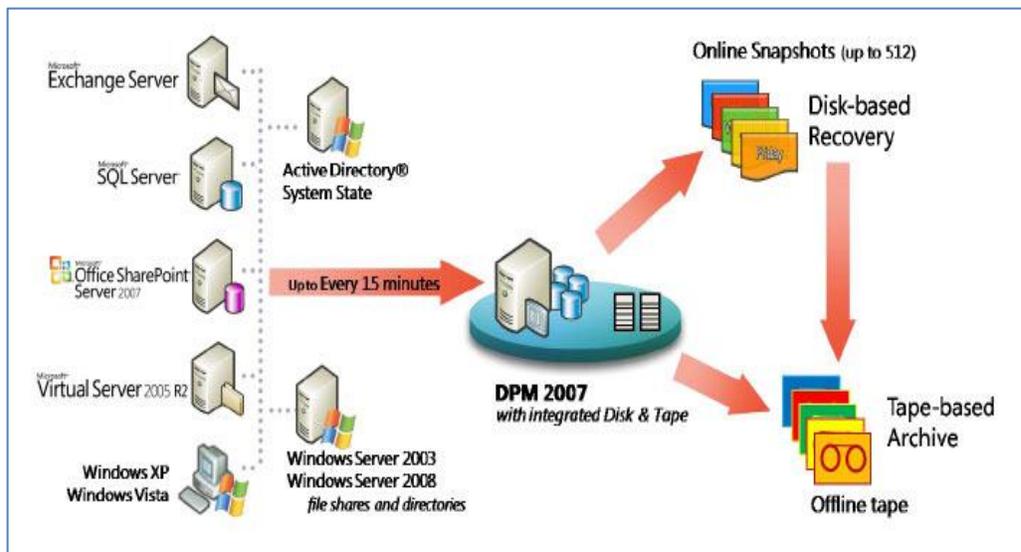


Figura 2.9. Esquema de RespalDOS de DPM

Fuente. [Web 9]

#### 2.4.5. Evolución de System Center Data Protection Manager.

Microsoft completó la producción de su sistema de recuperación y backup de datos basado en disco, Data Protection Manager (DPM) a razón del año 2005. El servidor, que puede gestionar backup continuos basados en disco de archivos que corre en entorno Windows Server, salió con su primera versión estable tanto para consumidores como para partners en agosto del 2005. El anuncio se lo realizó en el transcurso del evento anual Worldwide Partner Conference.

Microsoft empezó a trabajar en DPM desde el 2003, pero no anunció el producto hasta septiembre del año 2004. La primera beta pública del producto se lanzó en abril del 2005. Desde entonces, en ese entonces se llegó a contabilizar más de 100.000 copias de la beta.

La compañía diseñó DPM en un principio para interoperar con productos de recuperación y backup basados en cinta, pero recomienda a los clientes que utilicen también disco debido a la “inestabilidad” de los sistemas en cinta.

“Microsoft no está reemplazando nada. El producto está diseñado para ser complementario. El 90% de los consumidores confían en el backup de cinta, pero cuando llega la hora de hacer la recuperación, los sistemas se vuelven lentos e inestables”, señala Ben Matheson, jefe de producto para DPM en Microsoft.

Producto	Revisión	Año de lanzamiento
<b>System Center Data Protection Manager</b>	2006	2005
<b>System Center Data Protection Manager</b>	2007	2007
<b>System Center Data Protection Manager</b>	2010	2009
<b>System Center Data Protection Manager (beta)</b>	2012	2011

Tabla 2.5. Evolución de las Versiones de DPM

Fuente. Personal

<b>MICROSOFT DPM 2006</b>	<b>MICROSOFT DPM 2007</b>	<b>MICROSOFT DPM 2010</b>	<b>MICROSOFT DPM 2012</b>
Soporte para Proteger Sistemas de 64-bit Protection	Instalación de agentes de protección en los controladores de dominio	DPM no requiere de una SAN para toma de instantáneas lo puede realizar un DAS, o cualquier otro disco montado localmente, en el host, así como en el servidor DPM	Administración remota, ahora no solo podrá ingresar a su consola de administración por un interface GUI, sino también web.
Aumenta requerimientos de sistema para instalación	Soporte mejorado para WSS y Microsoft Office SharePoint Server	DPM no requiere software adicional de terceros para hacer copias de seguridad.	Utilización de roles de gestión, para filtrar el respaldo de información.
Soporte para Servidores Clúster	Soporte para Protección de Hyper-V	DPM deja la máquina virtual inactiva durante la copia de seguridad completa — si es necesario hibernar la máquina virtual, lo hace, crea la instantánea, y la conecta de nuevo.	SLA basado en alerta: Alerta cuando el SLA es violado.
Protección para SIS habilitado en Servidores	Soporte para Servidores de Exchange	Filtrado inteligente y personalizable para asegurar que se realice una copia de seguridad de los datos correctos.	Alertas consolidadas, asegura la generación de un ticket por cada fallo presentado.
Actualizaciones directas mediante Microsoft Update	Soporte para Servidores de Base de Datos de SQL espejados	Restaurar máquinas virtuales a máquinas alternativas de Hyper-V.	En DPM 2012 usted tendrá la posibilidad de realizar colocación de varios grupos y de protección de un

			conjunto específico de cintas
Cambio de Medios de Respaldo Principalmente a Disco.	Soporte de Protección de Datos para Bosques	Restauración de archivos individuales desde copias de seguridad basadas en host, sin necesidad de ningún agente local.	Toda la administración y operaciones comunes de DPM 2010 son soportadas.
Copias duplicadas de información compartida protegida son creadas en el servidor dpm	Respaldos de Información Local en el Servidor de DPM (Archivos y Hyper-V solamente)	Soporta más de 100 servidores, 1000 portátiles, o 2000 bases de datos con una sola instancia de DPM	Escalabilidad conjuntamente con la empresa, aumenta la tolerancia a fallos y es mucho más fiable.

**Tabla 2.6. Principales Diferencias entre Versiones de DPM**

**Fuente. Personal**

#### **2.4.6. Generación de Material de Entrenamiento.**

### **Anexo B**

### CAPÍTULO 3.



### ANÁLISIS Y COMPARATIVAS

### **3.1. REQUERIMIENTOS DEL SISTEMA**

Los requerimientos necesarios para poder realizar la implementación de cada una de las herramientas antes mencionadas en un punto sumamente importante ya que nos permitirá no tener inconvenientes tanto al momento de instalar el servidor y a su vez en el despliegue de agentes o configuración de herramientas específicas como son: Servidores de Correo, base de datos, file server y demás.

#### ***3.1.1. Requerimientos a nivel de Servidor.***

Los prerequisites para el correcto funcionamiento de Amanda Source Backup son los siguientes:

- ✓ GNU tar 1.12
- ✓ Samba 1.9.18p10 o superior
- ✓ Perl 5.004 o superior.
- ✓ GNU readline 2.2.1 o superior
- ✓ GNU awk 3.0.3 o superior
- ✓ Gnuplot 3.5 o superior

Antes de proceder con la instalación de Amanda Source Backup, debe estar configurado el servicio de Samba con un usuario perfectamente identificado el mismo que será utilizado para poder realizar conexiones con Sistemas Operativos Windows.

<b>REQUISITOS SERVIDOR</b>	<b>LINUX</b>	Debian-4.0 Debian-5.0 Debian-6.0 Fedora 10 Fedora 11 Fedora 12 Fedora 13 Open Suse 10 Redhat Enterprise 4.0 Redhat Enterprise 5.0 Redhat Enterprise 6.0 Source Suse Enterprise 10.0 Suse Enterprise 11.0 Suse Enterprise 9.0 Ubuntu-10.04 Ubuntu-10.10 Ubuntu-11.04 Ubuntu-8.04 Ubuntu-8.10 Ubuntu-9.04 Ubuntu-9.10
	<b>MEMORIA</b>	Al menos 2 GB. Un mínimo de 4 GB para servidores de producción con alta carga transaccional.
	<b>DISCO</b>	Al menos 1 GB de almacenamiento de disco disponible para la instalación
<b>REQUISITOS CLIENTES</b>	<b>LINUX &amp; WINDOWS</b>	Debian-4.0 Debian-5.0 Debian-6.0 Fedora 10

		Fedora 11 Fedora 12 Fedora 13 Open Suse 10 Redhat Enterprise 4.0 Redhat Enterprise 5.0 Redhat Enterprise 6.0 Source Suse Enterprise 10.0 Suse Enterprise 11.0 Suse Enterprise 9.0 Ubuntu-10.04 Ubuntu-10.10 Ubuntu-11.04 Ubuntu-8.04 Ubuntu-8.10 Ubuntu-9.04 Ubuntu-9.10 Windows XP Windows Vista Windows 7 Windows 2000 Windows 2003 Windows 2008 Windows 2008 R2
	<b>Memoria</b>	Al menos 2 GB.
	<b>Disco</b>	Al menos 50 MB de espacio para para la instalación del agente y 50 MB adicionales para configuraciones adicionales.

**Tabla 3.1. Sistemas Operativos Soportados por Amanda**

Fuente. Personal

En este caso para poder solventar las necesidades para la instalación de IBM Tivoli Storage Manager v6.2 sobre un ambiente Windows no necesita ningún paquete

adicional o configuraciones del sistema base por ende se detalla los requerimientos y soporte para el equipo servidor:

<b>REQUISITOS SERVIDOR</b>	<b>AIX</b>	AIX 5.3 64-bit AIX 5.3 (TL)11-(SP)1 AIX 6.1 64-bit AIX 6.1 TL 2 AIX 7.1 64-bit (SP)1
	<b>HP-UX</b>	HP Itanium 11 iv2 (11.23.0505). HP Itanium 11 iv3 (11.31) HP Itanium 11 iV2
	<b>WINDOWS</b>	Microsoft Windows Server 2003 Standard R2, 32-64 bit. Microsoft Windows Server 2003 Enterprise R2, 32-64 bit. Microsoft Windows Server 2003 Datacenter Edition R2, 32-64 bit. Microsoft Windows Storage Server 2003 Microsoft Windows Storage Server 2003 x64 Microsoft Windows Server 2008: Standard, Enterprise, or Datacenter Edition Microsoft Windows Server 2008: Standard, Enterprise, or Datacenter x64 Edition (64-bit) Microsoft Windows Server 2008 R2: Standard, Enterprise, or Datacenter Edition
	<b>SUN SOLARIS</b>	Sun Solaris 10 x86/x86_64 Sun Solaris 10 SPARC
	<b>LINUX</b>	Red Hat Enterprise Linux 5 64 bit SUSE Linux Enterprise Server 10 64 bit SUSE Linux Enterprise Server 11 64 bit GNU C libraries, Version 2.3.3-98.38 and later. Linux x86 no soportado.

	<b>MEMORIA</b>	<p>Sistemas de 64 bits Windows (recomendado) 12 GB.</p> <p>16 GB si está utilizando la eliminación de duplicados.</p> <p>Sistemas de 32 bits Windows 8 GB.</p> <p>No se admite la eliminación de duplicados.</p> <p>No se puede ejecutar más de una instancia del servidor en un sistema.</p>
	<b>DISCO</b>	<p>Al menos 3 GB de almacenamiento de disco disponible (para una instalación típica).</p> <p>200 MB de espacio en el directorio temporal.</p> <p>Una partición de 2 GB en la unidad C:\</p> <p>300 MB en el directorio de instancias</p>
<b>REQUISITOS CLIENTES</b>	<b>AIX</b>	<p>AIX V5.3 TL 5 and higher</p> <p>AIX V6.1</p> <p>AIX V7.1, TSM 6.2.2 mínimo.</p>
	<b>HP-UX ITANIUM</b>	<p>HP-UX 11i V2</p> <p>HP-UX 11i V3</p>
	<b>LINUX</b>	<p>SLES 11 (32-64 bit)</p> <p>SLES 10 (32-64 bit)</p> <p>RHEL 5 (32-64bit)</p> <p>RHEL 6 (32-64 bit), TSM 6.2.2 mínimo.</p>
	<b>MACINTOSH</b>	<p>Mac OS 10.5</p> <p>Mac OS 10.6</p>
	<b>SUN SOLARIS</b>	<p>Sun Solaris 10 SPARC</p> <p>Sun Solaris 10 x86/x86_64</p>
	<b>WINDOWS</b>	<p>Windows XP Professional (32 bit and 64 bit, SP 2 or later), excepto IA64</p> <p>Windows Server 2003 (todas las ediciones, 32 bit and 64 bit)</p> <p>Windows Server 2003 R2 (todas las ediciones, 32 bit and 64).</p>

		Windows Vista todas las ediciones Windows 2008 Server and Windows 2008 Server Core, todas las ediciones Windows Server 2008 R2 and Windows Server 2008 R2 Server Core, todas las ediciones.  Windows 7, todas las ediciones
	<b>Memoria</b>	Al menos 1 GB.
	<b>Disco</b>	El cliente requiere 1,5 GB de espacio de disco libre

**Tabla 3.2. Sistemas Operativos Soportados por TSM**  
Fuente. Personal

Requerimientos previos para la instalación de Microsoft System Data Protection Manager 2010 a nivel de servidor:

- ✓ Servidor Miembro de un dominio establecido.
- ✓ Usuario con privilegios de administración y modificación del registro del sistema.
- ✓ Usuario administrador de base de datos para MSSQL Server 2008 (en caso de disponer una instancia ya instalada).

	<b>WINDOWS</b>	Windows Vista Windows XP with Service Pack 2 Windows Server 2003 with Service Pack 2 (SP2) or later Windows Server 2008 R2 Windows Server 2008 Windows Server 2003 with Service Pack 2 (SP2) or later
	<b>MEMORIA</b>	Al menos 4 GB, recomendado 8 GB.

	<b>DISCO</b>	DPM directorio local: 3 GB. Base de Datos: 900 MB Controladores del Sistema: 1 GB
	<b>WINDOWS</b>	Windows Vista Windows XP with Service Pack 2 Windows Server 2003 with Service Pack 2 (SP2) or later Windows Server 2008 R2 Windows Server 2008 Windows Server 2003 with Service Pack 2 (SP2) or later
	<b>Memoria</b>	Al menos 2 GB.
	<b>Disco</b>	El cliente requiere 500 MB de espacio de disco libre

**Tabla 3.3. Sistemas Operativos Soportados por DPM**

Fuente. Personal

**3.1.2. Requerimientos a nivel de Respaldos.**

<b>AMANDA SOURCE BACKUP</b>	<b>TIVOLI STORAGE MANAGER</b>	<b>DATA PROTECTION MANAGER</b>
Espacio en disco suficiente, para albergar los respaldos de los clientes 5% más del total de los mismos.	Espacio en disco suficiente, para albergar los respaldos de los clientes 10% más del total de los mismos.	Espacio en disco suficiente, para albergar los respaldos de los clientes 5% más del total de los mismos.
Para uso de Medios Magnéticos como Cintas, nos proporciona un soporte de cintas todos los soportados por los diferentes sistemas operativos en los que se	Para uso de Medios Magnéticos como Cintas, nos proporciona un soporte de cintas desde unidades LTO2-LTO5, Autoloader, CD, DVD, cintas 8mm, 4mm, etc. soporta	Para uso de Medios Magnéticos como Cintas, nos proporciona un soporte de cintas LTO 4 – LTO5, con soporte para compresión por hardware.

puede instalar Amanda.	compresión a nivel de hardware.	
Amanda no utiliza drivers propietarios de dispositivos, cualquier dispositivo soportado por el sistema operativo será funcional con Amanda	Drivers Actualizados liberados por el fabricante del medio de almacenamiento	Drivers Actualizados liberados por el fabricante del medio de almacenamiento
Soporte para conexión por FIBRA, SAS y USB	Soporte para conexión por FIBRA, SAS y USB.	Soporte para conexión por, SAS y USB.
Instalación de Agentes en los clientes según la información a respaldar.	Instalación de Agentes en los clientes según la información a respaldar.	Instalación de Agentes en los clientes según la información a respaldar.
Versión sin costo alguno.	Versión con un costo elevado, parte desde los 1500 dólares.	Versión con un costo moderado,

**Tabla 3.4. Características de Almacenamiento.**  
Fuente. Personal.

### 3.1.3. *Requerimientos a nivel de Conectividad.*

<b>AMANDA SOURCE BACKUP</b>	<b>TIVOLI STORAGE MANAGER</b>	<b>DATA PROTECTION MANAGER</b>
Proporciona sus propios protocolos de red sobre TCP v4-v6 y UDP. No usa, por ejemplo, rsh o rdump/rmt. Cada programa cliente de copia de seguridad es instruido para grabar a la salida estándar, donde AMANDA recoge y transmite los datos copiados al servidor.	Al menos uno de los siguientes protocolos de comunicación (instalado por defecto con los sistemas operativos actuales de Windows): Named Pipes TCP/IP v4 - v6	Utilización de protocolo de conectividad TCP v4-v6, solamente.

Necesita un puerto privilegiado de red para una comunicación segura con los clientes y la unidad de cintas (Si existe alguna).	Necesita un único puerto privilegiado de red para una comunicación segura entre clientes y servidor.	Necesita un único puerto privilegiado de red para una comunicación segura entre clientes y servidor.
No soporta el uso de SAN (LAN FREE) para manejo de respaldos.	Soporte total para el uso de SAN (LAN FREE) para manejo de respaldos.	Soporte total para el uso de SAN (LAN FREE) para manejo de respaldos.

**Tabla 3.5. Características de Conectividad.**

**Fuente. Personal**

### **3.2. ADMINISTRACIÓN DE RESPALDOS**

La administración de Respaldos va orientada en este caso a como son definidas o como manejan las políticas para cada respaldo o grupo de respaldos.

Dichas políticas llevan consigo la configuración del número de versiones a mantener de un mismo archivo, medios que se utilizarán para almacenar los respaldos ya sea solo cintas solo disco o un mix de las dos tecnologías, clientes a los cuales afecta las políticas y registro de los mismos.

#### **3.2.1. Manejo de Políticas de Respaldo.**

<b>DESCRIPCIÓN</b>	<b>AMANDA SOURCE BACKUP</b>	<b>TIVOLI STORAGE MANAGER</b>	<b>DATA PROTECTION MANAGER</b>
Calendarización de Respaldos a Ejecutar en los Clientes.	Denominado Ciclo de copias. Límite máximo sobre con qué frecuencia se hacen las copias completas y parciales.	Denominado Planificaciones de Nodo Cliente, para especificar fechas de ejecución de respaldos.	Denominado Programación de Tareas, permite seleccionar fechas de calendario o periodos de copias tanto completas como incrementales.
Manejo de	Las versiones de	El Versionamiento	Las versiones las

Versionamiento de archivos respaldados.	archivos tienen relación con el ciclo de copias parciales ya que cada vez que se obtiene un nuevo respaldo completo las versiones vuelven a iniciar.	lo especifica el administrador del sistema y puede ir desde una versión hasta un número ilimitado de versiones.	define el usuario administrador y van de la mano tanto con la ejecución de un respaldo incremental como cuando se ejecuta un respaldo completo.
Tiempo de retención para respaldos y archivados de información de los clientes.	De igual manera está definida por el tiempo de ejecución de la copia completa de cada cliente.	Definida por el Administrador del Sistema y utiliza conceptos de la herramienta que son copias activas e inactivas.	Maneja copias denominadas de corta duración así como de larga duración para respaldos.
Manejo de respaldos a tape.	Los respaldos a Cinta no pueden superar el tamaño del medio de almacenamiento ya que la herramienta no soporta dividir un respaldo grande en varias cintas a la vez.	Los respaldos pueden ser almacenados en dos o más cintas según lo requiera el respaldo generado de manera automática.	Los respaldos pueden ser almacenados en dos o más cintas previamente asignadas al respaldo generado.
Creación de Medios de Almacenamiento ya sea espacio en disco o tape.	Puede utilizar un servidor dedicado para tape y/o disco conectado a la herramienta o agregar los dispositivos directamente al	Utiliza lo que se define como dispositivos de almacenamiento y agrupaciones de almacenamiento, para especificar tamaños y formas	Utiliza una o más particiones o unidades de cinta atachadas al servidor, en el caso de particiones de disco se agrega completamente el

	servidor de Amanda.	de almacenamiento.	espacio de los mismos.
Identificación de información de Clientes que será sujeta a respaldo.	Se instala el agente en cada cliente y se procede a configurar las carpetas y archivos a respaldar.	Se conoce como nodos clientes, utiliza un agente por cada equipo y un archivo de configuración para filtrar la información a respaldar.	Se instala un agente de manera remota o local para configurar la administración de los respaldos de los clientes.
Instalación de características especiales de respaldo como son respaldos para mail, base de datos, etc.	Esta versión solo soporta conectividad contra la base de datos My SQL Server, el resto de sistemas operativos es soportado a nivel de file system.	Instalación de un agente adicional conocido como Tivoli Data Protección for DataBase, Mail, ERP, FreeLan, etc.	Soporte exclusivo para sistemas operativos y aplicaciones Windows configurables para respaldar su información sin necesidad de agente adicional.
Proceso de De-duplicación de información	No soporta de-duplicación.	Soporte total para de-duplicación.	No soporta de-duplicación.

**Tabla 3.6. Manejo de Políticas de Respaldo.**

**Fuente. Personal**

### **3.2.2. Modelo de Respaldos Utilizado.**

Las tres herramientas aplican el mismo esquema de respaldos el mismo que eestá basado en el modelo denominado “Abuelo, Padre, Hijo” o GFS, que es muy utilizado ya que cubre la mayoría de las necesidades de backup, disaster recovery y archiving. Para archivados por largos períodos de tiempo, las cintas pueden ser administradas desde el esquema de rotación y remplazadas.

Una copia de seguridad generacional es uno de los métodos más simples y eficaces de crear y conservar copias de seguridad de los datos. Si se realiza correctamente, combina la facilidad de uso y la protección de datos.

En su forma más básica, implica realizar una copia completa de los datos que deben guardarse en un medio extraíble como, por ejemplo, cintas o CD. Este es el abuelo. En el siguiente período programado de copia de seguridad, por ejemplo al día siguiente, se realiza otra copia completa de los datos que, por supuesto, incluye los cambios realizados en los datos durante ese período. Es el padre. En la siguiente copia de seguridad programada, se produce la tercera copia, o hijo.

La cuarta copia de seguridad se realiza grabando encima (o sustituyendo, según el medio) la copia "abuelo". La nueva copia se convierte en "hijo", el hijo anterior pasa a ser el nuevo "padre", y el padre asciende a "abuelo". Esto continúa de manera rotatoria de manera que siempre hay tres copias de seguridad, cada una de ellas de un momento diferente.

La ventaja de guardar las dos copias de seguridad anteriores así como la actual es que, si los datos del equipo resultan dañados y el problema no es descubierto hasta después de realizar la copia de seguridad, aún quedan dos copias no dañadas, aunque cada vez más desfasadas en el tiempo. Si se presta una atención razonable, es improbable que un problema dañe las tres copias de seguridad antes de ser descubierto. De forma similar, si una de las copias de seguridad resulta dañada, aún quedan dos más. La copia de seguridad en tres generaciones también facilita el almacenamiento de una de las copias (generalmente la que es "abuelo") en un lugar más seguro y a menudo en una ubicación distinta. Se debe tener en cuenta que este enfoque no tiene en cuenta las copias de seguridad incrementales, sino que todas las copias de seguridad son completas.

Otro enfoque distinto consiste en crear una copia de seguridad completa que sirva como "abuelo". Digamos que esto se hace en domingo. La siguiente fecha para la copia de seguridad podría ser el domingo siguiente, cuando se crea la copia "padre", mientras que el "hijo" se crea una semana después. Puede seguir creando copias de seguridad incrementales todos los días entre copia y copia completa. De esta manera, en vez de perder una semana de datos, perdería como máximo un día, o los días transcurridos

desde que los datos resultaron dañados hasta que se descubrió el problema. Ello reduce aún más la posible pérdida y, como se utilizan copias de seguridad incrementales, las copias de seguridad diarias son mucho más rápidas que las completas.

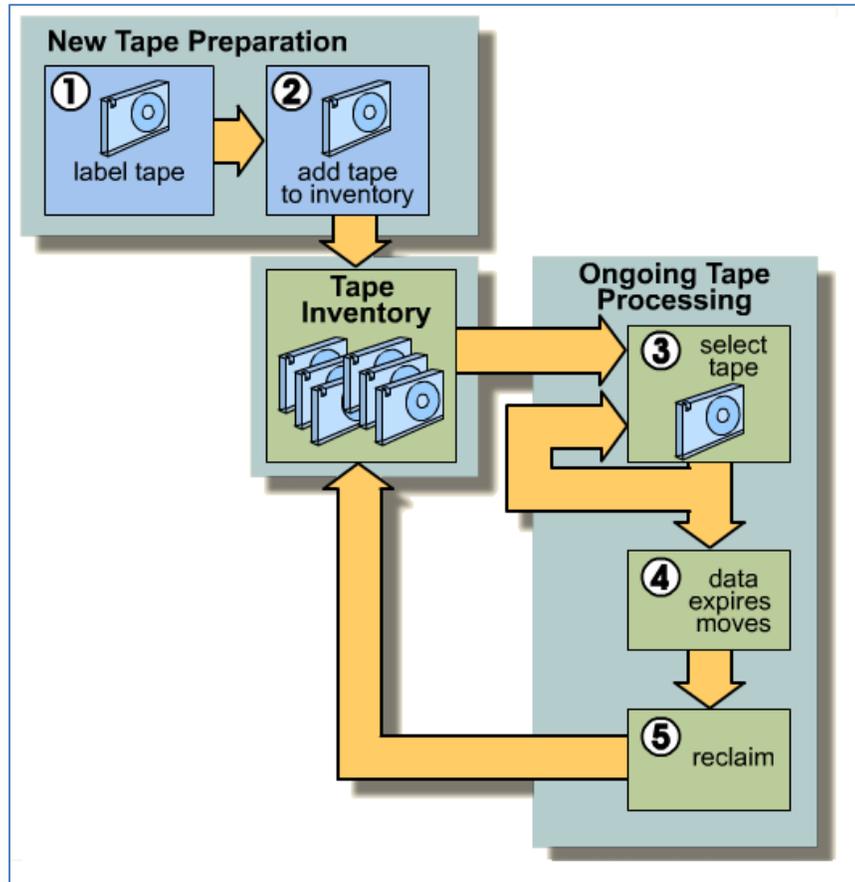


Figura 3.1. Manejo de Tapes

Fuente. [Web 10]

### 3.2.3. Flexibilidad de Configuración.

AMANDA SOURCE BACKUP	TIVOLI STORAGE MANAGER	DATA PROTECTION MANAGER
Instalación rápida sin complicaciones y sin configuraciones extensas, clientes rápidos de configurar.	Instalación rápida, configuraciones iniciales bastante complejas configuración de respaldos de cliente sencillas	Instalación rápida si se cumple con todos los requisitos, configuración sencilla, configuración de clientes en nivel medio de complejidad.

Administración vía consola del sistema operativo.	Administración sencilla, por consola y web.	Utilización de protocolo de conectividad TCP v4-v6, solamente.
Cambio de configuración del servidor y clientes rápida.	Configuraciones aplicables a clientes a través de un asistente de configuración o modificación del agente instalado.	Necesita un único puerto privilegiado de red para una comunicación segura entre clientes y servidor.
Nuevas configuraciones aplicables en tiempo real.	Nuevas configuraciones aplicables en tiempo real.	Nuevas configuraciones aplicables en tiempo real.
Proceso de restauración bajo demanda por consola del sistema del cliente.	Restauración desde el servidor, consola web del cliente o interface GUI del Cliente.	Restauración desde el cliente por uso de explorador de Windows.
Respaldos configurables para uso de compresión	Compresión por software o hardware desde el servidor o medios de almacenamiento.	Compresión por software o hardware desde el servidor o medios de almacenamiento.
Calendarización simple, solo por días transcurridos.	Calendarización a nivel de fecha y hora.	Calendarización a nivel de fecha y hora.
Soporte técnico inexistente, se puede utilizar blogs, Wikipedia para solventar dudas o configuraciones existentes.	Soporte especializado con un costo adicional, de parte del fabricante, por un canal asociado o por descarga de “RedBooks”.	Soporte especializado con costo adicional directamente con el fabricante, Wikipedia y blogs de información.
Parámetros Básicos modificables sobre el motor de Amanda.	Parámetros Avanzados modificables sobre el motor de TSM.	Parámetros Básicos modificables sobre el motor de Amanda.
Características especiales de respaldo para MYSQL, con alto nivel de complejidad.	Configuraciones para TDP, complejos y utiliza instaladores independientes.	Configuraciones sencillas para clientes especiales de base de datos o correo.

Al fallar un respaldo de un servidor cliente este se detiene y continuara en la siguiente ejecución desde el inicio.	Al fallar un respaldo de un nodo cliente este se detiene y continua desde el punto en el que fallo en la siguiente ejecución.	Al fallar un respaldo de un cliente este se detiene y continua desde el punto en el que fallo en la siguiente ejecución.
--	---	--

Tabla 3.7. Flexibilidad de Configuración.  
Fuente. Personal

### 3.2.4. Métodos de Administración.

Amanda Source Backup.

Amanda Source Backup, solo posee un método de administración el cual se ejecuta desde la consola de comandos de cualquier sistema operativo soportado por la herramienta.

La versión Amanda Network (con costo), posee un ambiente de administración basado en una interface web para facilitar la labor de configuración del servidor y de registro de sus servidores clientes.

```
# ./configure --with-user=amanda --with-group=backup
```

Figura 3.2. Línea de Comandos de Amanda Source Backup

Fuente. [Web 14]

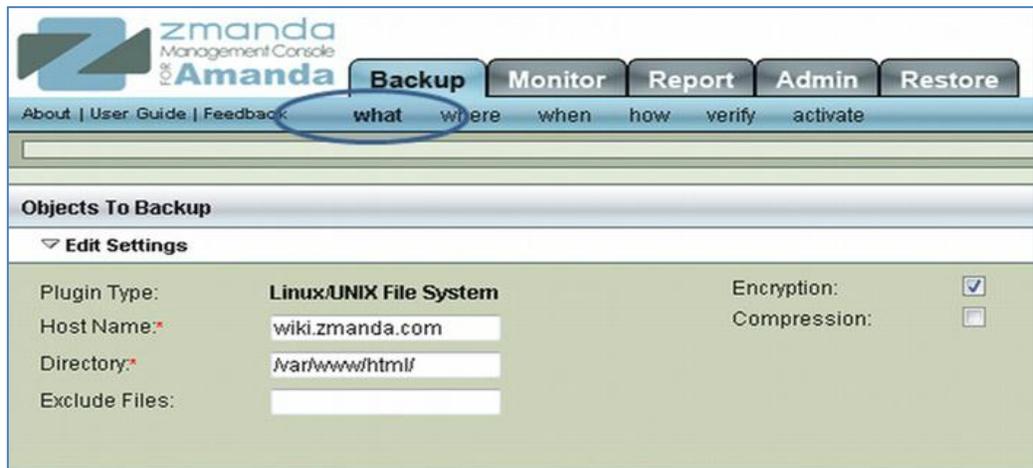
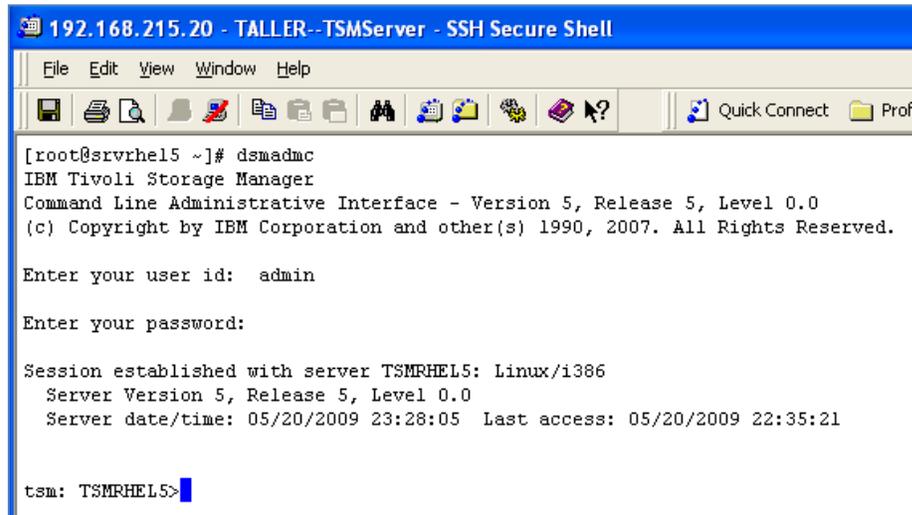


Figura 3.3. Interface de Administración Amanda Network.

Fuente. [Web 11]

Tivoli Storage Manager.

TSM, posee tres ambientes de administración dos de ellos se instalan conjuntamente con la herramienta servidor y una bajo demanda incluso puede ser instalada en un servidor completamente diferente del servidor base y puede administrar más de un servidor de TSM o instancias del mismo.



```
[root@srvrhel5 ~]# dsmadmc
IBM Tivoli Storage Manager
Command Line Administrative Interface - Version 5, Release 5, Level 0.0
(c) Copyright by IBM Corporation and other(s) 1990, 2007. All Rights Reserved.

Enter your user id: admin

Enter your password:

Session established with server TSMRHEL5: Linux/i386
Server Version 5, Release 5, Level 0.0
Server date/time: 05/20/2009 23:28:05 Last access: 05/20/2009 22:35:21

tsm: TSMRHEL5>
```

Figura 3.4. Línea de Comandos de TSM.

Fuente. Personal

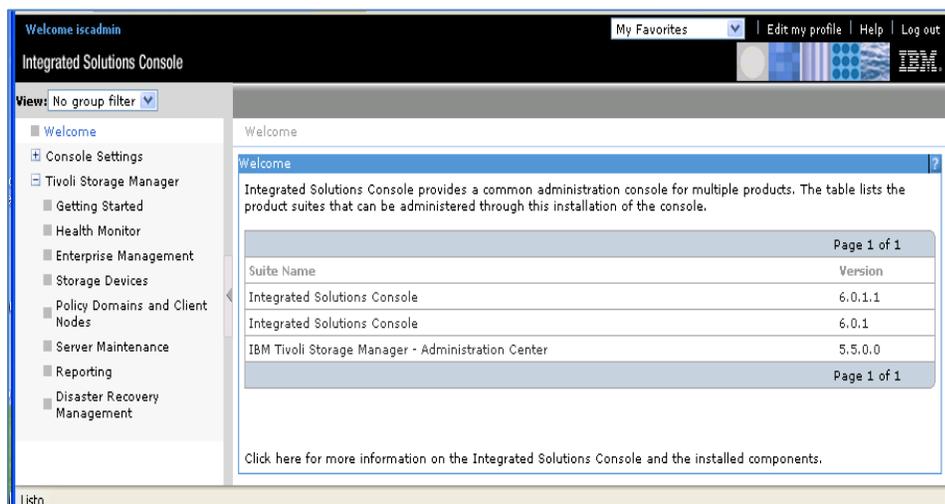


Figura 3.5. Interface Web de Administración de TSM

Fuente. Personal

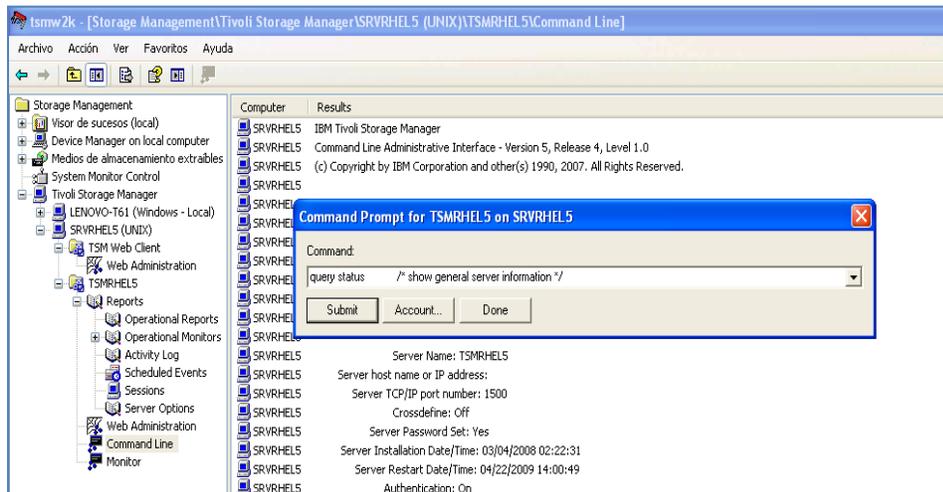


Figura 3.6. Interface GUI de Administración Windows.

Fuente. Personal

Data Protection Manager.

DPM, instala una consola GUI de administración de respaldos conjuntamente con la instalación del servidor de DPM y la base de datos MSSQL, esta consola solo puede utilizarse o acceder a ella desde el mismo servidor de respaldos.

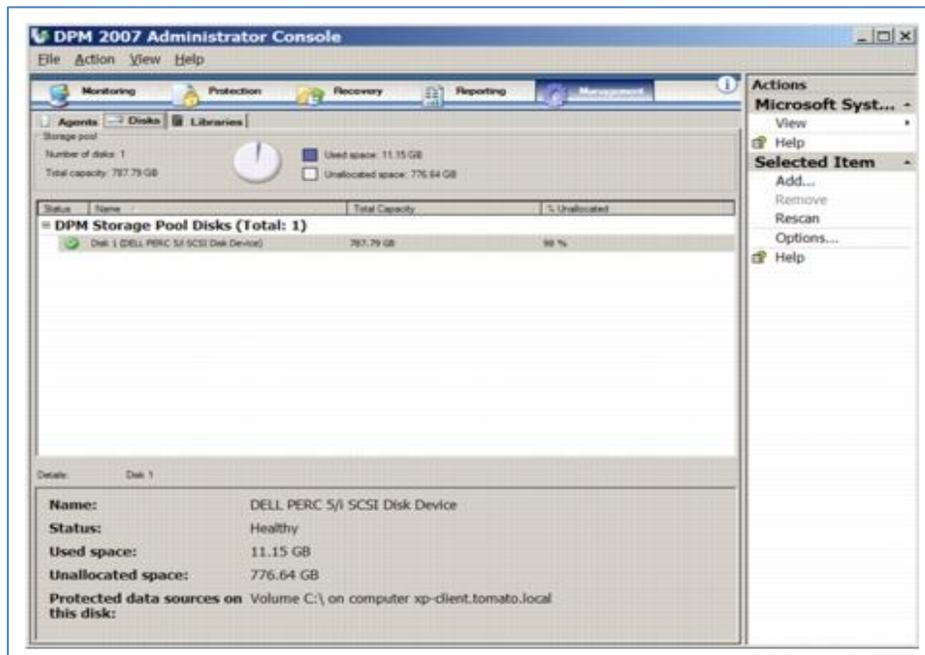


Figura 3.7. Interface de Administración GUI de DPM.

Fuente. Personal

### 3.3. Comparativas de las Herramientas

#### 3.3.1. Principales diferencias y similitudes.

CARACTERÍSTICA	AMANDA SOURCE BACKUP	TIVOLI STORAGE MANAGER	DATA PROTECTION MANAGER
Tema 3.2.4 Referente a: Tipos de Administración.	Administración mediante Consola de Comandos de Linux	Administración Web de uno o más servidores o instancias de TSM.	Administración desde una interface GUI del sistema operativo.
Tabla 3.1 Tabla 3.2 Tabla 3.3 Referente a: Sistemas Operativos Soportados	Soporta Sistemas Operativos Windows, Linux, Mac y Solaris.	Soporta Sistemas Operativos Windows, Linux, Mac, Solaris, AIX y Linux for Power.	Soporta Única y Exclusivamente Sistemas Operativos Windows.
Tabla 3.4 Referente a: Costo de Licenciamiento	Versión sin costo alguno.	Versión con un costo elevado, parte desde los 1500 dólares.	Versión con un costo moderado, parte desde los 600 dólares.
Tabla 3.4 Referente a: Drivers Soportados.	Amanda no necesita instalación de drivers de terceros para manejar dispositivos de almacenamiento, si el sistema operativo lo detecta, Amanda puede hacer uso de él.	Se necesita la instalación de drivers de terceros acordes al sistema operativo, para poder hacer uso de los dispositivos de almacenamiento.	Puede utilizar los dispositivos de almacenamiento, detectados en el sistema operativo o se puede utilizar drivers de terceros.
Tabla 3.6 Referente a:	Soporte solo para MYSQL.	Soporta múltiples bases de datos,	Soporta aplicaciones solo

Respaldos “ON-LINE” soportados.		correos y sistemas operativos.	en Windows y como fabricante Microsoft.
Tabla 3.6 Referente a: Manejo de Respaldo a Cintas	Los respaldos a Cinta no pueden superar el tamaño del medio de almacenamiento ya que la herramienta no soporta dividir un respaldo grande en varias cintas a la vez.	Los respaldos pueden ser almacenados en dos o más cintas según lo requiera el respaldos generado de manera automática.	Los respaldos pueden ser almacenados en dos o más cintas previamente asignadas al respaldo generado.
Tabla 3.6 Referente a: Deduplicación.	No soporta de-duplicación.	Soporte total para de-duplicación.	No soporta de-duplicación.
Tabla 3.7 Referente a: Soporte Técnico.	Soporte técnico inexistente, se puede utilizar blogs, Wikipedia para solventar dudas o configuraciones existentes.	Soporte especializado con un costo adicional, de parte del fabricante, por un canal asociado o por descarga de “RedBooks”.	Soporte especializado con costo adicional directamente con el fabricante, Wikipedia y blogs de información.
Tabla 3.7 Referente a: Manejo de Respaldos	Al fallar un respaldo de un servidor cliente este se detiene y continuara en la siguiente ejecución desde el inicio.	Al fallar un respaldo de un nodo cliente este se detiene y continua desde el punto en el que fallo en la siguiente ejecución.	Al fallar un respaldo de un cliente este se detiene y continua desde el punto en el que fallo en la siguiente ejecución.
Tabla 3.7	Instalación rápida	Instalación rápida,	Instalación rápida

Referente a: Instalación y Configuración.	sin complicaciones y sin configuraciones extensas, clientes rápidos de configurar.	configuraciones iniciales bastante complejas configuración de respaldos de cliente sencillas.	si se cumple con todos los requisitos, configuración sencilla, configuración de clientes en nivel medio de complejidad.
---	---	--	---

**Tabla 3.8. Principales Diferencias entre Herramientas.**

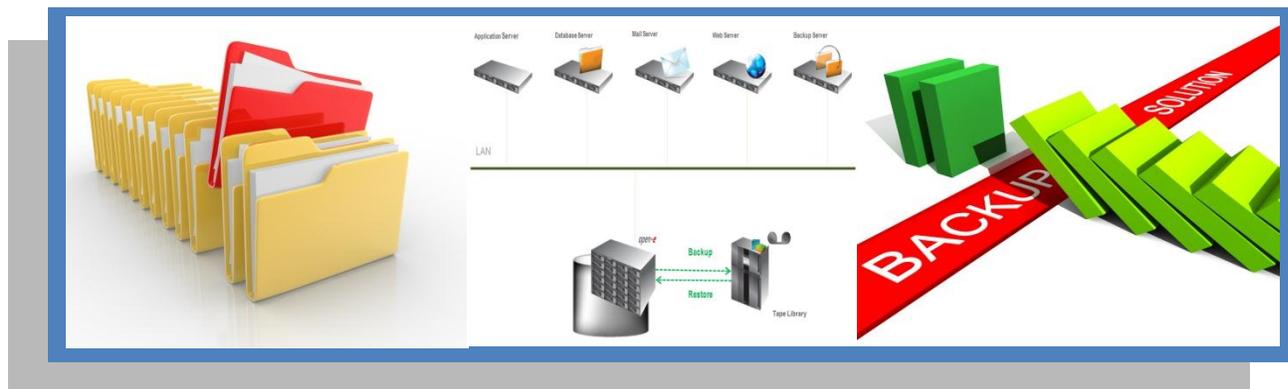
**Fuente. Personal**

#### Principales Similitudes.

- ✓ Utilizan el modelo GFS, para administrar los respaldos de servidores clientes como la manipulación de los dispositivos de cinta.
- ✓ Administran respaldos de servidores a través de un agente que se configura e instala en cada servidor a respaldar.
- ✓ Soporte para diferentes medios de almacenamiento, de diferentes fabricantes y medios de conexión ya sea mediante fibra, usb o sas.
- ✓ Administración centralizada de respaldos.
- ✓ Visualización de reportes acerca del estado de los medios de almacenamiento sean disco o cintas, estado de los respaldos, clientes asociados a la herramienta y espacio utilizado total e individual.
- ✓ Soportan el manejo de encriptación de datos desde la consola central y aplica a cada servidor.
- ✓ Manejan información propia para realizar tareas de “Archive” de información.
- ✓ Soporte para utilización de “colocación por cliente”.

- ✓ Ejecución de respaldos de manera calendarizada por días.
- ✓ Soporte para compresión de datos, cada vez que se genera un respaldo o archivamiento de información.
- ✓ Creación de Políticas de Respaldos para un servidor o grupos de servidores a respaldar.
- ✓ Proceso de Restauración de Archivos de tipo granular, es decir permite seleccionar desde un archivo hasta una carpeta o disco completo.

## CAPÍTULO 4.



## IMPLEMENTACIÓN, ACEPTACIÓN Y PRUEBAS DE LA HERRAMIENTA

#### 4.1. ACTIVIDADES BÁSICAS

Una vez analizadas las ventajas y desventajas de cada herramienta y comparado con los requerimientos de la empresa se obtuvo lo siguiente.

Requisitos del Negocio	Aranda Source Backup	Tivoli Storage Manager	Data Protection Manager
Respaldos de Base de Datos Microsoft SQL Server 2005		X	X
Respaldos de Base de Datos MY Sql Server	X	X	
Respaldos de File Systema Red Hat Enterprise Linux 5.5	X	X	
Respaldos de File System Ubuntu 10	X	X	
Calendarización para Respaldos Automáticos por Fecha		X	X
Calendarización para Respaldos Automáticos por Días	X	X	X
Calendarización para Respaldos Automáticos por Horas		X	X
Calendarizadas para Respaldos.			
Soporte Para utilización de varias cintas o varios espacios de disco en un solo Respaldo.		X	X
Soporte para compresión de ser necesario.	X	X	X
Administración de Respaldos tipo Full e Incremental o Diferencial	X	X	X
Administración centralizada.	X	X	X
Registro, Reportes de Respaldos Realizados y Fallidos.	X	X	X
% de Cumplimiento	66,66 %	100 %	75 %

Tabla 4.1. Cumplimiento de Requisitos del Negocio.

Fuente. Personal

Herramienta selecciona para proceder con la implementación es IBM Tivoli Storage Manager v6.2, sobre un ambiente Windows como servidor principal.

## 4.2. CONFIGURACIÓN SEGÚN REQUERIMIENTOS DE LA COMPAÑÍA.

A continuación se ilustra la configuración requerida por la empresa aplicando la herramienta seleccionada.

### 4.2.1. Instalación de Cliente Linux / Ubuntu / Windows.

La instalación del cliente de TSM es relativamente sencilla se detalla a continuación:

- ✓ Disponer de las versiones necesarias para la instalación en este caso:
  - TIVsm-API.i386.rpm.
  - TIVsm-API64.i386.rpm (para sistemas operativos de 64 bits).
  - TIVsm-BA.i386.rpm

Linux.

- ✓ Desde una consola de comandos del sistema operativo digitamos:
  - rpm -ivh TIVsm-API.i386.rpm.
  - rpm -ivh TIVsm-API64.i386.rpm (para sistemas operativos de 64 bits).
  - rpm -ivh TIVsm-BA.i386.rpm

Ubuntu.

- ✓ Cambiamos de formato de rpm a deb para poder instalarlo.
  - alien -d \*.rpm
- ✓ Se procede a instalar los nuevos paquetes .deb.
  - dpkg -i \*.deb

Windows

- ✓ Ejecutamos el instalador de TSM para Windows y seguimos el asistente de instalación.
  - 6.2.3.0-TIV-TSMBAC-WinX32.exe
  - 6.2.3.0-TIV-TSMBAC-WinX64.exe (para sistemas basados en 64 bits).

- ✓ Se procede a configurar los archivos de configuración de los clientes:

```
dsm.opt  
  
SErvername      RHEL55_server1
```

Figura 4.1. Configuración Archivo dsm.opt (Linux)  
Fuente. Personal

```
dsm.sys  
  
SErvername      RHEL55_server1  
COMMethod      TCPip  
TCPport        1500  
TCPserveraddress 172.20.1.75  
Passwordaccess generate  
Editor         yes  
  
NODENAME       client
```

Figura 4.2. Configuración Archivo dsm.sys (Linux)  
Fuente. Personal

Linux y Ubuntu.

- ✓ Archivos de configuración ubicados en la ruta /opt/Tivoli/tsm/client/ba/bin o /opt/Tivoli/tsm/client/ba/bin64 (para sistemas operativos de 64 bits).

Windows

- ✓ Archivo único de configuración existente en la ruta c:\Archivos de Programa\Tivoli\TSM\baclient\ , c:\Archivos de Programa(x86)\Tivoli\TSM\baclient\ , c:\Program Files\Tivoli\TSM\baclient\ o c:\Program Files(x86)\Tivoli\TSM\baclient\

```
dsm.opt  
  
COMMethod      TCPip  
TCPport        1500  
TCPserveraddress 10.1.1.92  
Passwordaccess generate  
  
NODENAME       client
```

Figura 4.3. Configuración Archivo dsm.opt (Windows)  
Fuente. Personal

#### 4.2.2. Instalación de Cliente MYSQL y Microsoft SQL Server.

La configuración para la Base de Datos MYSQL es la siguiente:

- ✓ Compilamos el utilitario ADSM-PIPE para soporte de MYSQL.
  - En la carpeta donde se descomprimió del archivo ejecutamos “MAKE”
- ✓ Una vez compilado, procedemos a utilizar los comandos propios de MYSQL.
  - `mysqldump [[-u <username>] [-p <password>]] [-h <mysqlhost>] [<database>] | adsmpipe -f /mysqldb -c`

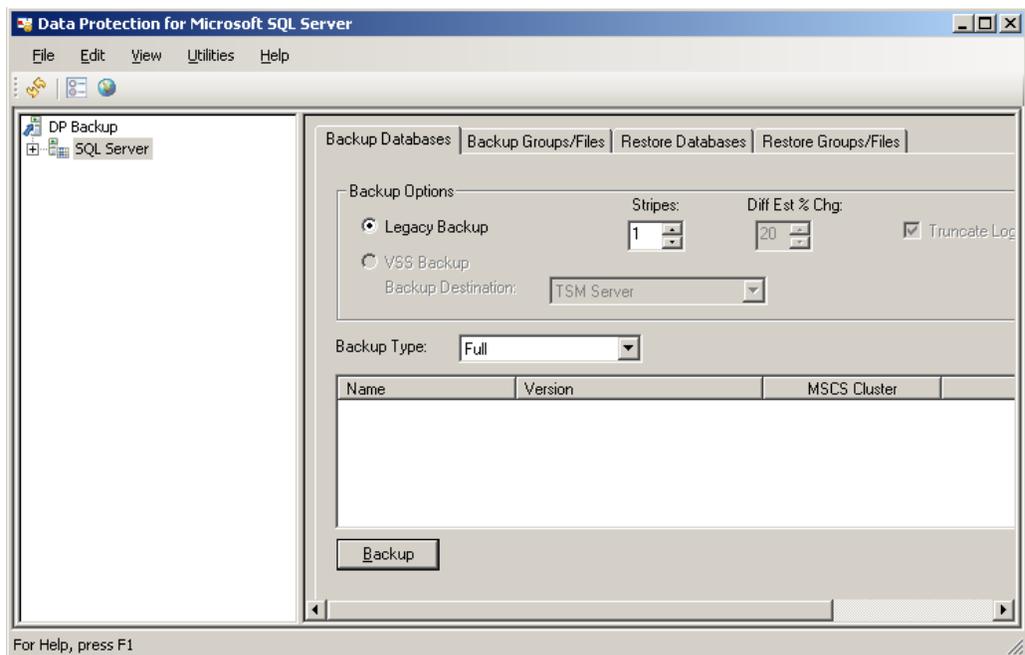
La configuración para la Base de Datos Microsoft SQL Server es la siguiente:

- ✓ Ejecute el instalador para TSM data Protection for DataBase en este caso Microsoft SQL Server.
  - IBM Tivoli Storage Manager for Databases V5.5 (Data Protection for MSSQL).rar
- ✓ Una vez terminado el asistente de instalación proceda a configurar el cliente de la siguiente manera:
  - Para proceder a utilizar el cliente de Tivoli Storage Manager para protección de datos de SQL Server, es necesario configurar algunos parámetros del archivo `dsm.opt` ubicado bajo el directorio de instalación de TDP for Databases.
  - Primero copiamos el archivo “**dsm.smp**” como “**dsm.opt**” y editamos varios de los parámetros por ejemplo:

<b>NODENAME</b>	<b>srvwin2003</b>
<b>PASSWORDAccess</b>	<b>generate</b>
<b>COMMMethod</b>	<b>TCPIP</b>
<b>TCPServeraddress</b>	<b>192.168.215.20</b>
<b>TCPPort</b>	<b>1500</b>
<b>TCPWindowSize</b>	<b>63</b>
<b>TCPBuffSize</b>	<b>32</b>
<b>COMPRESSIon</b>	<b>no</b>

<b>SCHEDLOGRetention</b>	<b>14</b>
<b>SCHEDMODE</b>	<b>Prompted</b>
<b>TCPCLIENTADDRESS</b>	<b>192.168.215.30</b>
<b>INCLUDE “\...\meta\...\*”</b>	<b>MC_SQL</b>
<b>INCLUDE “\...\data\...\*”</b>	<b>MC_SQL</b>
<b>INCLUDE “\...\meta\...\log*”</b>	<b>MC_SQL</b>
<b>INCLUDE “\...\data\...\log*”</b>	<b>MC_SQL</b>
<b>EXCLUDE “\...\master\...\log*”</b>	
<b>EXCLUDE “\...\msdb\...\log*”</b>	

- Tras editar y guardar los cambios en el archivo dsm.opt, procedemos a ejecutar el “SQL Client-GUI” de Tivoli Storage Manager Data Protection for SQL Server:



**Figura 4.4. Interface GUI de MSSQL Server.**

**Fuente. Personal.**

- Procedemos a cambiar las opciones de login hacia SQL Server:

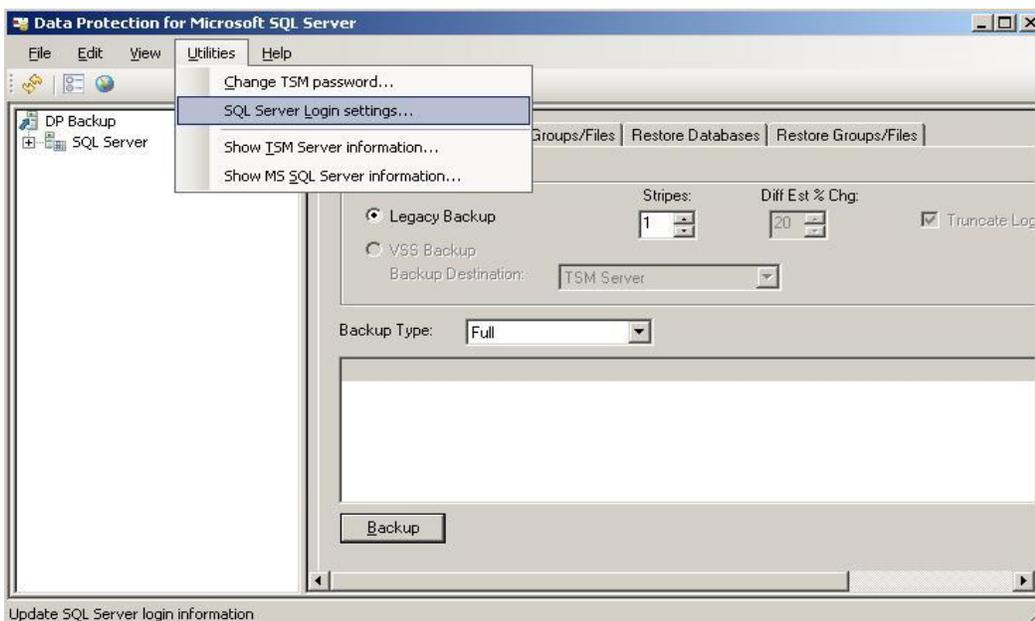


Figura 4.5. Configuración de Clave de MSSQL.

Fuente. Personal

- Una vez establecida la comunicación desde TDP for Databases hacia TSM y configurado el archivo **tdpsql.cfg**, escogemos una de las bases de datos para realizar una prueba de backup and restore.

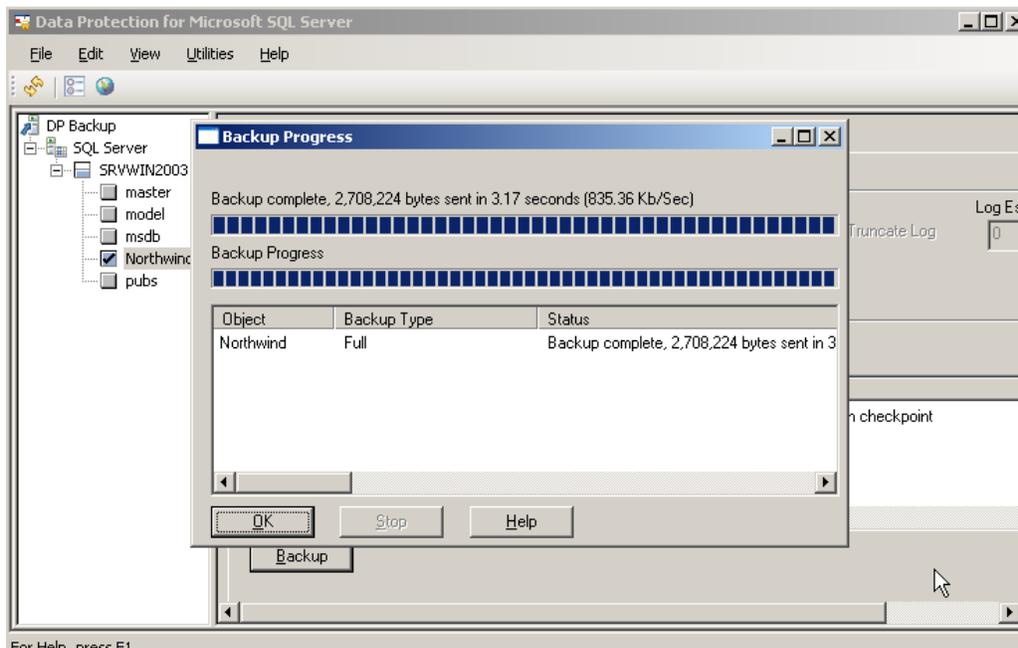


Figura 4.6. Ejemplo de Respaldo de MSSQL Server.

Fuente. Personal

### **4.3. MANTENIMIENTO DE LA HERRAMIENTA.**

El mantenimiento de la herramienta se realiza a través de:

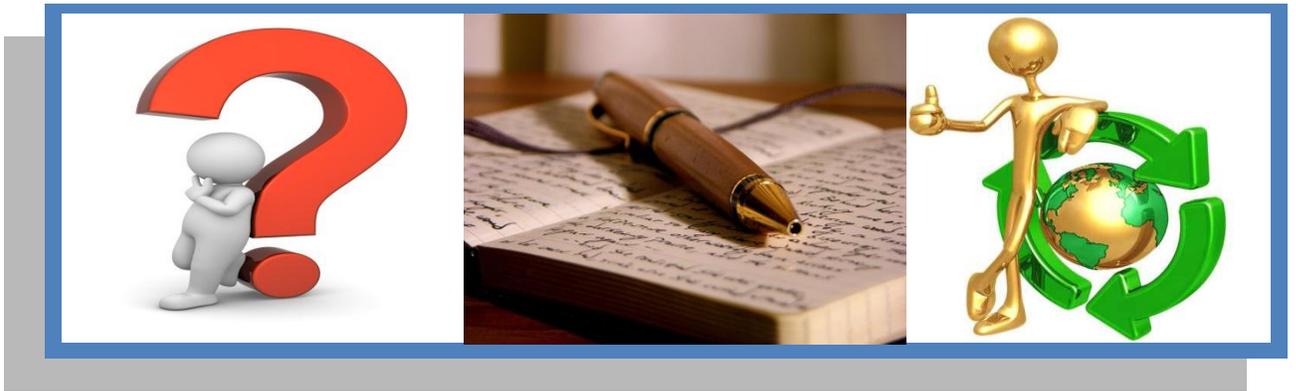
- ✓ Respaldos diarios sobre la configuración de la base de datos de TSM, mediante:
  - backup db devclass=fileclass type=full scratch=yes
  
- ✓ Borrado de respaldos anteriores a 5 días atrás es decir que se podrá restaurar al servidor de TSM hasta 5 días a tras luego de una pérdida total de toda configuración del servidor.
  - el volh todote=today-5 type=dbbackup
  
- ✓ Respaldos diarios de los archivos de configuración del servidor de TSM.
  - backup devconfig filenames=devcnfg.out
  - backup volhistory filenames=volhist.out
  
- ✓ Monitoreo de los Respaldos Generados en busca de errores, fallas o warning.
  - q act search=fail
  - q act search=error
  - q act search=warning

### **4.4. PRODUCCIÓN**

Después de las pruebas realizadas en la configuración de la herramienta seleccionada en este caso IBM Tivoli Storage Manager v6.2, y solucionado errores que se han presentado, se procede a detener todas las tareas y eliminar los scripts antes creados para realizar respaldos manualmente o semi-automatizado de los servidores presentes en la empresa, dando control total al ambiente de administración de TSM.

Con esta decisión se está monitoreando constantemente los procesos para detectar posibles fallos o inconsistencias en el envío de datos al Servidor de TSM y a los clientes conectados a él.

## CAPÍTULO 5.



## CONCLUSIONES Y RECOMENDACIONES

## 5.1. CONCLUSIONES

Las herramientas de código abierto en ciertas circunstancias nos pueden ayudar a satisfacer necesidades de una maneja ágil y a muy bajos costos, pero una vez que aparecen requerimientos puntuales del negocio y la necesidad de crecimiento nos podemos ver en la necesidad de actualizar a una versión comercial o cambiarnos a una nueva herramienta que soporte nuestras necesidades.

Por su parte la utilización de herramientas propietarias nos asegura atención oportuna sobre consultas, configuraciones o resolución de errores de una manera más efectiva, con lo que se reducen costos de operación al intentar configurar una aplicación desde cero o tratar de recuperar información perdida o borrada por equivocación.

Al inmiscuirse en un tema tan importante como es el salvaguardo de información, una de las principales dificultades que se presentan es el alto costo por la adquisición de este tipo de herramientas conjuntamente con el hardware que lo soporta, pero se debe tomar en cuenta el beneficio que otorga al momento de la recuperación rápida ante desastres y el ahorro significativo que se verá reflejado en la empresa al no perder su información o el core del negocio.

El estudio realizado en este documento nos ayuda a conocer algunos conceptos adicionales sobre el manejo adecuado de respaldos con lo que podemos estar plenamente seguros que el proceso de respaldar información no es simplemente el hecho de grabar una copia de toda la información disponible en el negocio, en un medio de almacenamiento masivo.

Se ha logrado llegar a un punto de automatización utilizando la herramienta elegida, para el registro de tareas de respaldo (reportes y logs), calendarización de respaldos, la herramienta es accesible desde cualquier punto en la organización, se ha llegado a automatizar las tareas de respaldos en gran medida, reemplazando las tareas manuales.

Se ha demostrado que hoy por hoy el manejo de información es un punto crítico en el desenvolvimiento de toda organización y es un pilar fundamental para que exista continuidad del negocio, por lo cual se debe sustentar con el uso de software acorde al avance tecnológico.

## 5.2. RECOMENDACIONES

Si se ha elegido una herramienta de código abierto, para solventar las necesidades internas de la empresa, se debe tomar en cuenta las limitaciones de la misma en cuanto a sus funcionalidades con respecto a una versión comercial.

En uso de un software comercial ayuda en gran medida el tener un punto de apoyo estable en caso de necesitar configuraciones especiales, o requerimientos puntuales, pero es necesario delimitar las necesidades para no caer en costos adicionales innecesarios.

Del estudio presentado, se recomienda antes de elegir una herramienta de salvaguardo de información se tenga en cuenta las necesidades primordiales de la empresa y a su vez saber diferenciar que podemos tener empresas similares en cuanto a infraestructura de servidores y aplicaciones pero completamente diferentes al conocer más a fondo el tipo de información que maneja.

Se recomienda realizar un análisis de que información se necesita proteger y de aquella información que se podría prescindir en el caso de un evento fortuito, para poder abaratar costos.

El administrador de la herramienta debe ser capaz de responder con rapidez, ante solicitudes de servidores o usuarios, para tener acceso a su información o recuperación de la misma.

La automatización del proceso de respaldos y calendarizaciones van de la mano con la correcta manipulación y verificación de la herramienta, se recomienda que cada cambio en la configuración o procesos de mantenimientos de los servidores sean claramente programados y registrados de ser factible fuera de horarios de carga transaccional para interrumpir el un porcentaje mínimo el desempeño de las actividades cotidianas.

La revisión diaria de las tareas de respaldo debe ser un tema primordial, para poder encontrar errores o fallar de dichos procesos y a su vez poder tomar acciones correctivas oportunamente.

La herramienta que se elija debe ser flexible, es decir no se debe atar a un solo tipo de aplicaciones o de sistemas operativos ya que nos veríamos limitados al momento de necesitar otro tipo de servicios que se presentes como requerimientos de la empresa.

### **5.3. POSIBLES TEMAS**

- ✓ Estudio y manejo del concepto de “DE-DUPLICACIÓN”.
- ✓ Estudio y manejo de respaldos a través del uso de una SAN (LAN Free).
- ✓ Estudio y recomendaciones al respaldar información a medios magnéticos.
- ✓ Implementación de Ambientes de Trabajo con HSM (Hierarchical Storage Manager).
- ✓ Estudio y manejo de respaldos de Ambientes Virtualizados.
- ✓ Implementación de un Clúster a nivel de base de datos para alta disponibilidad a nivel de Tivoli Storage Manager Server.

## GLOSARIO.

### Agente de Almacenamiento

Programa que permite a Tivoli Storage Manager realizar copias de seguridad y de los datos de cliente directamente en un almacenamiento conectado a través de una red SAN y restaurarlos de éste.

### Agente de Comunicación de Confianza

Programa que realiza tareas de comunicación en nombre del cliente o del servidor y garantiza la seguridad de las comunicaciones.

### Agrupación de Almacenamiento

Conjunto de volúmenes de almacenamiento, al que se da un nombre, que TSM utiliza para almacenar datos de clientes. Una agrupación de almacenamiento puede ser una agrupación de almacenamiento primaria o una agrupación de almacenamiento de copia.

### Almacenamiento de Servidor

Agrupaciones de almacenamiento primarias y de copia que el servidor utiliza para almacenar archivos de los usuarios: versiones de copia de seguridad, copias archivadas y archivos migrados desde nodos cliente (archivos bajo gestión de espacio).

### Amandahosts

Nombre del archivo de configuración para cliente de Amanda.

### Anotación Cronológica de empresa

Envío de eventos de servidores de IBM Tivoli Storage Manager a un servidor de eventos designado. El servidor de eventos dirige los eventos a receptores designados, como por ejemplo a una salida de usuario. Véase también evento.

### Anotaciones de Actividades

Archivo de anotaciones que registra mensajes de actividades normales generados por el servidor. Estos mensajes contienen información relativa a las operaciones del servidor y de los clientes, como por ejemplo, la hora de inicio de las sesiones o errores de E/S de dispositivos. Cada mensaje contiene un ID de mensaje, una indicación de la fecha y la hora, y un texto

descriptivo. Se puede especificar el número de días que se desea conservar los mensajes en las anotaciones de actividades

#### Anotaciones de recuperación

Anotaciones de actualizaciones que se van a grabar en la base de datos. Las anotaciones pueden utilizarse para realizar la recuperación de errores del sistema y de errores de medios de almacenamiento.

#### API

Application Programming Interface, interface gráfica para sistemas operativos soportados por las herramientas incluido el servidor.

#### Archivamiento

Proceso de salvaguardo de información que no cambiará en un lapso largo de tiempo, archivamiento prolongado a razón de años.

#### Autoloader

Hardware de administración de tape, cartuchos LTO, DM, etc.

#### BladeCenter

Chasis, que contiene solución de servidores a manera de cuchillas y almacenamiento en disco en algunos modelos, tarjetas de fibra, tarjetas SAS, etc.

#### Capacidad Estimada

Espacio disponible, en megabytes, de una agrupación de almacenamiento. Clase de dispositivo. Conjunto de características, con nombre, que se aplica a un grupo de dispositivos de almacenamiento. Cada clase de dispositivo tiene un nombre exclusivo y representa un tipo de dispositivo de disco, archivo, disco óptico o cinta.

#### Checksum

Una simple detección de errores de esquema en el que cada mensaje transmitido se acompaña de un valor numérico basado en el número de bits en el mensaje hacia la estación receptora y luego se aplica la misma fórmula para el mensaje y comprueba para asegurarse de que el valor

numérico correspondiente es el mismo. Si no, el receptor puede asumir que el mensaje ha sido corrupto.

## CISC-RISK

RISC (del inglés Reduced Instruction Set Computer, en español Computador con Conjunto de Instrucciones Reducidas) es un tipo de diseño de CPU generalmente utilizado en microprocesadores o microcontroladores.

## Clase de Gestión

Objeto de política que los usuarios pueden vincular a cada archivo para especificar cómo el servidor gestiona el archivo. La clase de gestión puede contener un grupo de copia de seguridad, un grupo de copia archivada y atributos de gestión del espacio. Los grupos de copia determinan cómo el servidor gestiona las versiones de copia de seguridad o las copias archivadas del archivo. Los atributos de gestión de espacio determinan si el cliente del gestor de espacio puede migrar el archivo al almacenamiento del servidor y en qué condiciones. Véase también grupo de copia, cliente de gestor de espacio, vincular y volver a vincular.

## Cmdlets

Por ejemplo, el nombre de cmdlet Get-SPSite combina el verbo (comando) "Get" con el nombre (objeto) "SPSite" para denominar al cmdlet que recupera un objeto SPSite especificado. Puede usar los cmdlets individualmente o unirlos como secuencias vinculadas para realizar tareas complejas.

## CMS

Es un Sistema de gestión de contenidos es un programa que permite crear una estructura de soporte ( framework, o marco de trabajo) para la creación y administración de contenidos por parte de los participantes principalmente en páginas web.

## Configuración Empresarial.

Función que permite al administrador distribuir la configuración de un servidor de TSM a otros servidores utilizando comunicación servidor a servidor

## CRM

El CRM corresponde a las siglas Customer Relationship Management, gestión de las relaciones con el cliente, el CRM no es una nueva filosofía de trabajo u organización, sino el resultado de unir las antiguas técnicas comerciales de los pequeños establecimientos, con la tecnología de la información

## Crontab

Crontab es impulsado por un crond, un archivo de configuración que especifica comando shell para ejecutarse periódicamente a una hora específica. Los archivos crontab son almacenados en donde permanecen las listas de trabajos y otras instrucciones para el demonio cron.

## D2D2T

Definición de formas de respaldos, es decir Disco to Disco to Tape.

## D2T

Definición de formas de respaldos, es decir Disco to Tape.

## DAS

DAS (Direct Attached Storage) es una tecnología de almacenamiento que se utiliza para aumentar la capacidad de almacenamiento de un servidor.

## DRM

Nombre abreviado de Gestor de recuperación ante siniestro de Tivoli.

## Dump cycle

Definición que se da al tiempo máximo entre copias de seguridad.

## ERP

ERP es un término genérico para un conjunto de actividades ejecutadas por un software multi-modular, que tiene por objetivo ayudar a los administradores de una empresa en las fases importantes de su negocio, incluyendo el desarrollo de productos, compra ventas de ítems, mantenimiento de stocks, interacción con los proveedores, servicios a clientes y seguimiento de órdenes de producción.

## Gestor de configuración

Servidor de TSM que distribuye información de configuración a otros servidores de TSM (denominados servidor gestionado) mediante perfiles. Dicha información puede incluir políticas y planificaciones

## GUI

Siglas de Graphical User Interface (interfaz gráfica de usuario).

## HSM

Un HSM es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas y suele aportar aceleración hardware para operaciones criptográficas. Estos dispositivos pueden tener conectividad SCSI / IP u otras y aportar funcionalidad criptográfica de clave pública (PKI) de alto rendimiento que se efectúa dentro del propio hardware.

## InfiniBand

Especificaciones para un tipo de bus de comunicaciones en serie de alta velocidad diseñado para conexiones internas y externas. Es usado en computadoras de alto rendimiento, y fue diseñado para ser "escalable" (ampliable).

## iSCSI

iSCSI (Abreviatura de Internet SCSI) es un estándar que permite el uso del protocolo SCSI sobre redes TCP/IP. iSCSI es un protocolo de la capa de transporte definido en las especificaciones SCSI-3.

## Kerberos

Es un protocolo de autenticación de redes de ordenador creado por Gerard Phillip Kominek que permite a dos computadores en una red insegura demostrar su identidad mutuamente de manera segura. Sus diseñadores se concentraron primeramente en un modelo de cliente-servidor, y brinda autenticación mutua: tanto cliente como servidor verifican la identidad uno del otro.

know how

El Know-How (del inglés saber-cómo) o Conocimiento Fundamental es una forma de transferencia de tecnología. Es una expresión anglosajona utilizada en los últimos tiempos en el comercio internacional para denominar los conocimientos preexistentes no siempre académicos, que incluyen: técnicas, información secreta, teorías e incluso datos privados (como clientes o proveedores).

Modalidad de Planificación

Método de interacción entre un servidor y un cliente para ejecutar operaciones planificadas en el cliente

Modalidad de Planificación de Sondeo de Clientes

Técnica de comunicaciones de cliente/servidor en la que el cliente consulta trabajos en el servidor. Compárese con modalidad de planificación por petición de servidor.

Modalidad de Planificación por Petición de Servidor

Técnica de comunicación cliente/servidor en la que el servidor contacta con el cliente cuando debe realizarse una operación planificada. Compárese con modalidad de planificación de sondeo de clientes.

MT

Comando de sistemas basados en Unix que se utiliza para montar dispositivos.

MVS

Uno de los sistemas primarios de IBM, uno de los primeros sistemas utilizados por el mismo.

Named Pipes

Protocolo de comunicaciones integrado en el sistema operativo Windows NT u OS/2. Puede utilizarse para establecer comunicaciones entre un servidor de TSM y cualquiera de los clientes de TSM del mismo sistema.

NAS

NAS (Network Attached Storage), es una tecnología de almacenamiento dedicada para compartir información entre servidores o computadoras dentro de una red.

## NDMP

NDMP, o Protocolo de gestión de datos de red (del inglés Network Data Management Protocol), es un protocolo abierto creado por las compañías NetApp y Legato (hoy EMC) que permite realizar copias de seguridad en entornos heterogéneos en los que existen dispositivos de almacenamiento integrados.

## Off-site

Sitio en el cual se puede tener contingencia del sitio principal en caso de pérdida total o parcial de este último.

## Outsourcing

Outsourcing es un término inglés muy utilizado en el idioma español, pero que no forma parte del diccionario de la Real Academia Española (RAE). Su vocablo equivalente es subcontratación, el contrato que una empresa realiza a otra para que realice determinadas tareas que, originalmente, fueron asignadas a la primera.

## RDUMP

Crea un respaldo nivel 0 del sistema de archivos /usr usando el dispositivo remoto /dev/rtape en la máquina pino. El acceso a la cinta remota es controlado por el archivo .rhosts de la máquina remota. Si no se confía en la privacidad de la red puede convenir más implementar un túnel seguro con ssh.

## Respaldo Completo

Un respaldo de información total en un punto en el tiempo.

## Respaldo Incremental

Un respaldo de información solo de aquella que ha cambiado desde el anterior Incremental o Completo.

## RMT

Rmt es un programa usado por los programas de restauración en la manipulación de una unidad de cinta magnética a través de un enlace de comunicación entre procesos. Rmt normalmente se inicia con una rexec o rcmd .

## RoadMap

Un RoadMap (que podría traducirse como hoja de ruta) es una planificación del desarrollo de un software con los objetivos a corto y largo plazo, y posiblemente incluyendo unos plazos aproximados de consecución de cada uno de estos objetivos. Se suele organizar en hitos o "milestones", que son fechas en las que supuestamente estará finalizado un paquete de nuevas funcionalidades.

## RSH

Es un programa de consola para ejecutar comandos en ordenadores remotos.

## SAN

SAN (Storage Área Network- Red de Área de Almacenamiento) es una red concebida para conectar servidores, arrays de discos y equipos de respaldo, está basada en tecnología fibre channel, o lo que es más común actualmente, en iSCSI.

## SAS

(Serial Attached SCSI o SAS). SAS es una tecnología de bus de computadoras diseñada principalmente para transferencia de datos desde o hacia dispositivos de almacenamiento (como discos duros, unidades de CD-ROM, etc.).

## Storage Clouds

Almacenamiento en la nube es un modelo de red de almacenamiento en línea donde los datos son almacenados en los repositorios de almacenamiento virtualizados que son generalmente organizados por terceros.

## TCP Wrappers

TCP Wrapper ("Envoltorio de TCP") es un sistema de red ACL que trabaja en terminales y que se usa para filtrar el acceso de red a servicios de protocolos de Internet que corren en sistemas operativos (tipo UNIX), como Linux o BSD. Permite que las direcciones IP, los nombres de terminales y/o respuestas de consultas ident de las terminales o subredes sean usadas como tokens sobre los cuales filtrar para propósitos de control de acceso.

### Tecnología LTO

(Linear Tape-Open o LTO). Tecnología de almacenamiento de datos en cinta magnética desarrollado como una alternativa abierta a las DLT.

### TI

IT, del inglés Information Technology (Tecnologías de la información). Se refiere en forma generalizada a la tecnología informática.

### VTL

Sistema Mainframe de manejo de espacio en disco a manera de virtualización de tapes para los servidores a los cuales presta servicios. Tape virtual.

### WDSF

Copia de Seguridad de PC/DOS, OS/2, AIX, utilizado como un proceso por parte de IBM.

## BIBLIOGRAFÍA Y REFERENCIAS.

- <http://technet.microsoft.com/es-es/library/ff399114.aspx>.
- <http://forums.zmanda.com/>.
- <http://forums.zmanda.com/forumdisplay.php?f=25>
- <http://www-01.ibm.com/software/tivoli/products/storage-mgr-db/>
- <http://www-01.ibm.com/software/tivoli/products/storage-mgr/platforms.html>
- <http://www-01.ibm.com/software/tivoli/products/storage-mgr/product-features.html>
- <http://blogxdextecnologia.blogspot.com/2011/05/introduccion-dpm-microsoft-system.html>
- <http://www.microsoft.com/en-us/server-cloud/system-center/data-protection-manager.aspx>
- <http://www.microsoft.com/systemcenter/es/es/data-protection-manager.aspx>
- [http://en.wikipedia.org/wiki/System\\_Center\\_Data\\_Protection\\_Manager](http://en.wikipedia.org/wiki/System_Center_Data_Protection_Manager)
- Charlotte Brooks, Peter McFarlane, Norbert Pott, Martin Trcka, Eduardo Tomaz. (2006). IBM Tivoli Storage Manager Implementation Guide
- Charlotte Brooks, Peter McFarlane, Norbert Pott, Martin Trcka, Eduardo Tomaz. (2006). IBM Tivoli Storage Manager Implementation Concepts.
- Lukasz Dobosz. (2002). TSM 5.1 Technical Guide Redbook
- Ryan Femling. (2006). Mastering System Center Data Protection Manager 2007
- Steve Buchanan. (2006). Microsoft Data Protection Manager 2010.
- Jason Buffington. (2006). Data Protection for Virtual Data Centers.

## REFERENCIAS GRÁFICAS.

[WEB1]. Amanda Source Backup

<http://www.zcom.cl/servicios.php?servicio=8>

[WEB2]. Amanda Source Backup

<http://amanda.zmanda.com/>

[WEB3]. Backup Center OB

<http://datacenter.openb.cl/backup.php>

[WEB4]. IBM partnerworld

<http://www-01.ibm.com/software/tivoli/products/storage-mgr/features.html>

[WEB5]. IBM Redbook Web

[http://publib.boulder.ibm.com/tividd/td/ITSML/GC23-4690-02/es\\_ES/HTML/anrlgd52218.htm](http://publib.boulder.ibm.com/tividd/td/ITSML/GC23-4690-02/es_ES/HTML/anrlgd52218.htm)

[WEB6]. Tecnologías Aplicadas

<http://prcerda.blogspot.com/2010/04/system-center-data-protection-manager.html>

[WEB7]. Microsoft Data Protection Manager.

<http://scug.be/mike/tag/dpm-scdpm-backup/>

[WEB8]. Amanda Source Backup

<http://richfrombechtle.wordpress.com/2008/10/07/microsoft-system-center-data-protection-manager-dpm/>

[WEB9]. Visión general sobre la configuración de la rotación de cintas

[http://publib.boulder.ibm.com/tividd/td/TSMCW/GC35-0410-01/es\\_ES/HTML/c1036768.htm](http://publib.boulder.ibm.com/tividd/td/TSMCW/GC35-0410-01/es_ES/HTML/c1036768.htm).

[WEB10]. Zamanda backup to Amazon S3

<http://www.zmanda.com/backup-Amazon-S3.html>

## ANEXOS.

