UNIVERSIDAD NACIONAL DEL SANTA

UNIVERSIDAD NACIONAL DEL SANTA
FACULTAD DE INGENIERÍA
ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

"IMPLEMENTACIÓN DE UN SERVIDOR TIVOLI STORAGE MANAGER PARA MEJORAR EL SALVAGUARDO DE LA INFORMACION EN LA OFICINA REGISTRAL CASMA DE LA ZONA REGISTRAL VII SEDE HUARAZ"

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMÁTICA

TESISTA:

Gerson Julio Torres Espinoza

ASESOR:

Dr. Guillermo Edward Gil Albarrán

NUEVO CHIMBOTE - PERÚ
2015

UNIVERSIDAD NACIONAL DEL SANTA

FACULTAD DE INGENIERIA

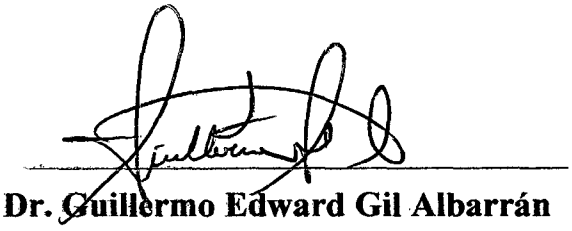
Escuela Académico Profesional de Ingeniería de Sistemas e Informática

TITULO

"IMPLEMENTACIÓN DE UN SERVIDOR TIVOLI STORAGE MANAGER PARA MEJORAR EL SALVAGUARDO DE LA INFORMACION EN LA OFICINA REGISTRAL CASMA DE LA ZONA REGISTRAL VII SEDE HUARAZ"

Tesis para optar el Título de Ingeniero de Sistemas e Informática

REVISADO Y APROBADO POR:



Dr. Guillermo Edward Gil Albarrán

Asesor

NUEVO CHIMBOTE–PERU

2015

UNIVERSIDAD NACIONAL DEL SANTA

FACULTAD DE INGENIERIA

Escuela Académico Profesional de Ingeniería de Sistemas e Informática

TITULO

"IMPLEMENTACIÓN DE UN SERVIDOR TIVOLI STORAGE MANAGER PARA MEJORAR EL SALVAGUARDO DE LA INFORMACION EN LA OFICINA REGISTRAL CASMA DE LA ZONA REGISTRAL VII SEDE HUARAZ"

Tesis para optar el Título de Ingeniero de Sistemas e Informática

REVISADO Y APROBADO POR EL JURADO EVALUADOR:

Dr. Juan Pablo Sánchez Chávez
Presidente

Ing. Carlos Guerra Cordero
Secretario

Dr. Guillermo Gil Albarrán
Miembro

Ing. Luis Ramírez Milla
Accesitario

NUEVO CHIMBOTE –PERU
2015

DEDICATORIA

A Dios que siempre ha estado a mi lado,
a mis amados Padres, por su amor,
comprensión y apoyo constante
para seguir siempre adelante con
el propósito de lograr mi superación
personal y profesional.

A mi hermana, cuñado y sobrinos que son una fuerza
que me insta a seguir superándome.

Gerson Julio Torres Espinoza

AGRADECIMIENTO

Desarrollar esta tesis solo fue posible gracias a la ayuda desinteresada de aquellas personas que laboran en la Oficina Registral Chimbote y Oficina Registral Casma de la Zona Registral VII – Sede Huaraz, quienes se comprometieron a ayudarme; a ellos mi más profundo respeto y agradecimiento sincero.

A mi asesor Dr. Guillermo Gil Albarrán, por sus sugerencias, correcciones y orientaciones importantes para la realización del presente proyecto.

Atentamente;

Gerson Julio Torres Espinoza

INDICE

LISTA DE GRAFICOS

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

El libre mercado y la competencia entre las empresas, hacen que éstas últimas adquieran herramientas y opten por procesos para mejorar o reajustar su calidad de atención y mejora en el servicio. Uno de esos servicios es mantener la seguridad de información, y sobre todo el respaldo constante de los datos importantes que diariamente se generan dentro de la institución.

Es ahí donde se hace, no opcional, sino imperativo, para una institución grande que tiene ámbito nacional, la adquisición de un Servidor que brinde este servicio que permita realizar los respaldos de información de manera periódica y automática, con la finalidad de lograr la seguridad del bien más preciado: la información.

Y dentro de las herramientas para lograr el propósito, Tivoli Storage Manager (TSM), producto de software IBM, nos brinda todas las facilidades y exigencias que las tareas de la Institución requieren, proporcionando un entorno seguro, confiable y restaurable; y luego del estudio, ha sido elegida por SUNARP para ser la herramienta que nos brinde el soporte y la utilidad mencionada antes.

Además se hicieron comparativas con otras herramientas, en las cuales se consideraron características y estándares a cumplir y como resultado de la evaluación se logró demostrar la hipótesis del estudio.

La presente investigación tiene como propósito desarrollar la implementación, partiendo desde la necesidad hasta el funcionamiento del Servidor TSM en la Oficina Registral de Casma que pertenece a la Zona Registral N° VII – Sede Huaraz, con la finalidad de demostrar su utilidad y que, su obtención es vital para el manejo de los procesos internos y para la imagen externa que quiere plasmar en cada uno de los usuarios que se acercan a SUNARP a realizar sus trámites jurídicos.

ABSTRACT

The free market and competition between firms, make the latter choose to acquire tools and processes to improve or adjust the quality of care and service improvement. One such service is to maintain information security, and especially the constant backup of important data that are generated daily within the institution.

Is where is not optional, but mandatory, for a large institution with national scope, the acquisition of a server that provides this service that allows information to perform backups periodically and automatically, in order to achieve security the most valuable asset: information.

And within the tools to achieve the purpose, Tivoli Storage Manager (TSM), IBM software product gives us all the facilities and requirements of the tasks require the institution, providing a safe, reliable and environment restorable; and after the study, it has been chosen by SUNARP to be the tool that gives us the support and the utility mentioned above.

They also made comparisons with other tools, in which features and standards to be met were considered and as a result of the evaluation was conducted to test the hypothesis of the study.

This research aims to develop the implementation, starting from the need to TSM Server performance in the Oficina Registral de Casma that belongs to the Zona Registral N° VII - Sede Huaraz, in order to demonstrate their usefulness and their procurement is vital to the management of internal processes and external image you want to capture in each of the users who come to SUNARP to perform their legal proceedings.

PRESENTACIÓN

Señores miembros del Jurado Evaluador:

En cumplimiento a lo dispuesto en el Reglamento General de Grados y Títulos de la Universidad Nacional del Santa, pongo a vuestra consideración el presente informe de tesis intitulado: "IMPLEMENTACIÓN DE UN SERVIDOR TIVOLI STORAGE MANAGER PARA MEJORAR EL SALVAGUARDO DE LA INFORMACION EN LA OFICINA REGISTRAL CASMA DE LA ZONA REGISTRAL VII SEDE HUARAZ" que es, requisito para optar el Título Profesional de Ingeniero de Sistemas e Informática.

El presente informe de tesis, producto del trabajo de investigación, es gracias al esfuerzo, dedicación y aplicación de los conocimientos logrados a través de mi formación profesional, que refleja el carácter empeñado de capacidad y la iniciativa por la investigación de cada uno de sus egresados inculcados en esta casa superior de estudios.

Por lo expuesto, a ustedes señores miembros del jurado evaluador, teniendo en cuenta las limitaciones propias del presente estudio, se presenta este informe, dejando a vuestro criterio y consideración, su revisión con el deseo de que cumpla con los requisitos mínimos para su correspondiente aprobación.

Atentamente,

Gerson Julio Torres Espinoza

INTRODUCCIÓN

Un mundo globalizado y sobre todo competitivo, hace, que las instituciones u organizaciones implementen procesos y adquieran herramientas para seguir a la par con la era de la tecnología. Una de las tareas de los gerentes es, precisamente, hacer lo necesario para que la institución no caiga en procesos engorrosos o desfasados, previniendo así, el desorden y la no organización de lo más valioso que tiene: La Información.

La utilización de un Servidor para gestionar los cambios en los archivos y hacer copias de respaldo de manera periódica (Versiones y en Tiempo), refleja la preocupación dc la Alta Gerencia de Sunarp, por salvaguardar la información. Teniendo experiencias anteriores, esto es muy relevante, dado que los procesos no están a salvo del error humano, hacer copias de seguridad de los archivos en una herramienta primordial que puede sacarnos del apuro en esos momentos. También el uso del servidor se puede aplicar en el histórico de información para procesos de fiscalización para la toma de decisiones en el ámbito jurídico.

Lo que esta tesis abarca, es la importancia del uso de este tipo de servidores, que, con el paso de los años, las organizaciones del Estado Peruano han adquirido para el beneficio de los servidores públicos y satisfacción de los usuarios.

Este estudio comprende los siguientes capítulos que se describe muy brevemente cada uno de ellos a continuación:

CAPÍTULO I: LA EMPRESA. Este capítulo se hace referencia a la ubicación geográfica de la Oficina Registral de Casma, las generalidades, organigrama, actividad de la empresa, misión y visión.

CAPÍTULO II: PLANTEAMIENTO DEL ESTUDIO. En este capítulo plantea la realidad problemática, se formula el problema, la justificación y la importancia de la investigación, hipótesis y objetivos

CAPÍTULO III: MARCO TEÓRICO Y CONCEPTUAL. Este capítulo presenta las teorías y los conceptos relacionados con el tema de investigación que sustentan las variables de estudio.

CAPÍTULO IV: METODOLOGIA DE DESARROLLO DE LA IMPLEMENTACION. Este capítulo aborda los requisitos mínimos para la implementación del servidor en estudio y aborda el trabajo realizado en las configuraciones previas a la puesta en funcionamiento del servidor Tivoli Storage Manager, además de brindar al detalle de la herramienta utilizada, los códigos en el lenguaje respectivo, las configuraciones a utilizar (Diario, Semanal y Mensual).

CAPÍTULO V: MATERIALES Y METODOS. Este capítulo hace referencia a herramientas utilizadas en el recojo y análisis de la información, así como las técnicas utilizadas.

CAPÍTULO VI: RESULTADOS Y DISCUSIÓN. Se presentan la validez del proyecto y el impacto positivo que tiene en las organizaciones del Estado.

CAPÍTULO VII: CONCLUSIONES Y RECOMENDACIONES. En este capítulo se presentan las conclusiones y recomendaciones del trabajo de investigación.

DATOS GENERALES DEL ESTUDIO

1.1. TITULO DEL PROYECTO

"IMPLEMENTACIÓN DE UN SERVIDOR TIVOLI STORAGE MANAGER PARA MEJORAR EL SALVAGUARDO DE LA INFORMACION EN LA OFICINA REGISTRAL CASMA DE LA ZONA REGISTRAL VII SEDE HUARAZ"

1.2. TESISTA

- Bach. GERSON JULIO TORRES ESPINOZA

1.3. ASESOR

- Dr. Guillermo Gil Albarrán

1.4. TIPO DE INVESTIGACIÓN

1.4.1. Según su Naturaleza

Explicativa, porque, dada la experiencia en otras oficinas registrales (Oficina Registral de Chimbote), se pudo identificar las bases, los requerimientos iniciales en cuanto a la implementación del servidor así lo requiere, así como los beneficios que esto atrae, sus principales características, y sobre todo, la seguridad que solo el hecho de la implementación, afirma que SUNARP apunta hacia la utilización de la más alta tecnología en cuanto a salvaguardo de la información se requiere, lo que permitió, evaluar y medir de manera independiente sus propiedades más importantes, con el propósito de implementar el servidor como una solución práctica lo que al final indujeron a la prueba de hipótesis como causa directa de la implementación del TSM en la oficina Registral de Casma.

1.4.2. Según su fin o propósito

Aplicada, porque dará una solución práctica, a la problemática planteada, sobre la Implementación del Servidor TSM, la aplicación de los conceptos de configuración, las políticas y normas de seguridad que se implementaran en la Oficina Registral de Casma, a fin de complementar el uso de la herramienta, y así generar la eficiencia y eficacia en los diversos procesos registrales cumpliendo así los objetivos planteados en este estudio.

1.5. MÉTODO DE INVESTIGACIÓN

Inductivo – Deductivo, porque luego de definir la realidad problemática y, por ser también este estudio, una investigación aplicada, se planteó la hipótesis que permitiera hacer pruebas a los indicadores o características de la variable dependiente para percibir u observar si las consecuencias de la hipótesis son viables o verificados con los resultados de la Implementación del Servidor TSM que permita dar una solución práctica, la cual es la administración responsable de la información, para cumplir el objetivo más grande que tiene la institución: Seguridad Jurídica para el usuario, variable tácita involucrada en el presente estudio.

1.6. DELIMITACIÓN DEL ESTUDIO

El estudio está orientado al desarrollo de la implementación de un Servidor Storage Manager para salvaguardar la información de cualquier institución estatal o privada, delimitando en este caso a la Superintendencia Nacional de los Registros Públicos, Oficina Registral de Casma.

CAPITULO I

LA INSTITUCIÓN

1.1 DESCRIPCION

La Superintendencia Nacional de los Registros Públicos SUNARP, es un Organismo Técnico Especializado, adscrito al Sector Justicia y Derechos Humanos, y ente rector del Sistema Nacional de los Registros Públicos, con Personería Jurídica de Derecho Público, con patrimonio propio y autonomía funcional, jurídico- registral, técnica, económica, financiera y administrativa.

1.1.1 Organización Institucional

La SUNARP, tiene por misión otorgar seguridad jurídica al ciudadano a través del registro y publicidad de derechos y titularidades, brindando servicios eficientes, transparentes y oportunos.

Asimismo, tiene por objeto dictar las políticas y normas técnico – administrativas de los Registros Públicos, estando encargada de planificar, organizar, normar, dirigir, coordinar y supervisar la inscripción y publicidad de los actos y contratos en los Registros Públicos que integran el Sistema Nacional de los Registros Públicos.

Para el cumplimiento de sus funciones a nivel nacional, cuenta con Órganos Desconcentrados - Zonas Registrales, aprobado con el Reglamento de Organizaciones y Funciones (ROF)de la Superintendencia Nacional de los Registros Públicos, mediante el Decreto Supremo N" 012-2013-JUS.

1.1.2 Estructura Orgánica.

La Estructura Orgánica de la SUNARP está definida por el ROF aprobado con el Decreto Supremo N" 012-2013-JUS, del 14 octubre 2013.

Gráfico N° 01 Organigrama – Sunarp

Fuente: Pagina Institucional

1.1.3 Cobertura Nacional

Cobertura Nacional.- La SUNARP cuenta a nivel nacional con 90 Oficinas Receptoras, 64 Oficinas Registrales y entre ellas se encuentran las Sedes Zonales con presencia en las principales ciudades, ver gráfico N° 02.

Las Oficinas Receptoras que se ubican a nivel de las Provincias, tienen el objetivo de cumplir los lineamientos estratégicos de la política de gobierno de inclusión social que ayudará a mejorar la situación económica y social en el marco de la reducción de la pobreza y pobreza extrema. El objetivo de los servicios registrales

es crear condiciones básicas para el desarrollo con igualdad de oportunidades para los más pobres, que viven en distritos urbanos y rurales de difícil acceso. En este sentido, la SUNARP cumple la política de inclusión social con presencia a nivel nacional, asumiendo la obligación de efectuar su aporte para el desarrollo de un Perú inclusivo en el ámbito de la seguridad jurídica de las inversiones, así como del registro de la propiedad.

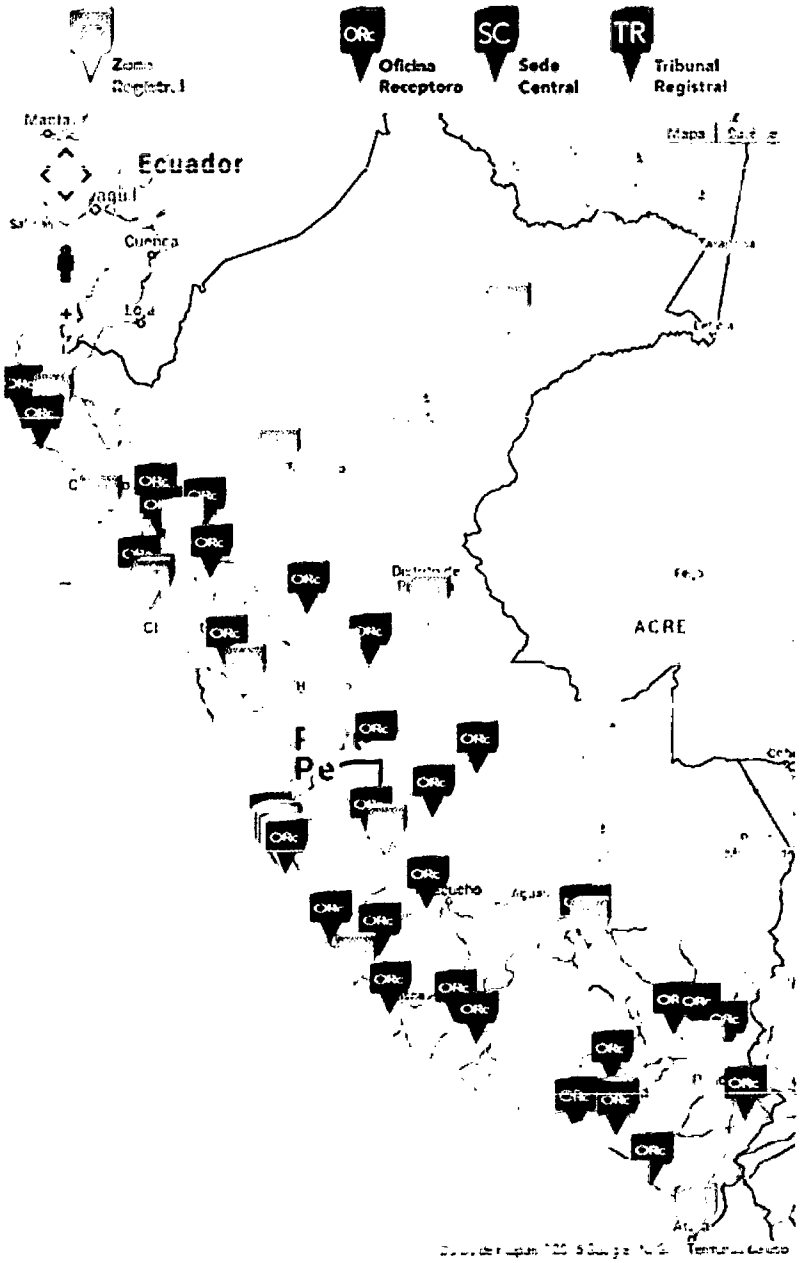


Gráfico N° 02 Oficinas Registrales y Oficinas Receptoras a Nivel Nacional

Fuente: Pagina Institucional

1.1.4 Registros que conforman el Sistema

El artículo 2° de la ley 26366, señala los Registros que conforman dicho sistema son:

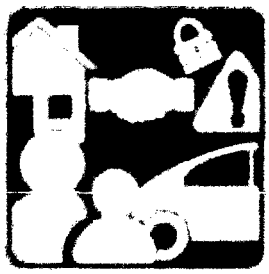
- Registro de Personas Naturales, que unifica los siguientes registros: el Registro de Mandatos y Poderes, el Registro de Testamentos, el Registro de Sucesión Intestada, el Registro Personal y Registro de Comerciantes
- Registro de Personas Jurídicas, que unifica los siguientes registros: el Registro de Personas Jurídicas, el Registro Mercantil, el Registro de Sociedades Mineras, el Registro de Sociedades de Registro Público de Hidrocarburos, el Registro de Sociedades Pesqueras, el Registro de Sociedades Mercantiles, el Registro de Personas Jurídicas creadas por Ley y el Registro de Empresas Individuales de Responsabilidad Limitada
- Registro de Propiedad Inmueble, que unifica los siguientes registros: el Registro de Predios, el Registro de Buques, el Registro Embarcaciones Pesqueras, el Registro de Aeronaves, el Registro de Naves, el Registro de Derechos Mineros y el Registro de Concesiones para la explotación de los Servicios Públicos.
- El Registro de Bienes Muebles, que unifica los siguientes registros : el Registro de Bienes Muebles, el Registro de Propiedad Vehicular, el Registro Fiscal de Ventas a Plazos, el Registro de Prenda Industrial, el Registro de Prenda Agrícola, el Registro de Prenda Minera, el Registro de Prenda Minera, el Registro de Prenda Vehicular y de Prenda Global y Flotante.

Asimismo por normas especiales se han creado los siguientes Registros: Registro Público de Gestión de Intereses(a cargo del Registro de Personas Naturales), Registro de Rondas Campesinas (a cargo del Registro de Personas Jurídicas).

1.2 BASE LEGAL

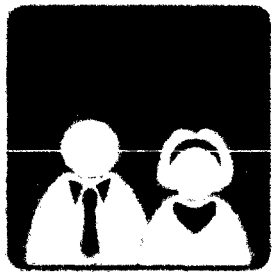
Mediante Ley26366, se crea el Sistema de Nacional de Registros Públicos, y la Superintendencia Nacional de Registros Públicos - SUNARP, y por Resolución Suprema N° 135-2002-JUS, se aprueba el Estatuto de la SUNARP.

1.3 DIRECCIONAMIENTO ESTRATEGICO



1.3.1 Misión de la Institución

Otorgar seguridad jurídica al ciudadano a través del registro y publicidad de derechos y titularidades en forma eficiente y transparente



1.3.2 Visión de la Institución

Ser una institución referente a nivel internacional, altamente tecnificada, proactiva confiable y con presencia efectiva en todo el territorio nacional. Brindando servicios registrales de calidad a satisfacción del ciudadano.

1.3.3 Valores

- **Respeto.-** Actuar respetando las normas, los principios y las opiniones o iniciativas, tanto internas como externas, en un proceso de toma de decisiones justo, objetivo, ponderado y socialmente responsable.
- **Compromiso.-** Disposición a brindar nuestro mayor esfuerzo y compromiso al logro de los objetivos y metas en la oportunidad requerida y al menor costo para la Institución y la sociedad en su conjunto.
- **Solidaridad.-** Implica actuar con fidelidad, rectitud y probidad, regidos por la cooperación para lograr los objetivos propuestos.
- **Responsabilidad.-** Se trata de uno de los valores humanos más importantes, el que nace a partir de la capacidad humana para poder optar entre diferentes opciones y actuar, haciendo uso de la libre voluntad, de la cual resulta la necesidad que asumir todas aquellas consecuencias que de estos actos se deriven.
- **Disciplina en el trabajo.-** La disciplina en el trabajo tiene una importancia muy grande en la producción puesto que garantiza que éste

1.4 OBJETIVOS ESTRATEGICOS

1.4.1 Objetivo General

Brindar a la ciudadanía la Seguridad Jurídica a través de la Inscripción y Publicidad Registral, de manera eficiente, oportuna y con calidad en la prestación.

1.4.2 Objetivos Específicos

- Fortalecer, innovar y descentralizar la prestación de los servicios registrales de inscripción y publicidad.
- Disponer de herramientas tecnológicas innovadoras y procesos articulados para desarrollar eficientemente los servicios registrales.
- Posicionar la imagen de la institución en la función de su competencia con inclusión social para el desarrollo socio económico del país.
- Fortalecer las competencias, habilidades y actitudes del personal para mejorar la calidad en la prestación de los servicios y lograr una Entidad eficacia, eficiencia y efectiva.
- Garantizar la auto sostenibilidad financiera de la institución.

1.5 LOGO INSTITUCIONAL

Grafico N° 03: Logo Institucional de Sunarp
Fuente: Página Oficial Sunarp

CAPÍTULO II

PLANTEAMIENTO DEL ESTUDIO

2.1 PROBLEMA

2.1.1. REALIDAD PROBLEMÁTICA

La Oficina Registral de Casma que pertenece a la Zona Registral N° VII – Sede Huaraz, tiene como necesidad la acción de generar diaria, semanal y mensualmente respaldos de sus servidores presentes en el Centro de Datos, con respecto a base de datos y servidores de archivos, y 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 ha 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 cuentas 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.
- Perdida 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 institución.

2.1.2. ANALISIS DEL PROBLEMA

En consideración al diagnóstico a la problemática, incidiendo particularmente en la carencia de un Servidor que permita el salvaguardo de la información, debemos analizar cada una de las problemáticas identificadas, para profundizar a mayor detalle este problema y dar posibles soluciones en su implementación:

- *La Sunarp, en busca de la calidad de la protección de la información está* en plena aplicación de los estándares para la certificación de las normas de calidad ISO 9001, para así crecer y tener una mayor participación en el mercado peruano, acercándonos al ciudadano y brindándole una atención oportuna; se debe tener conciencia de cuan valiosa es la necesidad de consolidarse en la actual coyuntura de nuestra economía y tener en cuenta que es importantísimo.

  En esta actividad confluyen las responsabilidades de la Unidad Registral así como de la Unidad de Tecnologías de la Información, dado que en conjunto deben crear el esquema óptimo para proponer un rol de responsabilidades y crear las tareas que deben dar la solución a fin de proteger el recurso más valioso de la institución.

- La Sunarp (Oficina Registral de Casma) aún no tiene claro que un enfoque basado en la prevención en lo que concierne a la protección de los datos, y como esta herramienta puede ser un hito en el referente del marco de competitividad y así crear valor añadido por el bien de la institución.

  Asimismo implementar una bitácora de sucesos que servirá en un corto o largo plazo al análisis de los problemas que pueden surgir al momento de administrar la información.

- En la institución se está implementando politicas para gestionar la protección de la información que atienda a una mayor posibilidad de generación de reportes, backups, y archivos que sean el sostén de confiabilidad. Esto conllevaría a la correcta administración y sobre todo generaría rentabilidad.

  La SUNARP que trabaja con plazos en todos sus procesos registrales, tendrá que volcar estos paradigmas hacia la administración de la información a fin de poder poner las bases de una correcta manera de

enfocar las tareas de gestión. Tanto la Unidad Registral y la Unidad de las Tecnologías de la Información acentúan los plazos correspondientes.

- Actualmente la empresa no cuenta con la herramienta planteada (versiones anteriores) lo cual significa la carencia de estrategias para la administración y el desarrollo de la correcta gestión de la información. Por lo que es prioridad implementar esta solución a fin de marcar el *comienzo de la administración moderna de los procesos de gestión de la* información.

  Enmarcado en plena implementación del SGSI (Sistema de Gestión de la Seguridad la Información ISO 27001), la SUNARP está implementando esta herramienta de Backups de archivos en todas sus Zonas Registrales, para estandarizar la administración de la información. La Unidad de Tecnologías de la Información, lleva de la mano a la SUNARP, a la implementación progresiva de este estándar, en todos sus procesos, y claro está, la solución propuesta está dentro del marco de desarrollo del SGSI.

- Si bien la seguridad de la información, ha tenido un papel preponderante en el desarrollo de nuestra institución, esta también se ha visto mellada por falta de seguridad física (interna y externa) que la Unidad Registral ha planteado en brindar las pautas legales a fin de solucionar este problema y la Unidad de Tecnologías de la Información brindara las herramientas tecnologías (planteara) fin de consolidar una seguridad en todos los ámbitos.

Con el propósito de dar solución alternativa a estos problemas, es que la Superintendencia Nacional de los Registros Públicos implementará el Servidor Tivoli Storage Manager en la Oficina Casma perteneciente a la Zona Registral VII – Sede Huaraz para el salvaguardo de la Información.

2.2 ANTECEDENTES DEL PROBLEMA DE ESTUDIO

Introducción.

La implementación de un servidor Tivoli Storage Manager, se puede considerar en un estado inicial de implantarse en la Sunarp, donde aún se están estableciendo claramente las características necesarias para realizar con éxito todo lo que conlleva su utilización. Sin embargo, por experiencia, se conoce que un gran número de empresas nacionales e internacionales han implementado esta herramienta y es en esa experiencia en la cual la SUNARP puede sostenerse.

Empresas buscan mayor respaldo a sus bases de datos [URL 01]

Muchas empresas en la actualidad comienzan a interesarse y adquirir mayores conocimientos acerca del cuidado de sus bases de datos, así como de sus sistemas de recuperación y soluciones a los problemas cotidianos. Se está viviendo una era en donde la información va creciendo, por lo tanto, la capacidad de los datos se hace infinita.

Softline International del Perú, empresa transnacional de TI, líder reconocido en el aprovisionamiento de licencias de software y prestación de servicios relacionados con TI, realizó un desayuno tecnológico con clientes, en el cual se expusieron la mejores prácticas de respaldo de contenido de bases de datos, para que las empresas aseguren la continuidad del negocio y reduzcan los riesgos asociados a la pérdida de datos.

Junto con IBM y su herramienta Tivoli Storage Manager, Softline Perú continúa trabajando en repartir a sus clientes el conocimiento de las soluciones y productos específicos que cuentan con la experiencia necesaria para las distintas fases que pueden surgir en el negocio. En la cita, Francisco Robledo, gerente de cuentas corporativas de Softline Perú y expositor del encuentro, comentó que es vital que las empresas desarrollen un adecuado plan de recuperación de su información relevante ante cualquier contingencia (independientemente del tamaño y sector del giro del negocio de la empresa).

"Se tiene un estimado de que el 92% de las PyMEs sigue usando el backup y la recuperación tradicional y sólo una de cada cinco nombra la protección de datos como una de sus principales prioridades en los planes de gastos de Tecnología de la Información (TI), esta es una realidad preocupante en cuanto a la seguridad e integridad de la data, ya que puede romper la continuidad efectiva del negocio. En cuanto a las grandes empresas, aún existe desconocimiento a las tareas comunes y pérdidas de datos al no saber cómo

controlar el crecimiento de la información", finalizó Robledo. "Aún no existe una seguridad, ni pautas a seguir para poder concentrar nuestros esfuerzos en la información o datos de la empresa, se debe asegurar una protección de datos automatizada y centralizada, con un software escalable y flexible", continuó el especialista.

Según el gerente, el crecimiento de los datos es inevitable, por lo que habría que crear y adoptar mecanismo para cuidar las áreas de trabajo que nos mantenga alertas a los desafíos en TI. Es decir, la gestión de recuperación, de políticas de seguridad y administración nos va a llevar a reducir costos en el almacenamiento de datos y simplificar nuestras tareas de administración y gestión de seguridad de la información.

2.2.1 En donde estamos a nivel Nacional e Internacional sobre el Tema

A nivel nacional e internacional el salvaguardo de la información está tomando cada vez mayor relevancia en la administración responsable de la misma en las empresas, por lo que podríamos asegurar que se han generado diversos trabajos, artículos y proyectos sobre esta Implementación. A continuación se presentan las aportaciones que en mayor medida guardan relación con esta investigación:

Max Alonso Huamán (2009) Titulo: "Fundamentos de Sistemas de Respaldo de Información"

Esta investigación presenta "los conceptos básicos a tener en cuenta al momento de respaldar nuestra información. Se hace énfasis en IBM Tivoli Storage Manager como una herramienta que ayuda a tener soluciones robustas en Sistemas de Respaldo de Información. Y como resultado del modelo teórico se podrían determinar las fortalezas y debilidades que posee esta herramienta para poder insertarse en una organización capaz de invertir en este tipo de seguridad informática.

López López, Isvel (2010) "Implementación de una solución de respaldos de información en la empresa Uniplex Systems en Quito"

Este proyecto abarca la total implementación de una solución de respaldos de información digital para la empresa UNIPLEX Systems, con el objetivo de resolver problemas como la disponibilidad de aplicaciones críticas como lo es el correo electrónico y otras, dicha implementación hace uso de las mejores prácticas ITIL v3 acerca del almacenamiento, como recomendaciones y no como creación de un nuevo servicio. La solución debe garantizar que la información se mantenga de manera segura, confiable y disponible frente a cualquier amenaza

que se presente, para esto se utilizó el software Tivoli Storage Manager (TSM) de IBM ya que es una herramienta empresarial que está disponible para UNIPLEX Systems sin costo alguno por ser partner de IBM. Se realizó la toma de requerimientos en base al estándar 'Software Requirements Specifications (SRS)' de la IEEE. Para cumplir a cabalidad con los mismos, se efectuó un análisis de la información y se creó un SLA para ofrecer niveles de servicios en base a tiempos de respaldos y tiempos de recuperación total en caso de un desastre.

Xavier Mauricio Rea Peñafiel (2012) "Implementación de una de las Herramientas de Salvaguardo de Información para Sinergy Team Cia. Ltda."

Este investigador, ha estudiado las propuestas para uso como herramienta de Salvaguardo de Información para esta empresa. La propuesta teórica que es introducida en esta investigación se realizó en base 3 Gestores de Backups de Información, tales como son Amanda y TSM.

2.3 FORMULACIÓN DEL PROBLEMA

"De qué manera la implementación de un Servidor Tivoli Storage Manager mejorará el salvaguardo de la Información en la Oficina Registral Casma de la Zona Registral VII Sede Huaraz"

2.4 JUSTIFICACIÓN DE LA INVESTIGACIÓN

Esta investigación se justifica en sus siguientes aspectos:

2.4.1 JUSTIFICACIÓN SOCIAL

El siguiente proyecto tiene una justificación social, pues, la solución definitiva definirá normas y estándares en los que el personal a cargo se verá involucrado y la propuesta definirá un conjunto de reglas que involucren a las personas usuarios internos y externos, y al crecimiento profesional – Oficina Registral de Casma, las mismas que se traducirán en beneficios sociales incluso en sus familias pues se busca generar sinergia.

2.4.2 JUSTIFICACIÓN OPERATIVA

El proyecto se justifica **operativamente,** dado que los involucrados en el estudio conociendo y aplicando un conjunto de reglas sobre el crecimiento, proceso y desarrollo de la utilización del Servidor Tivoli Storage Manager, tendrán un mejor desempeño, es decir, de calidad y mayor facilidad para realizar las actividades operativas con eficiencia y eficacia, ya que tendrán mejor y mayor acceso al uso planificado de los diferentes recursos que esta herramienta nos brinda en el nivel que les corresponde desempeñar su función.

2.4.3 JUSTIFICACIÓN ECONÓMICA

El proyecto tiene una justificación **Económica,** pues desarrollaremos una implementación lograr consolidarnos en el mercado y hacer que se logre una mayor demanda para lograr mayores ingresos y por ende sea una institución más rentable.

2.5 IMPORTANCIA DE LA INVESTIGACIÓN

Porque el valor de las empresas en la actualidad es la información, se debe contar con diferentes medidas de seguridad de respaldos; diseñadas según la necesidad de nuestra institución:

Las copias de seguridad son una parte muy importante en el funcionamiento de la Superintendencia Nacional de los Registros Públicos, debido a que la pérdida de información o datos críticos podría ser perjudicial e interrumpir en el funcionamiento de la institución.

Llevando acabo ciertas medidas de seguridad ante la pérdida de información, es posible restaurar los datos con copias efectuadas del día anterior, perdiendo como máximo un día de trabajo. Si se eliminó uno o varios archivos en días anteriores, tenemos la opción de recuperar estos, con la copia semanal o mensual realizada según nuestra política de seguridad.

2.6 HIPOTESIS

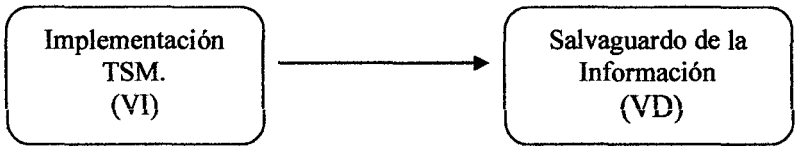
"La Implementación de un Servidor Tivoli Storage Manager mejora el salvaguardo de la información en la Oficina Registral Casma de la Zona Registral VII Sede Huaraz"

VARIABLE INDEPENDIENTE (VI)

La Implementación de un Servidor Tivoli Storage Manager (TSM)

VARIABLE DEPENDIENTE (VD)

El Salvaguardo de la Información



2.6.1 Operacionalización de Variables

Variable	Definición Conceptual	Dimensiones	Indicadores	Medicion
Implementación de un Servidor Tivoli Storage Manager	*Es la instalación de una aplicación informática, realización o la ejecución de un plan, idea, modelo científico, diseño, especificación, estándar, algoritmo o política.*	* Uso de Herramienta.	Confianza.	* Test Internos
			Fácil Uso	
		* Robustez de Implementación	Backups	* Reportes de Servidor
			Restore	
Salvaguardo de la información	*Buena Práctica de consignar la información que es de gran valor y relevante para la institución y tenerlo a salvo (medios internos o extraíbles)*	* Evaluación de la funcionalidad de la solucion	Costos	* Test Externos
			Limitaciones	
			Indispensabilidad	

Tabla N°1 Operacionalización de Variables

2.7 OBJETIVOS

2.7.1 Objetivo General

Implementar un Servidor Tivoli Storage Manager para mejorar el salvaguardo la Información en la Oficina Registral Casma de la Zona Registral VII Sede Huaraz

2.7.2 Objetivos Específicos

- Crear calendarios diarios, semanales y mensuales 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.
- Administrar la herramienta haciendo que sea accesible desde la red interna a través de un acceso web y si lo solicita la Institución 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 crear sinergia.
- Generar material de entrenamiento para que sea objeto de estudio y práctica dentro de la Oficina Registral de Casma.

CAPÍTULO III
MARCO TEÓRICO Y CONCEPTUAL

3.1 SISTEMAS DE RESPALDO DE INFORMACIÓN.

No es ninguna novedad el valor que tiene la información y los datos para nuestros negocios . Los que resulta increíble de esto es la falta de precauciones que solemos tener al confiar al núcleo de nuestros negocios al sistema de almacenamiento de lo que en la mayoría de los casos resulta ser una computadora pobremente armada tanto del punto de vista de hardware como de software.

Si el monitor, la memoria e incluso la CPU de nuestro computador dejan de funcionar, simplemente lo reemplazamos, y no hay mayores dificultades. Pero si falla el disco duro, el daño puede ser irreversible, puede significar la pérdida total de nuestra información. Es principalmente por esta razón, por la que debemos respaldar la información importante. Imaginémonos ahora lo que pasaría si esto le sucediera a una empresa, las pérdidas económicas podría ser cuantiosas. Los negocios de todos los tipos y tamaños confían en la información computarizada para facilitar su operación. La pérdida de información provoca un daño de fondo:

- Pérdida de oportunidades de negocio
- Clientes decepcionados
- Reputación perdida
- Etc.

La tecnología no está exenta de fallas o errores, y los respaldos de información son utilizados como un plan de contingencia en caso de que una falla o error se presente.

Asimismo, hay empresas, que por la naturaleza del sector en el que operan (por ejemplo Banca) no pueden permitirse la más mínima interrupción informática.

Las interrupciones se presentan de formas muy variadas: virus informáticos, fallos de electricidad, errores de hardware y software, caídas de red, hackers, errores humanos, incendios, inundaciones, etc. Y aunque no se pueda prevenir cada una de estas interrupciones, la empresa sí puede prepararse para evitar las consecuencias que éstas puedan tener sobre su negocio. Del tiempo que tarde en reaccionar una empresa dependerá la gravedad de sus consecuencias.

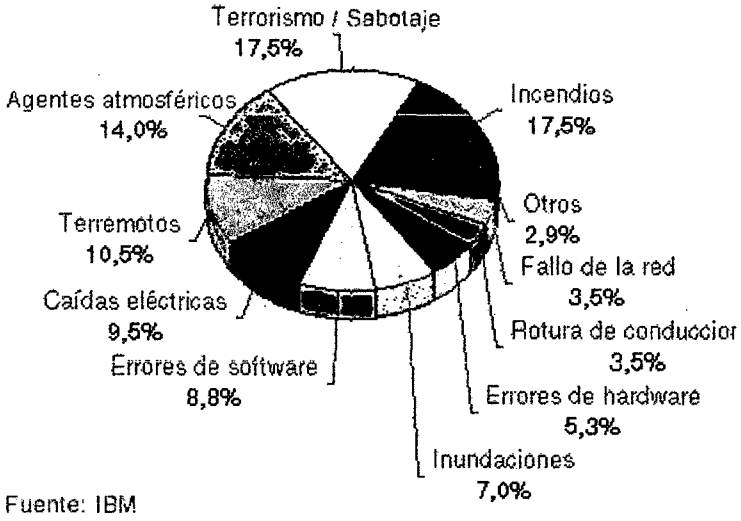


Grafico N° 04 Riesgo a los cuales se encuentran inmersos los Sistemas de Información

Además, podríamos recordar una de las leyes de mayor validez en la informática, la "Ley de Murphy":

- Si un archivo puede borrarse, se borrará.
- Si dos archivos pueden borrarse, se borrará el más importante.
- Si tenemos una copia de seguridad, no estará lo suficientemente actualizada.

La única solución es tener copias de seguridad, actualizarlas con frecuencia y esperar que no deban usarse.

Respaldar la información significa copiar el contenido lógico de nuestro sistema informático a un medio que cumpla con una serie de exigencias:

- Ser confiable: Minimizar las probabilidades de error. Muchos medios magnéticos como las cintas de respaldo, los disquetes, o discos duros tienen probabilidades de error o son particularmente sensibles a campos magnéticos, elementos todos que atentan contra la información que hemos respaldado allí. Otras veces la falta de confiabilidad se genera al rehusar los medios magnéticos. Las cintas en particular tienen una vida útil concreta. Es común que se subestime este factor y se reutilicen más allá de su vida útil, con resultados nefastos, particularmente porque vamos a descubrir su falta de confiabilidad en el peor momento: cuando necesitamos RECUPERAR la información.
- Estar fuera de línea, en un lugar seguro: Tan pronto se realiza el respaldo de información, el soporte que almacena este respaldo debe ser desconectado de la computadora y almacenado en un lugar seguro tanto desde el punto de

vista de sus requerimientos técnicos como humedad, temperatura, campos magnéticos, como de su seguridad física y lógica. No es de gran utilidad respaldar la información y dejar el respaldo conectado a la computadora donde potencialmente puede haber un ataque de cualquier índole que lo afecte.

- La forma de recuperación sea rápida y eficiente: Es necesario probar la confiabilidad del sistema de respaldo no sólo para respaldar sino que también para recuperar. Hay sistemas de respaldo que aparentemente no tienen ninguna falla al generar el respaldo de la información pero que fallan completamente al recuperar estos datos al sistema informático. Esto depende de la efectividad y calidad del sistema que realiza el respaldo y la recuperación.

Esto nos lleva a que un sistema de respaldo y recuperación de información tiene que ser probado y eficiente.

Seguridad física y lógica:

Puede llegar a ser necesario eliminar los medios de entrada/salida innecesarios en algunos sistemas informáticos, tales como disqueteras y cdroms para evitar posible infecciones con virus traídos desde el exterior de la empresa por el personal, o la extracción de información de la empresa.

Las copias de seguridad son uno de los elementos más importantes y que requieren mayor atención a la hora de definir las medidas de seguridad del sistema de información, la misión de las mismas es la recuperación de los ficheros al estado inmediatamente anterior al momento de realización de la copia.

La realización de las copias de seguridad se basará en un análisis previo del sistema de información, en el que se definirán las medidas técnicas que puedan condicionar la realización de las copias de seguridad, entre los que se encuentran:

Volumen de información a copiar

Condicionará las decisiones que se tomen sobre la política de copias de seguridad, en una primera consideración está compuesto por el conjunto de datos que deben estar incluidos en la copia de seguridad, sin embargo, se pueden adoptar diferentes estrategias respecto a la forma de la copia, que condicionan el volumen de información a copiar, para ello la copia puede ser:

Copiar sólo los datos, poco recomendable, ya que en caso de incidencia, será preciso recuperar el entorno que proporcionan los programas para acceder a los mismos, influye negativamente en el plazo de recuperación del sistema.

Copia completa, recomendable, si el soporte, tiempo de copia y frecuencia lo permiten, incluye una copia de datos y programas, restaurando el sistema al momento anterior a la copia.

Copia incremental, solamente se almacenan las modificaciones realizadas desde la última copia de seguridad, con lo que es necesario mantener la copia original sobre la que restaurar el resto de copias. Utilizan un mínimo espacio de almacenamiento y minimizan el tipo de desarrollo, a costa de una recuperación más complicada.

Copia diferencial, como la incremental, pero en vez de solamente modificaciones, se almacenan los ficheros completos que han sido modificados. También necesita la copia original.

Tiempo disponible para efectuar la copia

El tiempo disponible para efectuar la copia de seguridad es importante, ya que el soporte utilizado, unidad de grabación y volumen de datos a almacenar, puede hacer que el proceso de grabación de los datos dure horas, y teniendo en cuenta que mientras se efectúa el proceso es conveniente no realizar accesos o modificaciones sobre los datos objeto de la copia, este proceso ha de planificarse para que suponga un contratiempo en el funcionamiento habitual del sistema de información.

Soporte utilizado

Es la primera decisión a tomar cuando se planea una estrategia de copia de seguridad, sin embargo esta decisión estará condicionada por un conjunto de variables, tales como la frecuencia de realización, el volumen de datos a copiar, la disponibilidad de la copia, el tiempo de recuperación del sistema, etc.

Entre los soportes más habituales, podemos destacar las cintas magnéticas, discos compactos (como las unidades de Iomega Zip y Jazz), grabadoras de CD-ROM o cualquier dispositivo capaz de almacenar los datos que se pretenden salvaguardar.

La estimación del coste de un soporte de almacenamiento para las copias de seguridad no se basa simplemente en el precio de las unidades de cinta o de disco, el coste de la unidad de grabación es también muy importante, ya que puede establecer importantes diferencias en la inversión inicial.

La unidad será fija o extraíble, es otra decisión importante, ya que la copia de seguridad se puede realizar sobre otro disco duro del sistema de información, o bien, mediante los elementos descritos anteriormente.

Una vez definidas las medidas de índole técnica, quedan por definir las medidas organizativas, ya que de nada sirve el mejor soporte si las copias no se realizan de acuerdo a un plan de copias de seguridad.

La política de copias de seguridad debe garantizar la reconstrucción de los ficheros en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Frecuencia de realización de copias de seguridad

La realización de copias de seguridad ha de realizarse diariamente, éste es el principio que debe regir la planificación de las copias, sin embargo, existen condicionantes, tales como la frecuencia de actualización de los datos, el volumen de datos modificados, etc. que pueden hacer que las copias se realicen cada más tiempo.

Planificación de la copia

Las copias de seguridad se pueden realizar en diferentes momentos día, incluso en diferentes días, pero siempre se han de realizar de acuerdo a un criterio, y este nunca puede ser "cuando el responsable lo recuerda", si es posible, la copia se debe realizar de forma automática por un programa de copia, y según la configuración de éste, se podrá realizar un día concreto, diariamente, semanalmente, mensualmente, a una hora concreta, cuando el sistema esté inactivo, ..., etc, todos estos y muchos más parámetros pueden estar presentes en los programas que realizan las copias de seguridad y deben permitirnos la realización únicamente de las tareas de supervisión.

Mecanismos de comprobación

Se deben definir mecanismos de comprobación de las copias de seguridad, aunque los propios programas que las efectúan suelen disponer de ellos para verificar el estado de la copia, es conveniente planificar dentro de las tareas de seguridad la restauración de una parte de la copia o de la copia completa periódicamente, como mecanismo de prueba y garantía.

Responsable del proceso

La mejor forma de controlar los procesos que se desarrollan en el sistema de información, aunque estos estén desarrollados en una parte importante por el propio sistema, es que exista un responsable de la supervisión de que " lo seguro es seguro", para ello se debe designar a una persona que incluya entre

sus funciones la supervisión del proceso de copias de seguridad, el almacenamiento de los soportes empleados en un lugar designado a tal fin e incluso de la verificación de que las copias se han realizado correctamente.

Por último, se debe considerar en la realización de las copias de seguridad, el uso de diferentes soportes para almacenar los datos, entre las diferentes posibilidades que se presentan en función del número de soportes empleados, se puede considerar la siguiente:

Un posible esquema de copia de seguridad sería realizar una copia de seguridad completa cada mes y se guarda la cinta durante un año (preferentemente en algún sitio seguro ajeno a la empresa), una copia de seguridad completa semanalmente que se guarda durante un mes y copias de seguridad diarias, que se guardan durante una semana y que pueden ser completas, incrementales o diferenciales. Con este sistema se pueden utilizar 7 soportes que garantizan un alto nivel de seguridad en cuanto a recuperaciones de datos.

También se recomienda guardar las copias de seguridad en un lugar alejado, como, por ejemplo, una caja de seguridad o cualquier otro sitio asegurado contra incendios, para que, en caso de que se produzca algún desastre como un incendio, los datos se encuentren protegidos.

Medidas de Seguridad

Respecto a las copias de seguridad, se deben tener en cuenta los siguientes puntos:

Deberá existir un usuario del sistema, entre cuyas funciones esté la de verificar la correcta aplicación de los procedimientos de realización de las copias de respaldo y recuperación de los datos.

Los procedimientos establecidos para la realización de las copias de seguridad deberán garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Deberán realizarse copias de respaldo al menos semanalmente, salvo que en dicho periodo no se hubiera producido ninguna actualización de los datos.

3.2 SERVIDOR.

Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia. Los servidores se pueden ejecutar en cualquier tipo de computadora, incluso en computadoras dedicadas a las cuales se les conoce individualmente como "el servidor". En la mayoría de los casos una misma computadora puede proveer múltiples servicios y tener varios servidores en funcionamiento. La ventaja de montar un servidor en computadoras dedicadas es la seguridad. Por esta razón la mayoría de los servidores son procesos diseñados de forma que puedan funcionar en computadoras de propósito específico.

Los servidores operan a través de una arquitectura cliente-servidor. Los servidores son programas de computadora en ejecución que atienden las peticiones de otros programas, los clientes. Por tanto, el servidor realiza otras tareas para beneficio de los clientes. Ofrece a los clientes la posibilidad de compartir datos, información y recursos de hardware y software. Los clientes usualmente se conectan al servidor a través de la red pero también pueden acceder a él a través de la computadora donde está funcionando. En el contexto de redes Internet Protocol (IP), un servidor es un programa que opera como oyente de un socket.

Comúnmente los servidores proveen servicios esenciales dentro de una red, ya sea para usuarios privados dentro de una organización o compañía, o para usuarios públicos a través de Internet. Los tipos de servidores más comunes son servidor de base de datos, servidor de archivos, servidor de correo, servidor de impresión, servidor web, servidor de juego, y servidor de aplicaciones.

Un gran número de sistemas usa el modelo de red cliente-servidor, entre ellos los sitios web y los servicios de correo. Un modelo alternativo, el modelo red peer-to-peer permite a todas las computadoras conectadas actuar como clientes o servidores acorde a las necesidades.

3.3 SERVIDOR DE RESPALDO DE INFORMACION (BACKUP)

La Información de toda empresa es crítica e importante, por lo que tenemos la solución para evitar pérdidas. Instalamos un sistema que permite guardar respaldo de cada uno de los equipos de la red: se instala un agente en cada máquina, el cual interactúa con el servidor y se pueden realizar respaldos diarios, semanales, mensuales, lo que nos permite guardar nuestra valiosa información.

Las copias de seguridad son una parte muy importante del funcionamiento de una empresa, ya que la pérdida de información, puede suponer un gran coste de reconstrucción de la misma (si es posible), llegando incluso a detener parcialmente el funcionamiento de la empresa.

Las copias de seguridad se pueden realizar de muchas maneras, dependiendo del sistema de copias que la empresa disponga; pueden ser copias internas (en las mismas instalaciones de la empresa) o externas, enviando de manera cifrada la información a través de Internet a un servidor ubicado físicamente en un lugar lejano a las instalaciones de la empresa.

Es importante disponer de una copia de seguridad en una ubicación externa a la empresa, ya sea en nuestras instalaciones o dependiendo del tráfico en casa del gerente o responsable de la empresa.

Tanto si se realizan las copias interna como externamente, únicamente se envía la parte del archivo que ha se modificado, nunca se envía el archivo entero, por lo que la realización del respaldo es muy rápido.

Ej. Si disponemos de un archivo de 1Mb y lo modificamos añadiéndole 30 Kb, la información que se enviará a través de la red, es de 30Kb, ósea la parte modificada desde la última copia, a esto se le llama respaldo incremental.

Una buena manera de realizar copias de seguridad es:

1 copia diariamente

1 copia semanal

1 copia mensual

1 copia anual (histórico)

De esta manera, ante la pérdida de información, se podrá restaurar la información de la copia de ayer, perdiendo como máximo un día de trabajo. Si se eliminó uno o varios archivos hace varios días, se puede recuperar de la copia de la semana pasada o del mes pasado. Se guarda una copia de todos los años.

Si las copias están en un servidor externo, estarán sus datos seguros ante cualquier pérdida de información, fallo del disco duro o robo de computadores.

3.3.1 BACKUP y RESTORE

Planear y comprobar los procedimientos de backup del sistema es la única garantía que existe contra fallos del sistema, del SO, del software o cualquier otro tipo de circunstancias.

Las causas de error en un sistema de BD pueden agruparse en las siguientes categorías:

Físicas

- Son causadas por fallos del hardware, como por ejemplo del disco o de la CPU.

De Diseño

- Son agujeros en el software, ya sea en el SO o en el SGBD.

De Funcionamiento

- Son causadas por la intervención humana, debidos a fallos del DBA, configuraciones inapropiadas o mal planteamiento de los procedimientos de backup.

Del entorno

- Como por ejemplo desastres naturales, fallos de corriente, temperatura excesiva.

De entre todas estas posibilidades, el DBA sólo puede influir y prever los errores de funcionamiento, ya que el resto habitualmente no está dentro de sus responsabilidades y capacidades.

Dada la complejidad de los sistemas actuales y las necesidades cada vez más críticas en la disponibilidad de los sistemas, donde una BD caida puede causar pérdidas millonarias, puede ser interesante considerar los mecanismos de protección hardware y de redundancia que la tecnología nos proporciona:

- UPS o fuentes de corriente ininterrumpida,
- espejado de disco, o tecnología RAID,
- Componentes duplicados,
- Sistemas redundantes.

Una de las más importantes decisiones que un DBA debe tomar es decidir si arrancar la BD en modo ARCHIVELOG o no. Esta decisión tiene sus ventajas e inconvenientes:

Ventajas:

Aunque se pierdan los ficheros de datos, siempre se puede recuperar la BD con una copia antigua de los ficheros de datos y los ficheros de redo log archivados.

Es posible realizar backups en caliente.

Inconvenientes:

Se necesitará más espacio en disco.

El trabajo del DBA se incrementa al tener que determinar el destino del archivado de los redo log.

3.3.1.1 Presentación del Backup

Los backups se pueden clasificar en físicos y lógicos. Los físicos se realizan cuando se copian los ficheros que soportan la BD. Entre estos se encuentran los backups del SO, los backups en frío y los backups en caliente.

Los backups lógicos sólo extraen los datos de las tablas utilizando comandos SQL y se realizan con la utilidad export/import.

Backups del SO

Este tipo de backup es el más sencillo de ejecutar, aunque consume mucho tiempo y hace inaccesible al sistema mientras se lleva a cabo. Aprovecha el backup del SO para almacenar también todos los ficheros de la BD. Los pasos de este tipo de backup son los siguientes:

- Parar la BD y el SO
- Arrancar en modo superusuario.
- Realizar copia de todos los ficheros del sistema de ficheros
- Arrancar el sistema en modo normal y luego la BD.

Backups de la BD en Frio

Los backups en frio implican parar la BD en modo normal y copiar todos los ficheros sobre los que se asienta. Antes de parar la BD hay que parar también todas las aplicaciones que estén trabajando con la BD. Una vez realizada la copia de los ficheros, la BD se puede volver a arrancar.

Backups de la BD en Caliente

El backup en caliente se realiza mientras la BD está abierta y funcionando en modo ARCHIVELOG. Habrá que tener cuidado de realizarlo cuando la carga de la BD sea pequeña. Este tipo de backup consiste en copiar todos los ficheros correspondientes a un tablespace determinado, los ficheros redo log archivados y los ficheros de control. Esto para cada tablespace de la BD.

Backups Lógicos con Export/Import

Estas utilidades permiten al DBA hacer copias de determinados objetos de la BD, así como restaurarlos o moverlos de una BD a otra. Estas herramientas utilizan comandos del SQL para obtener el contenido de los objetos y escribirlos en/leerlos de ficheros

Una vez que se ha planeado una estrategia de backup y se ha probado, conviene automatizarla para facilitar así su cumplimiento.

3.3.1.2 Presentación de Restore

Existen diferentes modos de recuperar un fallo en la BD, y es importante que el DBA conozca cómo funciona cada uno de ellos para determinar cuándo ha de ser utilizado.

Una de las mayores responsabilidades del DBA consiste en tener la BD a punto, y prepararla ante la posibilidad de que se produzca un fallo. Así, ante un fallo el DBA podrá recuperar la BD en el menor tiempo posible. Los procesos de recuperación dependen del tipo de error y de las estructuras afectadas.

Así, los tipos de error que se pueden producir son:

Errores de Usuario

Como por ejemplo un usuario borrando una fila o eliminando una tabla. Estos errores se solucionan importando una tabla de una copia lógica anterior. Si no se dispone de la copia lógica, se puede recuperar la BD en una instancia auxiliar, exportar la tabla en cuestión de la instancia auxiliar e importarla en la instancia operativa.

Fallos de Sentencias

Se definen como la imposibilidad del SGBD Oracle de ejecutar alguna sentencia SQL. Un ejemplo de esto se produce cuando se intenta una selección de una tabla que no existe. Estos fallos se recuperan automáticamente mediante un rollback de la transacción que contenía la sentencia fallida. El usuario necesitará volver a ejecutar otra vez la transacción cuando se haya solucionado la causa del problema.

Fallos de Procesos

Es una terminación anormal de un proceso. Si el proceso era un proceso de usuario, del servidor o de una aplicación el PMON efectuará la recuperación del proceso. Si el proceso era alguno de los de background, la instancia debe de ser parada y arrancada de nuevo, proceso durante el cual se recupera la caída efectuando un roll forward y un rollback de las transacciones no confirmadas.

Fallos de la Red

Algunas veces los fallos en la red producen fallos de proceso, que son tratados por el PMON. Si en el error de red se ve envuelta una transacción distribuida, una vez que se reestablece la conexión, el proceso RECO resuelve los conflictos automáticamente.

Fallos de Instancia

Pueden deberse a fallos físicos o de diseño del software que hacen que algún proceso background caiga y la instancia con él. La recuperación es automática cuando se levanta la BD, tomándose más o menos tiempo en la recuperación.

Fallos del Sistema

Son los fallos más peligrosos, no sólo porque se pueden perder datos, sino porque se tarda más tiempo en recuperar que los otros fallos. Además se depende mucho de la experiencia del DBA para levantar la BD rápidamente y sin pérdida (o casi) de datos.

Existen tres tipos de recuperación básicas: a nivel de bloque, de thread y física.

Recuperación de bloques

Es el mecanismo de recuperación más simple, y se realiza automáticamente. Se produce cuando un proceso muere justo cuando está cambiando un bloque, y se utilizan los registros redo log en línea para reconstruir el bloque y escribirlo en disco.

Recuperación de threads

Se realiza automáticamente cuando Oracle descubre que una instancia muere dejando abierto un thread, entonces se restauran los bloques de datos modificados que estaban en el cache de la instancia muerta, y cerrando el thread que estaba abierto. La recuperación se efectúa automáticamente cuando la BD se levanta.

Recuperación física

Se realiza como respuesta a un comando RECOVER. Se utiliza para convertir los ficheros de backup en actuales, o para restaurar los cambios que fueron perdidos cuando un fichero de datos fue puesto offline sin un checkpoint, aplicando los fichero redo log archivados y en línea.

3.3.1.3 Backup (Full, Incremental y Diferencial)

Backup Full

Se crea una copia de resguardo de todas las carpetas y archivos que seleccionemos en la herramienta para hacer el backup. Es ideal para crear la primera copia de todo el contenido de una unidad o bien de sus archivos de datos solamente.

Ventajas:

- Todos los archivos seleccionados pasan a formar parte de este backup.
- Para restaurar uno o más archivos, se los toma directamente de este backup.

Backup Incremental

Esta clase de backup, como su nombre lo indica, solamente genera una copia de resguardo con todos aquellos archivos que hayan sido modificados (o aparenten haberlo sido debido a cambios en su fecha de modificación) o se hayan creado desde el último backup realizado, ya sea este último incremental o completo. Si se utiliza por primera vez en una unidad en vez de un backup completo, se comportará como este último, pero en los backups siguientes, irá copiando solamente lo nuevo o lo modificado.

Ventajas:

- Es mucho más rápido que el uso de sucesivos backups completos.
- Requiere menor cantidad de espacio en el medio destino que sucesivos backups completos.
- Se pueden ir manteniendo diferentes versiones de los mismos archivos en cada uno de los backups incrementales, con lo que se podría restaurar la versión deseada.

Desventajas:

- Se pueden estar copiando archivos cuyo contenido no haya sido modificado, ya que compara las fechas de modificación, y se pueden haber guardado sin que se hayan efectuado cambios en su contenido.
- Para restaurar determinados archivos o inclusive, todos, es necesario tener todos los medios de los backups incrementales que se hayan efectuado desde el último backup completo o primer backup incremental.
- Como consecuencia de esta búsqueda por varios backups, la restauración de unos pocos archivos toma mucho más tiempo.

Backup Diferencial

Es similar al incremental, la única diferencia es que compara el contenido de los archivos a la hora de determinar cuáles se modificaron de manera tal que solamente copia aquéllos que hayan cambiado realmente y no se deja engañar por las fechas de modificación de los mismos.

Ventajas:

- Todas las del backup incremental, pero requieren aún menor espacio en el medio de destino.

Desventajas:

- Todas las del backup incremental, menos la última.
- No todas las herramientas del backup dan soporte a esta clase.

3.4 STORAGES

Son sistemas (combinación de hardware y software) dedicados exclusivamente a guardar información que sea accesible por entes consumidores (básicamente servidores).

Apoyados en estos sistemas se pueden crear estructuras que permitan su uso, ya sea mediante SAN (Storage Área Network), DAS (Direct Attach Storage), NAS (Network Attached Storage)

3.4.1 SAN (Storage Area Network)

Una "SAN" (Red de área de almacenamiento) es una red de almacenamiento integral. Se trata de una arquitectura completa que agrupa los siguientes elementos:

- Una red de alta velocidad de canal de fibra o SCSI
- Un equipo de interconexión dedicado (conmutadores, puentes, etc.)
- Elementos de almacenamiento de red (discos duros)

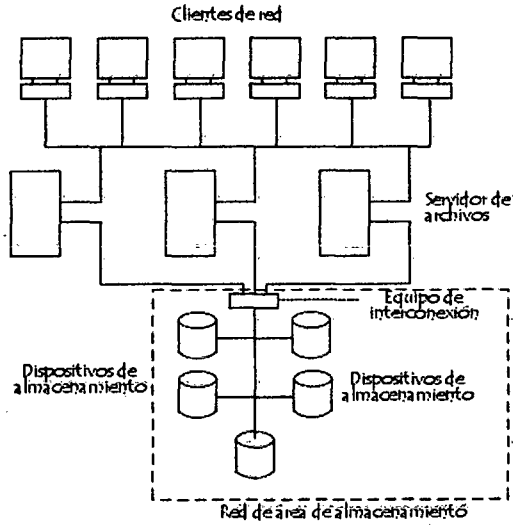


Gráfico N° 05 SAN (Storage Area Network)

Una SAN es una red dedicada al almacenamiento que está conectada a las redes de comunicación de una compañía. Además de contar con interfaces de red tradicionales, los equipos con acceso a la SAN tienen una interfaz de red específica que se conecta a la SAN.

Ventajas y desventajas

El rendimiento de la SAN está directamente relacionado con el tipo de red que se utiliza. En el caso de una red de canal de fibra, el ancho de banda es de aproximadamente 100 megabytes/segundo (1.000 megabits/segundo) y se puede extender aumentando la cantidad de conexiones de acceso.

La capacidad de una SAN se puede extender de manera casi ilimitada y puede alcanzar cientos y hasta miles de terabytes.

Una SAN permite compartir datos entre varios equipos de la red sin afectar el rendimiento porque el tráfico de SAN está totalmente separado del tráfico de usuario. Son los servidores de aplicaciones que funcionan como una interfaz entre la red de datos (generalmente un canal de fibra) y la red de usuario (por lo general Ethernet).

Por otra parte, una SAN es mucho más costosa que una NAS ya que la primera es una arquitectura completa que utiliza una tecnología que todavía es muy cara. Normalmente, cuando una compañía estima el TCO (Coste total de propiedad) con respecto al coste por byte, el coste se puede justificar con más facilidad.

3.4.2 DAS (Direct Attach Storage)

Es el método tradicional de almacenamiento y el más sencillo. Consiste en conectar el dispositivo de almacenamiento directamente al servidor o estación de trabajo, es decir, físicamente conectado al dispositivo que hace uso de él.

Tanto en DAS como en SAN (Storage Area Network), las aplicaciones y programas de usuarios hacen sus peticiones de datos al sistema de ficheros directamente. La diferencia entre ambas tecnologías reside en la manera en la que dicho sistema de ficheros obtiene los datos requeridos del almacenamiento. En una DAS, el almacenamiento es local al sistema de ficheros, mientras que en una SAN, el almacenamiento es remoto. En el lado opuesto se encuentra la tecnología NAS (Network-attached storage), donde las aplicaciones hacen las peticiones de datos a los sistemas de ficheros de manera remota.

Características

Los protocolos principales usados en DAS son SCSI, SAS y Fibre Channel, tradicionalmente un sistema DAS habilita capacidad extra de almacenamiento a un servidor, mientras mantiene alto ancho de banda y tasas de acceso. Un típico sistema DAS está hecho de uno o más dispositivos de almacenamiento como discos rígidos, y uno o más controladores. La interfaz con el servidor o con la estación de trabajo está hecha por medio de un "host bus adapter" (HBA).

Un típico sistema DAS provee controladores embebidos. El manejo del RAID es "off-load", o simplemente sin RAID. Los HBA´s pueden ser usados reduciendo costos. Los controladores RAS también habilitan acceso compartido al almacenamiento, que permite servidores múltiples (no más de cuatro) para acceder a la misma unidad lógica, una característica que es simplemente usada para "clustering". En este punto, los sistemas DAS de alto rango comparten similaridades con los sistemas SAN de nivel básico

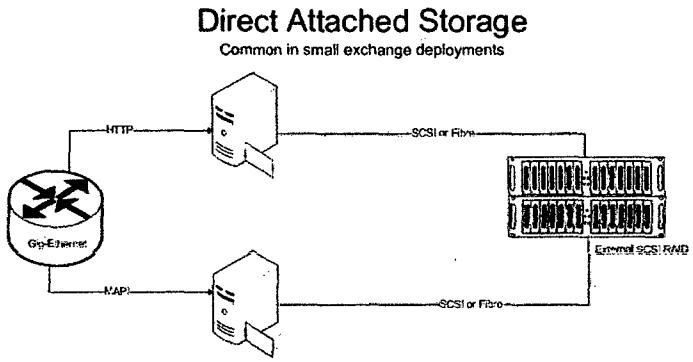


Gráfico N° 06 DAS (Direct Attach Storage)

Desventajas

Se está usando el término DAS como "Islas de Información". Las desventajas de DAS incluyen incapacidad para compartir datos o recursos no usados con otros servidores. Ambas arquitecturas, NAS (almacenamiento adjuntado en red) y SAN (red de área de almacenamiento), intentan tratarlas, pero introducen nuevas cuestiones a tratar, tales como altos costos iniciales, manejabilidad, seguridad y contención para recursos

3.4.3 NAS (Network Attached Storage)

Es todo sistema que permita compartir almacenamiento de data en un punto central a través de la red. Este punto central se le conoce como el servidor NAS (NAS server). El servidor NAS puede incluir uno o más discos duros, y tiene la capacidad de almacenar y compartir data proveniente de diferentes fuentes (computadoras, servidores, servicios en el web, entre otros).

Un servidor NAS puede manejar el intercambio de documentos utilizando protocolos como SMB y NFS. Este puede autenticar los usuarios y determinar que privilegios tienen para cada directorio. A diferencia de un servidor de archivos (File Server), el servidor NAS es uno más simplificado y no incluye un sistema operativo completo. Estos también no suelen a incluir accesorios tales como teclados, ratón y monitores.

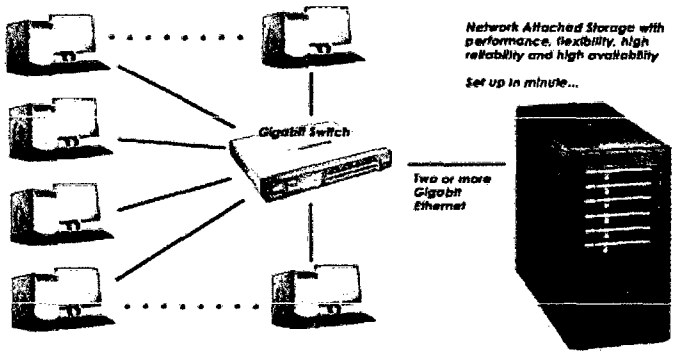


Gráfico N° 07 NAS (Network Attached Storage)

Es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador (Servidor) con computadoras personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un Sistema Operativo optimizado para dar acceso con los protocolos CIFS, NFS, FTP o TFTP.

Generalmente, los sistemas NAS son dispositivos de almacenamiento específicos a los que se accede desde los equipos a través de protocolos de red (normalmente TCP/IP). También se podría considerar un sistema NAS a un servidor (Microsoft Windows, Linux, etc.) que comparte sus unidades por red, pero la definición suele aplicarse a sistemas específicos.

Los protocolos de comunicaciones NAS están basados en archivos por lo que el cliente solicita el archivo completo al servidor y lo maneja localmente, están por ello orientados a información almacenada en archivos de pequeño tamaño y gran cantidad. Los protocolos usados son protocolos de compartición de archivos como NFS o Microsoft Common Internet File System (CIFS).

Muchos sistemas NAS cuentan con uno o más dispositivos de almacenamiento para incrementar su capacidad total. Frecuentemente, estos dispositivos están dispuestos en RAID (Redundant Arrays of Independent Disks) o contenedores de almacenamiento redundante.

Un servidor NAS puede ser tan sencillo como un producto para el hogar, como tan complejo para un ambiente empresarial. Un ejemplo de un servidor NAS para

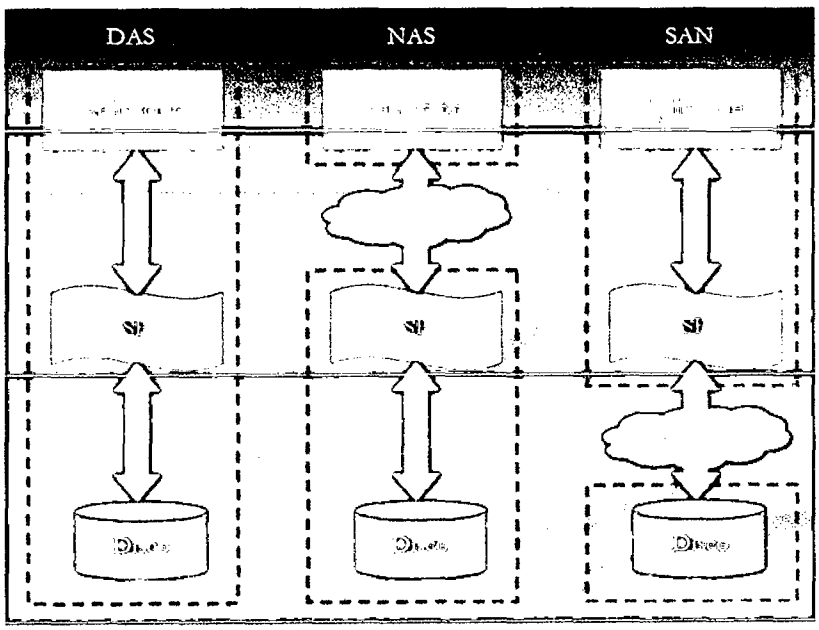
el hogar es el Drobo (favorito en dgtallikä), a diferencia del Windows Home Server quien su funcionamiento se asimila más al de un servidor de archivos (File Server) al contar este último con un sistema operativo completo (basado en Windows 2003). Un ejemplo de un servidor NAS para un ambiente empresarial son los productos StorageWorks de HP y estos incluyen toda una serie de herramientas para la administración de cada servidor.

Comparativas

El opuesto a NAS es la conexión DAS (Direct Attached Storage) mediante conexiones SCSI o la conexión SAN (Storage Area Network) por fibra óptica, en ambos casos con tarjetas de conexión específicas de conexión al almacenamiento. Estas conexiones directas (DAS) son por lo habitual dedicadas.

En la tecnología NAS, las aplicaciones y programas de usuario hacen las peticiones de datos a los sistemas de archivos de manera remota mediante protocolos CIFS y NFS, y el almacenamiento es local al sistema de archivos. Sin embargo, DAS y SAN realizan las peticiones de datos directamente al sistema de archivos.

Las ventajas del NAS sobre la conexión directa (DAS) son la capacidad de compartir las unidades, un menor coste, la utilización de la misma infraestructura de red y una gestión más sencilla. Por el contrario, NAS tiene un menor rendimiento y confiabilidad por el uso compartido de las comunicaciones.



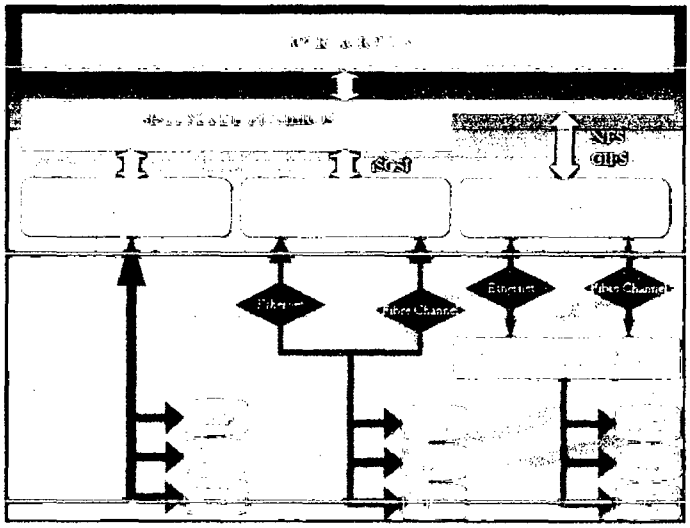


Gráfico N° 08 Comparativas entre DAS SAN y NAS

A pesar de las diferencias, NAS y SAN no son excluyentes y pueden combinarse en una misma solución: Híbrido SAN-NAS .

3.5 TAPE BACKUP

Son unidades de respaldo de información. Es un término general y abarca muchas tecnologías (DATs, DLTs, Ultrium, etc) y por lo general se utilizan en el ámbito empresarial, para realizar las copias de seguridad de la información de las empresas. Tienen capacidades desde varios megas (unidades viejas) hasta varios cientos de GB o aún más en unidades tope de línea, que por lo son robotizadas y capaces de manejar cientos o miles de cintas (se llaman librerías por lo general).

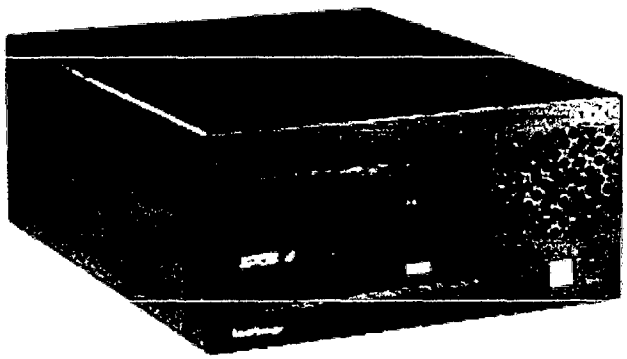


Gráfico N°9 Tape Backup

3.6 AUTOLOADER

Es un dispositivo que automáticamente carga los cartuchos de cinta de manera secuencial o en un orden específico, para luego grabar o leer información.

Requieren de un software para su funcionamiento que normalmente no se incluye como parte de la solución.

Pueden ser administrados remotamente.

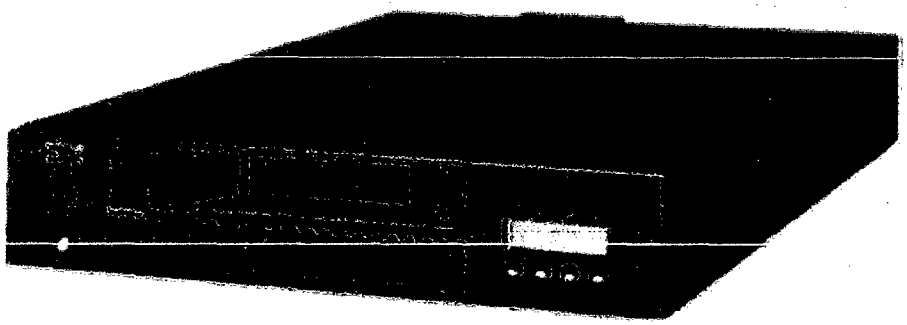


Gráfico N°10 AutoLoader

3.7 RAID

Proviene del inglés Redundant Array of Independent Disks (Conjunto redundante de discos independientes), hace referencia a un sistema de almacenamiento de datos que usa múltiples unidades de almacenamiento de datos (discos duros o SSD) entre los que se distribuyen o replican los datos. Dependiendo de su configuración (a la que suele llamarse «nivel»), los beneficios de un RAID respecto a un único disco son uno o varios de los siguientes: mayor integridad, mayor tolerancia a fallos, mayor throughput (rendimiento) y mayor capacidad.

En el nivel más simple, un RAID combina varios discos duros en una sola unidad lógica. Así, en lugar de ver varios discos duros diferentes, el sistema operativo ve uno solo. Los RAIDs suelen usarse en servidores y normalmente se implementan con unidades de disco de la misma capacidad. Debido al decremento en el precio de los discos duros y la mayor disponibilidad de las opciones RAID incluidas en los chipsets de las placas base, los RAIDs se encuentran también como opción en las computadoras personales más avanzadas. Esto es especialmente frecuente en las computadoras dedicadas a tareas intensivas y que requiera asegurar la integridad de los datos en caso de fallo del sistema.

Todas las implementaciones pueden soportar el uso de uno o más discos de reserva (hot spare), unidades preinstaladas que pueden usarse inmediatamente

tras el fallo de un disco del RAID. Esto reduce el tiempo del período de reparación al acortar el tiempo de reconstrucción del RAID.

- **PARIDAD**

Vamos a intentar explicar de forma simple por qué la información de paridad permite realizar la recuperación de los datos perdidos. La premisa fundamental *es dotar al sistema de capacidad para recuperar la información al vuelo en el caso* de un error de disco usando una forma de redundancia a la que se le llama paridad.

Para explicarlo de una forma sencilla, la paridad es la suma de todos los dispositivos utilizados en una matriz. Recuperarse del fallo de dispositivo es posible leyendo los datos buenos que quedan y comparándolos con el dato de paridad almacenado en el conjunto. La paridad es usada por los niveles de RAID 2, 3, 4 y 5. RAID 1 no utiliza la paridad puesto que todos los datos están completamente duplicados al tratarse de un espejo.

Para entender la paridad podemos asemejarla a una ecuación algebraica sencilla en la que la Paridad es el cálculo de la suma de todos los datos (en la práctica será un checksum de datos). Si se produce un error en un disco ese dato pasa a ser una incógnita que se puede calcular despejándola de la ecuación.

Gráfico N° 11 Paridad

3.7.1 RAID 0 (Data Striping)

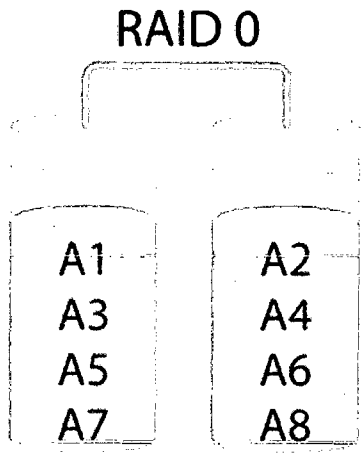


Gráfico N°12 RAID 0

Un RAID 0 distribuye los datos equitativamente entre dos o más discos sin información de paridad que proporcione redundancia. Es importante señalar que el RAID 0 no era uno de los niveles RAID originales y que no es redundante. El RAID 0 se usa normalmente para incrementar el rendimiento, aunque también puede utilizarse como forma de crear un pequeño número de grandes discos virtuales a partir de un gran número de pequeños discos físicos. Un RAID 0 puede ser creado con discos de diferentes tamaños, pero el espacio de almacenamiento añadido al conjunto estará limitado por el tamaño del disco más pequeño (por ejemplo, si un disco de 300 GB se divide con uno de 100 GB, el tamaño del conjunto resultante será sólo de 200 GB, ya que cada disco aporta 100GB). Una buena implementación de un RAID 0 dividirá las operaciones de lectura y escritura en bloques de igual tamaño, por lo que distribuirá la información equitativamente entre los dos discos. También es posible crear un RAID 0 con más de dos discos, si bien, la fiabilidad del conjunto será igual a la fiabilidad media de cada disco entre el número de discos del conjunto; es decir, la fiabilidad total —medida como MTTF o MTBF— es (aproximadamente) inversamente proporcional al número de discos del conjunto (pues para que el conjunto falle es suficiente con que lo haga cualquiera de sus discos).

3.7.2 RAID 1 (Mirroring)

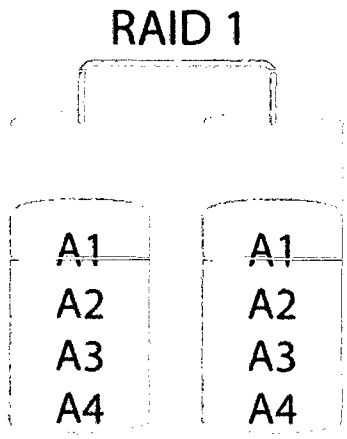


Gráfico N°13 RAID 1

Un RAID 1 crea una copia exacta (o espejo) de un conjunto de datos en dos o más discos. Esto resulta útil cuando el rendimiento en lectura es más importante que la capacidad. Un conjunto RAID 1 sólo puede ser tan grande como el más pequeño de sus discos. Un RAID 1 clásico consiste en dos discos en espejo, lo que incrementa exponencialmente la fiabilidad respecto a un solo disco; es decir, la probabilidad de fallo del conjunto es igual al producto de las probabilidades de fallo de cada uno de los discos (pues para que el conjunto falle es necesario que lo hagan todos sus discos).

Adicionalmente, dado que todos los datos están en dos o más discos, con hardware habitualmente independiente, el rendimiento de lectura se incrementa aproximadamente como múltiplo lineal del número del copias; es decir, un RAID 1 puede estar leyendo simultáneamente dos datos diferentes en dos discos diferentes, por lo que su rendimiento se duplica. Para maximizar los beneficios sobre el rendimiento del RAID 1 se recomienda el uso de controladoras de disco independientes, una para cada disco (práctica que algunos denominan splitting o duplexing).

Como en el RAID 0, el tiempo medio de lectura se reduce, ya que los sectores a buscar pueden dividirse entre los discos, bajando el tiempo de búsqueda y subiendo la tasa de transferencia, con el único límite de la velocidad soportada por la controladora RAID. Sin embargo, muchas tarjetas RAID 1 IDE antiguas leen sólo de un disco de la pareja, por lo que su rendimiento es igual al de un único disco. Algunas implementaciones RAID 1 antiguas también leen de ambos discos simultáneamente y comparan los datos para detectar errores.

Al escribir, el conjunto se comporta como un único disco, dado que los datos deben ser escritos en todos los discos del RAID 1. Por tanto, el rendimiento no mejora.

3.7.3 RAID 2

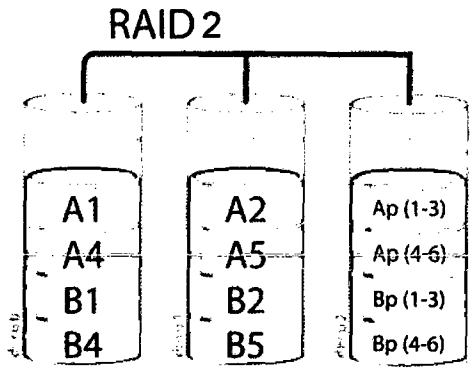


Gráfico N°14 RAID 2

Un RAID 2 usa división a nivel de bits con un disco de paridad dedicado y usa un código de Hamming para la corrección de errores. El RAID 2 se usa rara vez en la práctica. Uno de sus efectos secundarios es que normalmente no puede atender varias peticiones simultáneas, debido a que por definición cualquier simple bloque de datos se dividirá por todos los miembros del conjunto, residiendo la misma dirección dentro de cada uno de ellos. Así, cualquier operación de lectura o escritura exige activar todos los discos del conjunto, suele ser un poco lento porque se producen cuellos de botella. Son discos paralelos pero no son independientes (no se puede leer y escribir al mismo tiempo).

3.7.4 RAID 3

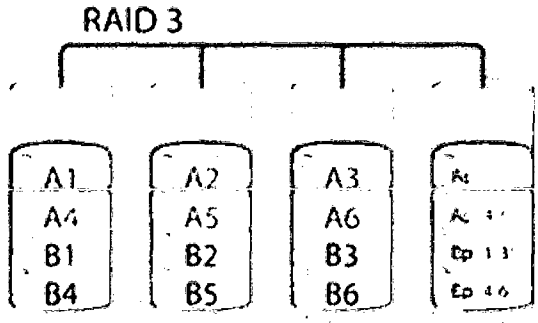


Gráfico N°15 RAID 3

Un RAID 3 divide los datos a nivel de bytes en lugar de a nivel de bloques . Los discos son sincronizados por la controladora para funcionar al unísono. Éste es el

único nivel RAID original que actualmente no se usa. Permite tasas de transferencias extremadamente altas.

Teóricamente, un RAID 3 necesitaría 39 discos en un sistema informático moderno: 32 se usarían para almacenar los bits individuales que forman cada palabra y 7 se usarían para la corrección de errores.

En el ejemplo del gráfico, una petición del bloque «A» formado por los bytes A1 a A6 requeriría que los tres discos de datos buscaran el comienzo (A1) y devolvieran su contenido. Una petición simultánea del bloque «B» tendría que esperar a que la anterior concluyese.

3.7.5 RAID 4

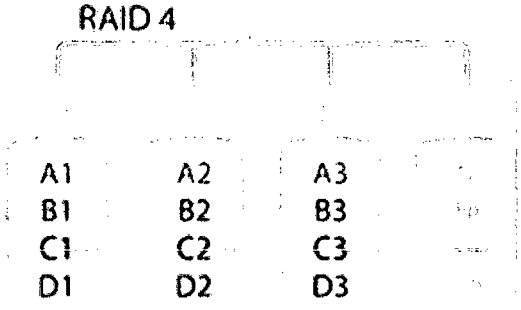


Gráfico N°16 RAID 4

Un RAID 4, también conocido como IDA (acceso independiente con discos dedicados a la paridad) usa división a nivel de bloques con un disco de paridad dedicado. Necesita un mínimo de 3 discos físicos. El RAID 4 es parecido al RAID 3 excepto porque divide a nivel de bloques en lugar de a nivel de bytes. Esto permite que cada miembro del conjunto funcione independientemente cuando se solicita un único bloque. Si la controladora de disco lo permite, un conjunto RAID 4 puede servir varias peticiones de lectura simultáneamente. En principio también sería posible servir varias peticiones de escritura simultáneamente, pero al estar toda la información de paridad en un solo disco, éste se convertiría en el cuello de botella del conjunto.

En el gráfico de ejemplo anterior, una petición del bloque «A1» sería servida por el disco 0. Una petición simultánea del bloque «B1» tendría que esperar, pero una petición de «B2» podría atenderse concurrentemente.

3.7.6 RAID 5

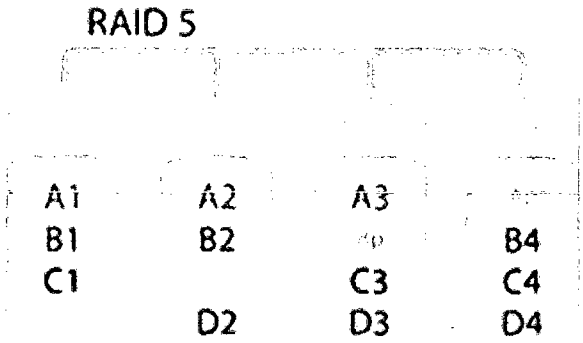


Gráfico N°17 RAID 5

Un RAID 5 (también llamado distribuido con paridad) es una división de datos a nivel de bloques distribuyendo la información de paridad entre todos los discos miembros del conjunto. El RAID 5 ha logrado popularidad gracias a su bajo coste de redundancia. Generalmente, el RAID 5 se implementa con soporte hardware para el cálculo de la paridad. RAID 5 necesitará un mínimo de 3 discos para ser implementado.

En el gráfico de ejemplo anterior, una petición de lectura del bloque «A1» sería servida por el disco 0. Una petición de lectura simultánea del bloque «B1» tendría que esperar, pero una petición de lectura de «B2» podría atenderse concurrentemente ya que sería servida por el disco 1.

Cada vez que un bloque de datos se escribe en un RAID 5, se genera un bloque de paridad dentro de la misma división (stripe). Un bloque se compone a menudo de muchos sectores consecutivos de disco. Una serie de bloques (un bloque de cada uno de los discos del conjunto) recibe el nombre colectivo de división (stripe). Si otro bloque, o alguna porción de un bloque, es escrita en esa misma división, el bloque de paridad (o una parte del mismo) es recalculada y vuelta a escribir. El disco utilizado por el bloque de paridad está escalonado de una división a la siguiente, de ahí el término «bloques de paridad distribuidos». Las escrituras en un RAID 5 son costosas en términos de operaciones de disco y tráfico entre los discos y la controladora.

Los bloques de paridad no se leen en las operaciones de lectura de datos, ya que esto sería una sobrecarga innecesaria y disminuiría el rendimiento. Sin embargo, los bloques de paridad se leen cuando la lectura de un sector de datos provoca un error de CRC. En este caso, el sector en la misma posición relativa dentro de cada uno de los bloques de datos restantes en la división y dentro del bloque de paridad en la división se utiliza para reconstruir el sector erróneo. El error CRC se oculta

así al resto del sistema. De la misma forma, si falla un disco del conjunto, los bloques de paridad de los restantes discos son combinados matemáticamente con *los bloques de datos de los restantes discos para reconstruir los datos del disco* que ha fallado «al vuelo».

Lo anterior se denomina a veces Modo Interino de Recuperación de Datos (Interim Data Recovery Mode). El sistema sabe que un disco ha fallado, pero sólo con el fin de que el sistema operativo pueda notificar al administrador que una unidad necesita ser reemplazada: las aplicaciones en ejecución siguen funcionando ajenas al fallo. Las lecturas y escrituras continúan normalmente en el conjunto de discos, aunque con alguna degradación de rendimiento. La diferencia entre el RAID 4 y el RAID 5 es que, en el Modo Interno de Recuperación de Datos, el RAID 5 puede ser ligeramente más rápido, debido a que, cuando el CRC y la paridad están en el disco que falló, los cálculos no tienen que realizarse, mientras que en el RAID 4, si uno de los discos de datos falla, los cálculos tienen que ser realizados en cada acceso.

El fallo de un segundo disco provoca la pérdida completa de los datos.

El número máximo de discos en un grupo de redundancia RAID 5 es teóricamente ilimitado, pero en la práctica es común limitar el número de unidades. Los inconvenientes de usar grupos de redundancia mayores son una mayor probabilidad de fallo simultáneo de dos discos, un mayor tiempo de reconstrucción y una mayor probabilidad de hallar un sector irrecuperable durante una reconstrucción. A medida que el número de discos en un conjunto RAID 5 crece, el MTBF (tiempo medio entre fallos) puede ser más bajo que el de un único disco. Esto sucede cuando la probabilidad de que falle un segundo disco en los N-1 discos restantes de un conjunto en el que ha fallado un disco en el tiempo necesario para detectar, reemplazar y recrear dicho disco es mayor que la probabilidad de fallo de un único disco. Una alternativa que proporciona una protección de paridad dual, permitiendo así mayor número de discos por grupo, es el RAID 6.

Algunos vendedores RAID evitan montar discos de los mismos lotes en un grupo de redundancia para minimizar la probabilidad de fallos simultáneos al principio y el final de su vida útil.

Las implementaciones RAID 5 presentan un rendimiento malo cuando se someten a cargas de trabajo que incluyen muchas escrituras más pequeñas que el tamaño de una división (stripe). Esto se debe a que la paridad debe ser actualizada para cada escritura, lo que exige realizar secuencias de lectura, modificación y escritura tanto para el bloque de datos como para el de paridad. Implementaciones

más complejas incluyen a menudo cachés de escritura no volátiles para reducir este problema de rendimiento.

En el caso de un fallo del sistema cuando hay escrituras activas, la paridad de una división (stripe) puede quedar en un estado inconsistente con los datos. Si esto no se detecta y repara antes de que un disco o bloque falle, pueden perderse datos debido a que se usará una paridad incorrecta para reconstruir el bloque perdido en dicha división. Esta potencial vulnerabilidad se conoce a veces como «agujero de escritura». Son comunes el uso de caché no volátiles y otras técnicas para reducir la probabilidad de ocurrencia de esta vulnerabilidad.

3.7.7 RAID 6

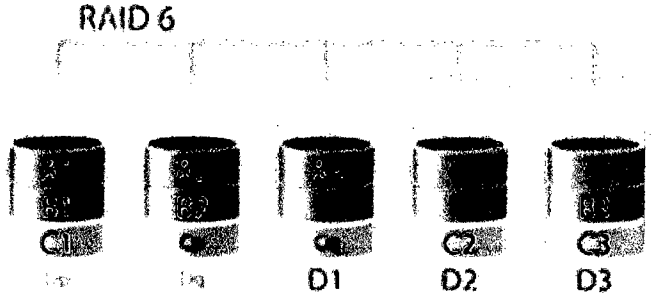


Gráfico N°18 RAID 6

Un RAID 6 amplía el nivel RAID 5 añadiendo otro bloque de paridad, por lo que divide los datos a nivel de bloques y distribuye los dos bloques de paridad entre todos los miembros del conjunto. El RAID 6 no era uno de los niveles RAID originales.

El RAID 6 puede ser considerado un caso especial de código Reed-Solomon.1 El *RAID 6*, siendo un caso degenerado, exige sólo sumas en el Campo de galois. Dado que se está operando sobre bits, lo que se usa es un campo binario de Galois ($GF(2^m)$). En las representaciones cíclicas de los campos binarios de Galois, la suma se calcula con un simple XOR.

Tras comprender el RAID 6 como caso especial de un código Reed-Solomon, se puede ver que es posible ampliar este enfoque para generar redundancia simplemente produciendo otro código, típicamente un polinomio en $GF(2^3)$ (m = 8 significa que estamos operando sobre bytes). Al añadir códigos adicionales es posible alcanzar cualquier número de discos redundantes, y recuperarse de un fallo de ese mismo número de discos en cualquier punto del conjunto, pero en el nivel RAID 6 se usan dos únicos códigos.

Al igual que en el RAID 5, en el RAID 6 la paridad se distribuye en divisiones (stripes), con los bloques de paridad en un lugar diferente en cada división.

El RAID 6 es ineficiente cuando se usa un pequeño número de discos, pero a medida que el conjunto crece y se dispone de más discos la pérdida en capacidad de almacenamiento se hace menos importante, creciendo al mismo tiempo la probabilidad de que dos discos fallen simultáneamente. El RAID 6 proporciona protección contra fallos dobles de discos y contra fallos cuando se está reconstruyendo un disco. En caso de que sólo tengamos un conjunto puede ser más adecuado que usar un RAID 5 con un disco de reserva (hot spare).

La capacidad de datos de un conjunto RAID 6 es n-2, siendo n el número total de discos del conjunto.

Un RAID 6 no penaliza el rendimiento de las operaciones de lectura, pero sí el de las de escritura debido al proceso que exigen los cálculos adicionales de paridad. Esta penalización puede minimizarse agrupando las escrituras en el menor número posible de divisiones (stripes), lo que puede lograrse mediante el uso de un sistema de archivos WAFL.

3.8 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.

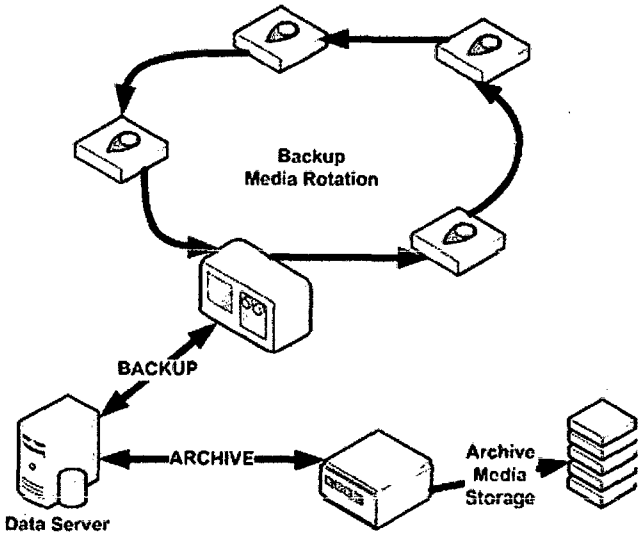


Gráfico N°19 Diagrama de Respaldos Genérico

3.8.1 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. 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.

3.8.2 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 ™, 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.

3.8.3. 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.

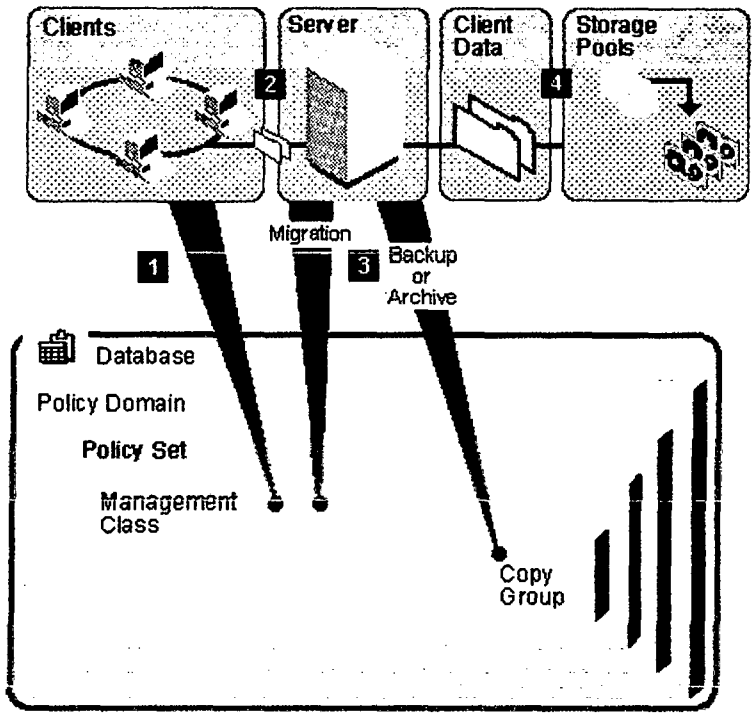


Gráfico N°20 Procesos de Copia de Seguridad, Archivado y migración

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.

3.8.4. 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.

3.8.5. Evolución de Tivoli Storage Manager.

TSM Manager 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".

TSM Manager 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

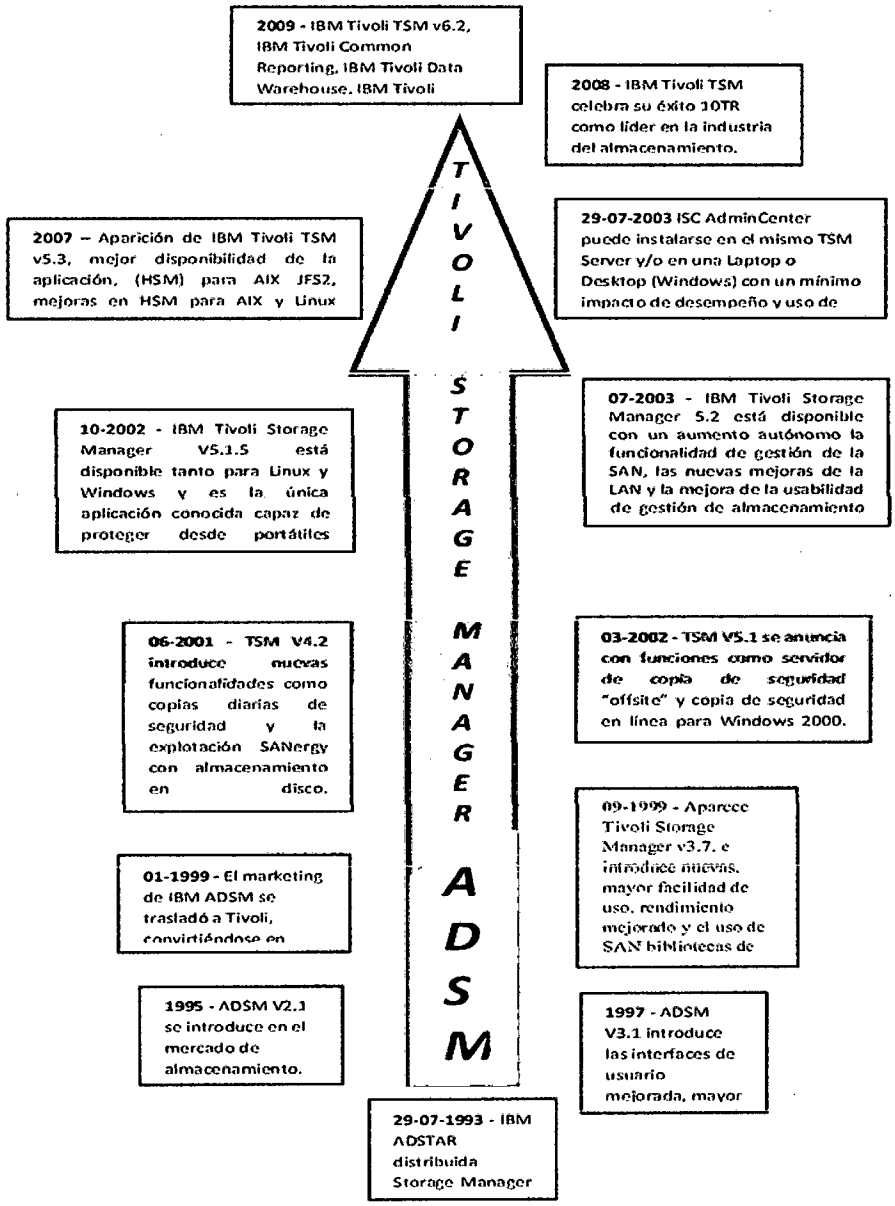


Gráfico N°21 Evolución de TSM.

3.9 SYSTEM CENTER DATA PROTECTION MANAGER.

Data Protection Manager 2012 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 Copyl 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 2012, apoya la protección de servidores de archivos Windows, Exchange Server, Microsoft SQL Server, SharePoint, Microsoft Virtual Server y Bare Metal Restore (BMR).

3.9.1 Componentes de System Center Data Protection Manager.

Para la base de datos DPM, DPM requiere una instancia dedicada de la versión de 64 bits de SQL Server 2012, SQL Server 2008 R2 o SQL Server 2008 R2 SP1, edición Enterprise o Standard. Durante la instalación, puede seleccionar que el programa de instalación de DPM instale SQL Server 2008 R2 en el servidor DPM o bien especificar que DPM use una instancia remota de SQL Server.

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

3.9.2. 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 2012 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 2012 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 perdida de información en el proceso de restauración de la información.
- DPM 2012 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 2012 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 2012 para proporcionar copias de seguridad de agente de aplicación coherente de todas y todos los huéspedes que residen en un host. DPM 2012 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 2012 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 2012 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 2012 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 2012 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 realicé 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 2012 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 2012 también puede cargar todos sus informes y alertas a la consola de Microsoft Operations Manager.

- Protección y recuperación para servidores de Exchange.
- DPM 2012 protege intercambio de bases de datos de servidores cada 15 minutos.
- Protección y recuperación de Sharepoint.
- *DPM 2012 proporciona la mejor clase de protección y recuperación para* Microsoft Office SharePoint Technologies.
- Protección y recuperación para Microsoft SQL Server.
- DPM 2012 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 2012 extiende la protección para ordenadores portátiles y no solo para PC's de escritorios fijos.

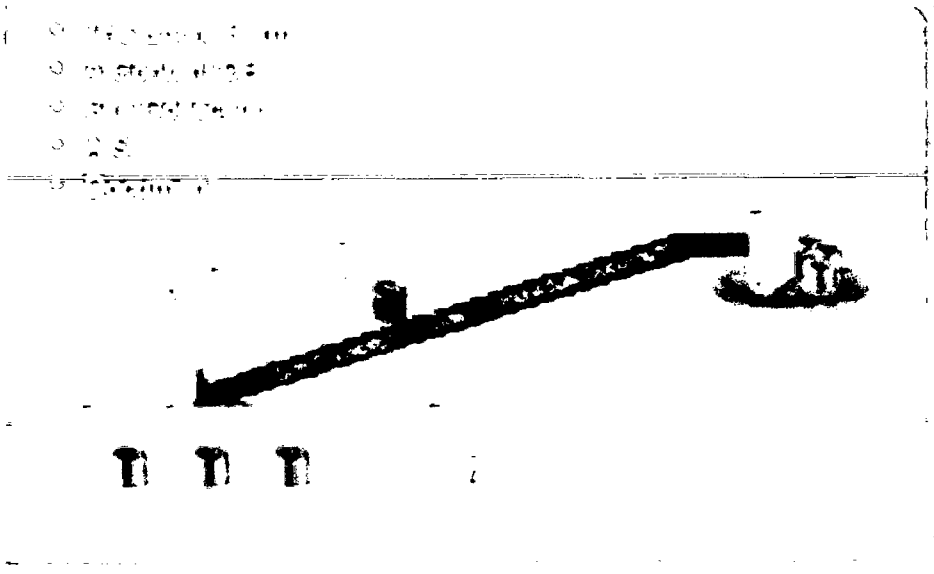


Gráfico N°22 Estructura de Data Protection Manager.

3.9.3. 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 2012 (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 2012 Management Shell (PowerShell) cmdlets.

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

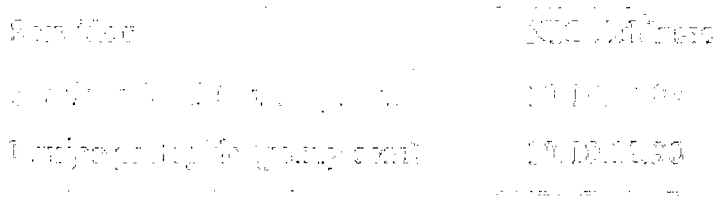
- Asegúrese de que la resolución de nombres este activa y que tanto el servidor de DPM como el servidor del cual se realizará la copia de seguridad se puede conectar sin problema.
- Configurar la subred de copia de seguridad y su máscara correspondiente utilizando el complemento BackupNetworkAddress.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

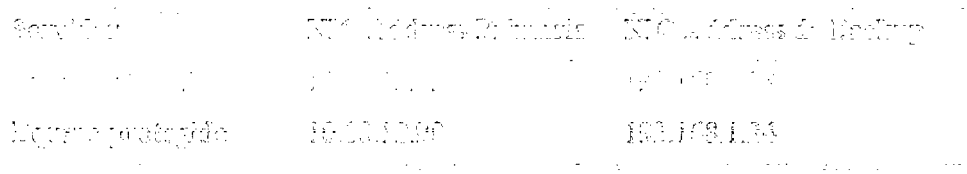
En este ejemplo se detalla el proceso de creación de una dirección de red de copia de seguridad de un servidor DPM para proteger otro servidor. Todos los nombres y direcciones son hipotéticos y sólo como ejemplo.

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".



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.



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.

3.9.4. 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.

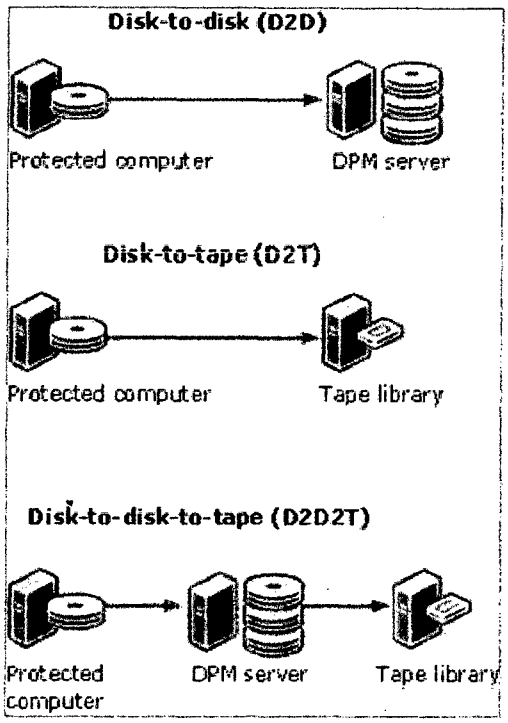


Gráfico N°23 Tratamiento de la información DPM.

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.

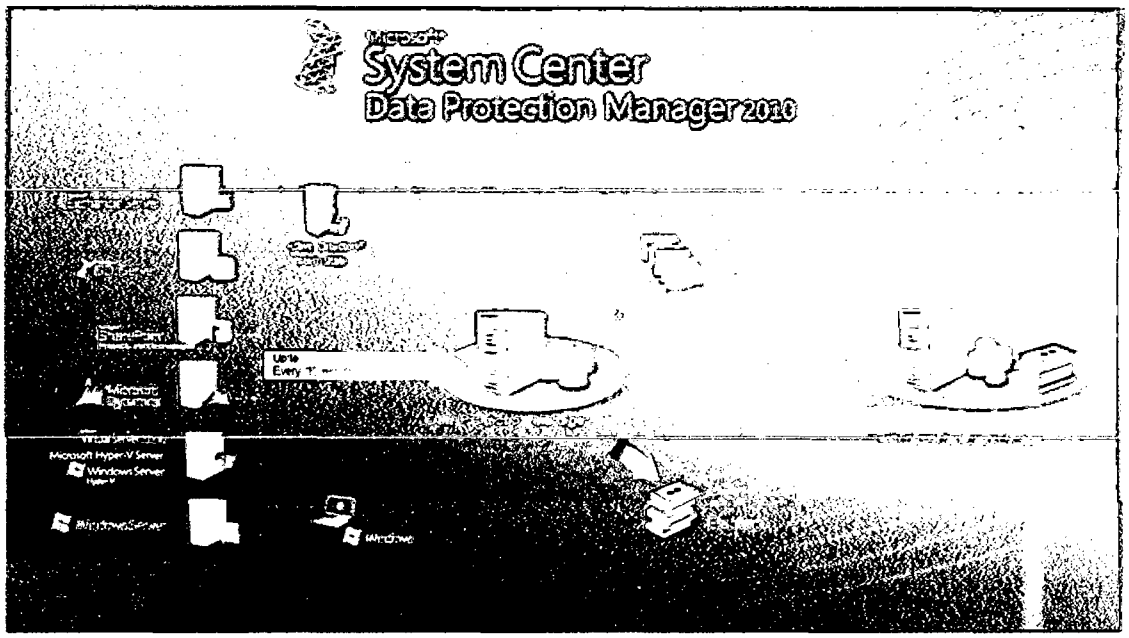


Gráfico N°24 System Center Data Protection Manager 2010.

3.9.5. 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
System Center Data Protection Manager	2006	2005
System Center Data Protection Manager	2007	2007
System Center Data Protection Manager	2010	2009
System Center Data Protection Manager	2012	2011

Tabla N°2 Evolución de System Center Data Protection Manager

MICROSOFT DMP 2006	MICROSOFT DMP 2007	MICROSOFT DMP 2010	MICROSOFT DMP 2012
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	SLA basado en alerta: Alerta cuando el SLA es violado.

		instantánea, y la conecta de nuevo.	
Protección para SIS habilitado en Servidores	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 especifico 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 N°3 Evolución de System Center Data Protection Manager al detalle

3.10 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.

3.10.1. 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.

3.10.2. Características de Amanda Source Backup.

- Amanda simplifica la vida de un administrador del sistema que puede 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.

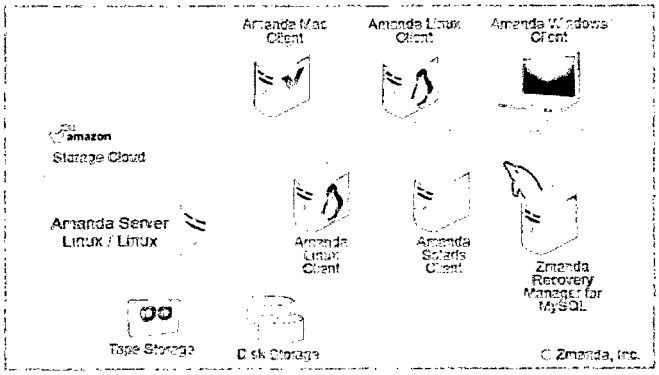


Gráfico N°25 Ambiente de Amanda

3.10.3. 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.

3.10.4. 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.

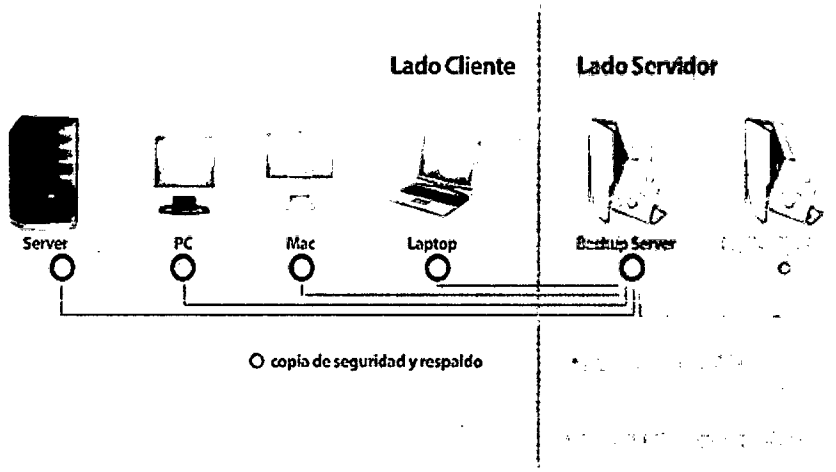


Gráfico N°26 Proceso de Respaldos

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.

3.10.5. 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**

Tabla N° 4 Evolución de Amanda Source Backup.

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 armazón 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.

3.11 OFICINA REGISTRAL.

La actividad del Sistema Nacional de los Registros Públicos, es brindar servicios de inscripción y publicidad registral a los usuarios, con el fin de otorgar la seguridad jurídica a las transacciones que realizan los ciudadanos. La Sunarp brinda sus servicios de Inscripción y Publicidad Registral, en los siguientes Registros: a. Registro de Personas Naturales, que comprende los siguientes registros: el Registro de Mandatos y Poderes, el Registro de Testamentos, el Registro de Sucesiones Intestadas, el Registro Personal, el Registro de Comerciantes, y el Registro de Gestión de Intereses. b. Registro de Personas Jurídicas, que comprende los siguientes registros: El Registro de Personas Jurídicas (incluyendo al registro de Asociaciones, Fundaciones, Comités, Cooperativas y de Personas Jurídicas creadas por Ley, así como cualquier Persona Jurídica distintas a las Sociedades y a las EIRL); el Registro de Sociedades Mercantiles, el Registro de Sociedades Mineras, el Registro de Sociedades del Registro Público de Hidrocarburos, el Registro de Sociedades Pesqueras y el Registro de Empresas Individuales de Responsabilidad Limitada. c. Registro de Propiedad Inmueble, que comprende los siguientes registros: el Registro de Predios, el Registro de Concesiones para la explotación de los Servicios Públicos, el Registro de Derechos Mineros, el Registro de Áreas Naturales Protegidas, y el Índice de Verificadores. d. El Registro de Bienes Muebles, que comprende los siguientes registros: el Registro de Propiedad Vehicular, el Registro de Naves, el Registro de Aeronaves (incluye Aeronaves y Motores de Aeronaves), el Registro de Embarcaciones Pesqueras, el Registro de Buques, el Registro Mobiliario de Contratos, el Registro de bienes vinculados a la actividad minera, y el Registro de Martilleros Públicos.

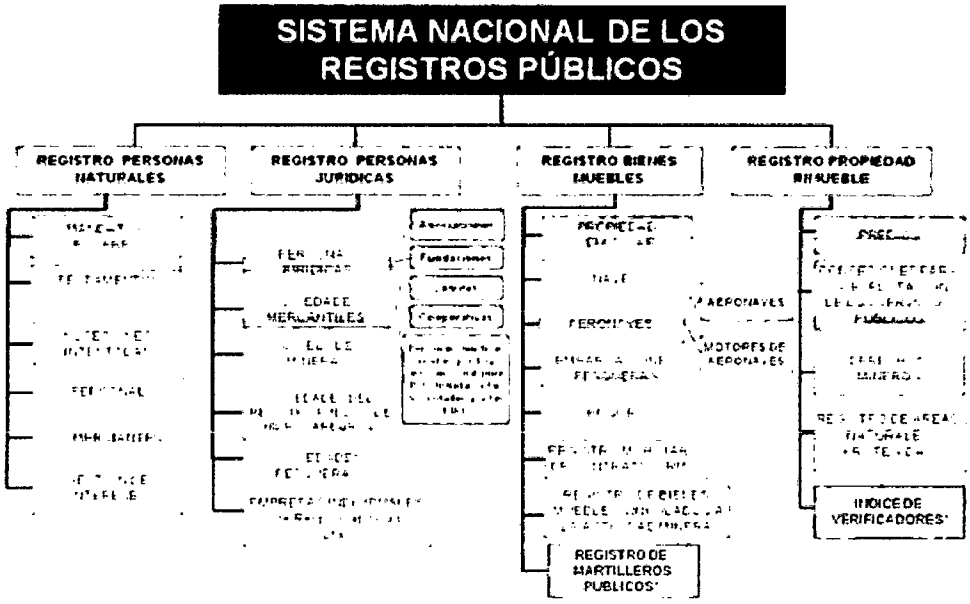


Gráfico N°27 Sistema Nacional de los Registros Públicos

Para desarrollar su labor de otorgar Seguridad Jurídica, el Sistema Nacional de los Registros Públicos está conformado por la Superintendencia Nacional de los Registros Públicos, como su ente rector normativo y supervisor, 64 Oficinas Registrales y 90 Oficinas Receptoras, que brindan los servicios registrales a la sociedad. Su distribución obedece a una zonificación registral, dentro de la que cada Oficina Registral tiene jurisdicción geográfica y los Registradores autonomía en su labor de servicio público.

3.12 ZONAS REGISTRALES

Las Zonas Registrales presentan las siguientes funciones generales:

a) Planificar, organizar, dirigir, ejecutar y controlar las actividades de carácter registral y catastral.

b) Planificar, organizar, dirigir, ejecutar y controlar las actividades de carácter administrativo, en coordinación con la Gerencia General.

c) Dirigir y ejecutar las acciones de gestión administrativa de las Oficinas Registrales correspondientes, de acuerdo con los lineamientos establecidos por la Alta Dirección.

d) Elaborar y mantener actualizada la estadística registral.

e) Celebrar convenios para el desarrollo de sus funciones con autorización de la Gerencia General.

f) Realizar la correcta ejecución de la función registral, acorde con la normatividad vigente; como la Inscripción previa calificación, los hechos, actos, contratos y resoluciones judiciales y/o administrativas que las normas legales determinan.

g) Impulsar el desarrollo tecnológico y la modernización de la gestión registral.

h) Elaborar su proyecto de presupuesto anual y remitirlo con la anticipación debida a la Gerencia General para su consolidación en el presupuesto general de la SUNARP.

i) Organizar y mantener actualizado el catastro de la Zona Registral, así como resguardar la información catastral, mediante los medios de seguridad existentes.

j) Nombrar a los Registradores Públicos de acuerdo a Ley.

k) Resolver en primera instancia los reclamos, denuncias y quejas que se presenten.

l) Coordinar con la Escuela de Capacitación, la ejecución de actividades de formación, capacitación y entrenamiento del personal de las Oficinas Registrales bajo su competencia.

m) Difundir, en coordinación con la Oficina de Imagen Institucional y Relaciones Públicas de la Sede Central, las actividades y eventos realizados por la Zona Registral que contribuyan a destacar la imagen de la Institución.

n) Brindar orientación a los usuarios en los trámites o procedimientos que éstos inicien ante las Oficinas Registrales.

o) Canalizar los reclamos que pudieran presentarse en la atención de los Servicios Registrales.

p) Informar permanentemente a la Gerencia General sobre su gestión administrativa y la productividad registral.

q) Expedir las resoluciones de su competencia.

r) Dar publicidad de los actos y contratos, conforme a las normas legales que la regulan.

s) Custodiar y otorgar seguridad al archivo registral de su competencia.

t) Promover, fomentar y realizar estudios e investigaciones en el área registral, que permitan generar nuevas técnicas registrales.

u) Elaborar y proponer a la Superintendencia Nacional de los Registros Públicos, los estudios técnicos para la creación de oficinas registrales dentro del ámbito de su jurisdicción.

v) Las demás funciones que le asigne la Superintendencia Nacional de los Registros Públicos.

CAPÍTULO IV

METODOLOGIA DE DESARROLLO DE LA IMPLENTACION

4.1 REQUERIMIENTOS

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 evaluar y 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.

Una vez analizadas las ventajas y desventajas de la herramienta seleccionada y de acuerdo a los requerimientos de la institución se obtuvo lo siguiente.

4.1.1 Requerimientos a nivel de Servidor.

Los prerrequisitos 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.

Requisitos Servidor	Linux	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
	Memoria	Al menos 2 GB. Un mínimo de 4 GB para servidores de producción con alta carga transaccional.
	Disco	Al menos 1 GB de almacenamiento de disco disponible para la instalación.
Requisitos Clientes	Linux & Windows	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
	Memoria	Al menos 2 GB.

Tabla N° 5 Requerimientos a nivel de Servidor - Amanda Source Backup.

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:

REQUISITOS SERVIDOR	AIX	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
	HP-UX	HP Itanium 11 iv2 (11.23.0505). HP Itanium 11 iv3 (11.31) HP Itanium 11 iV2
	WINDOWS	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
	SUN SOLARIS	Sun Solaris 10 x86/x86_64 Sun Solaris 10 SPARC
	LINUX	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.
	MEMORIA	Sistemas de 64 bits Windows (recomendado) 12 GB.

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

Tabla N° 6 Requerimientos a nivel de Servidor – Tivoli Storge Manager.

Requerimientos previos para la instalación de Microsoft System Data Protection *Manager 2012 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).

REQUISITOS SERVIDOR	WINDOWS	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
	MEMORIA	Al menos 4 GB, recomendado 8 GB
	DISCO	DPM directorio local: 3 GB. Base de Datos: 900 MB Controladores del Sistema: 1 GB
REQUISITOS CLIENTE	WINDOWS	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
	MEMORIA	Al menos 2 GB.
	DISCO	El cliente requiere 500 MB de espacio de disco libre

Tabla N° 7 Requerimientos a nivel de Servidor – System Data Protection Manager 2012.

4.1.2. Requerimientos a nivel de Respaldos.

AMANDA SOURCE BACKUP	TIVOLI STORAGE MANAGER	DATA PROTECTION MANAGER
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 puede instalar Amanda.	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 compresión a nivel de hardware.	Para uso de Medios Magnéticos como Cintas, nos proporciona un soporte de cintas LTO 4 – LTO5, con soporte para compresión por 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 FIBRA, 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 N° 8 Requerimientos a nivel de Respaldos.

4.1.3. Requerimientos a nivel de Conectividad.

AMANDA SOURCE BACKUP	TIVOLI STORAGE MANAGER	DATA PROTECTION MANAGER
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	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.

transmite los datos copiados al servidor.		
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 N° 9 Requerimientos a nivel de Conectividad.

4.2 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.

4.2.1. Manejo de Políticas de Respaldo.

Descripción	AMANDA SOURCE BACKUP	TIVOLI STORAGE MANAGER	DATA PROTECTION MANAGER
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 Versionamiento de archivos respaldados.	Las versiones de 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	El Versionamiento lo especifica el administrador del sistema y puede ir desde una versión hasta un número ilimitado de versiones.	Las versiones las 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	De igual manera está definida por el tiempo de ejecución	Definida por el Administrador del Sistema y utiliza	Maneja copias denominadas de corta duración así como de

archivados de información de los clientes.	de la copia completa de cada cliente.	conceptos de la herramienta que son copias activas e inactivas.	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 respaldos 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 servidor de Amanda.	Utiliza lo que se define como dispositivos de almacenamiento y agrupaciones de almacenamiento, para especificar tamaños y formas de almacenamiento.	Utiliza una o más particiones o unidades de cinta atachadas al servidor, en el caso de particiones de disco se agrega completamente el 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 N° 10 Manejo de Políticas de Respaldo.

4.2.2. *Modelo de Respaldos Utilizado.*

Las tres herramientas aplican el mismo esquema de respaldos el mismo que eestá basado en el modelo denominado —Abuelo, Padre, Hijol 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.

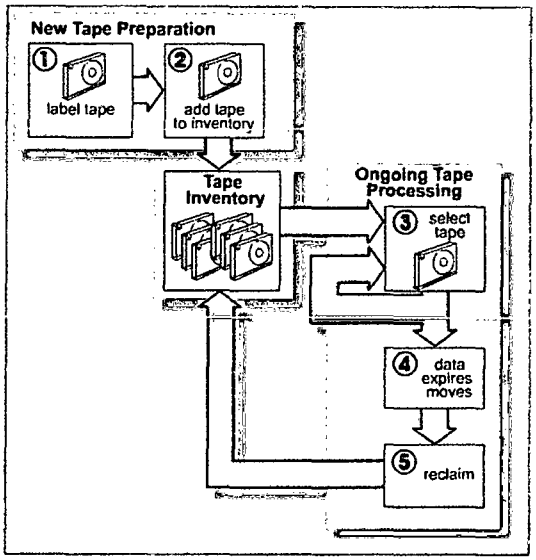


Grafico N° 28 Modelo de Respaldos Utilizado

4.2.3. 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 simple, solo por días transcurridos.	Calendarización simple, solo por días transcurridos.
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 N° 11 Flexibilidad de Configuración.

4.2.4. 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
```

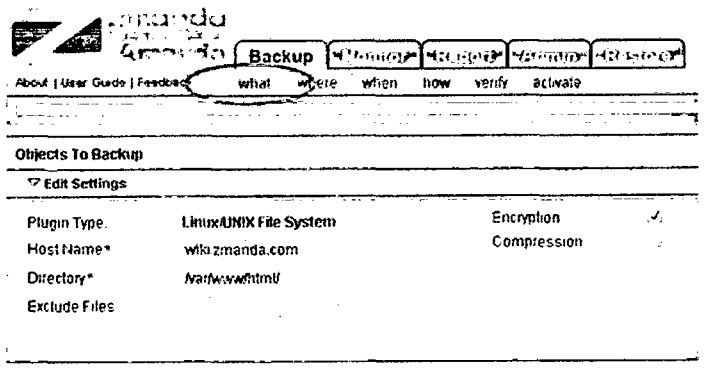
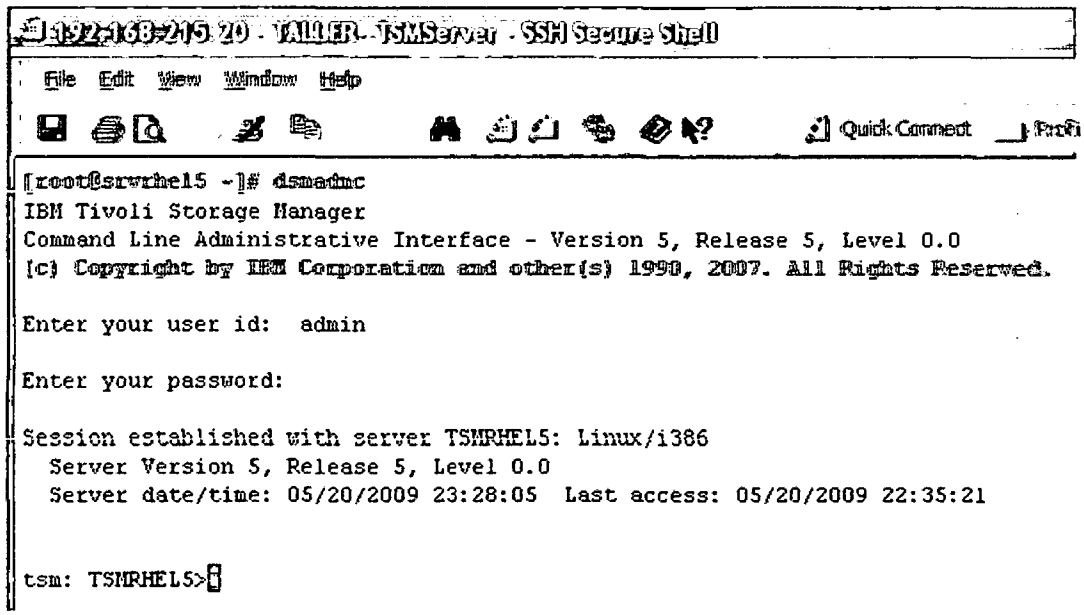
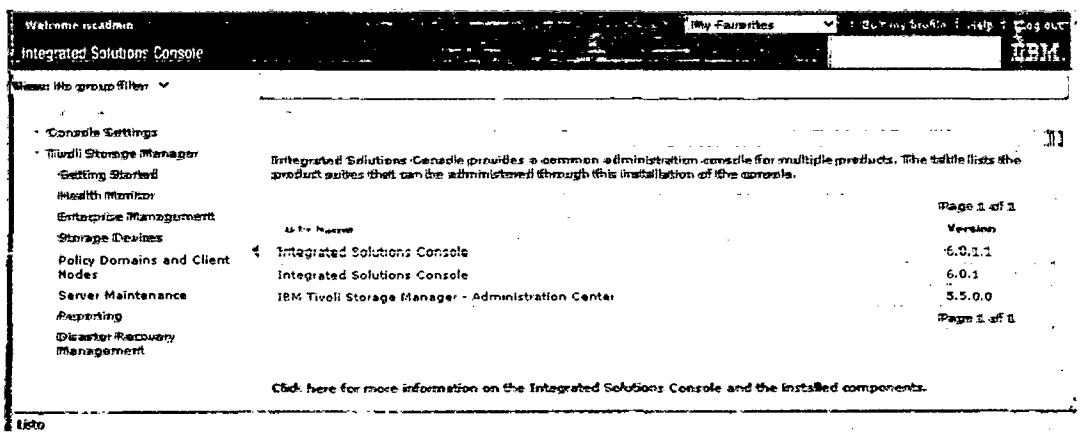


Grafico N° 29 Métodos de Administración: Amanda Source Backup.

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.





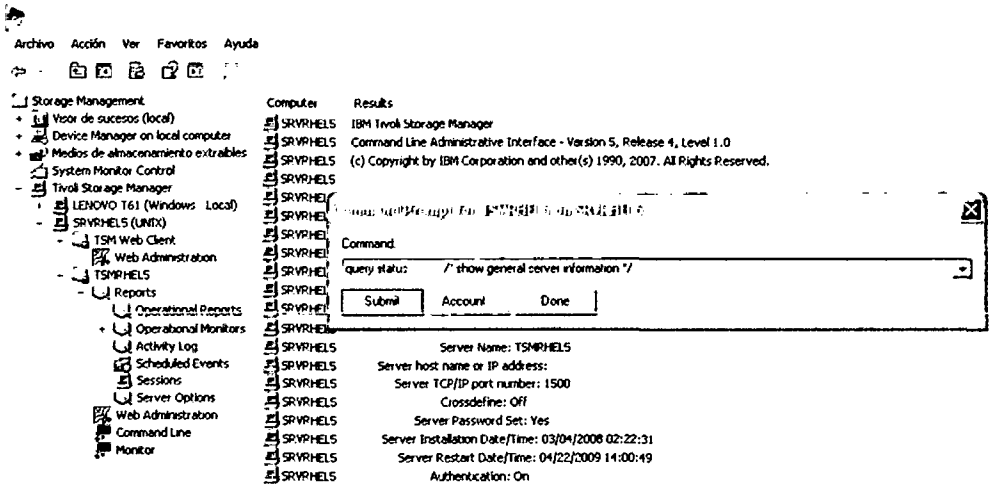


Grafico N° 30 Métodos de Administración: Tivoli Storage Manager

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.

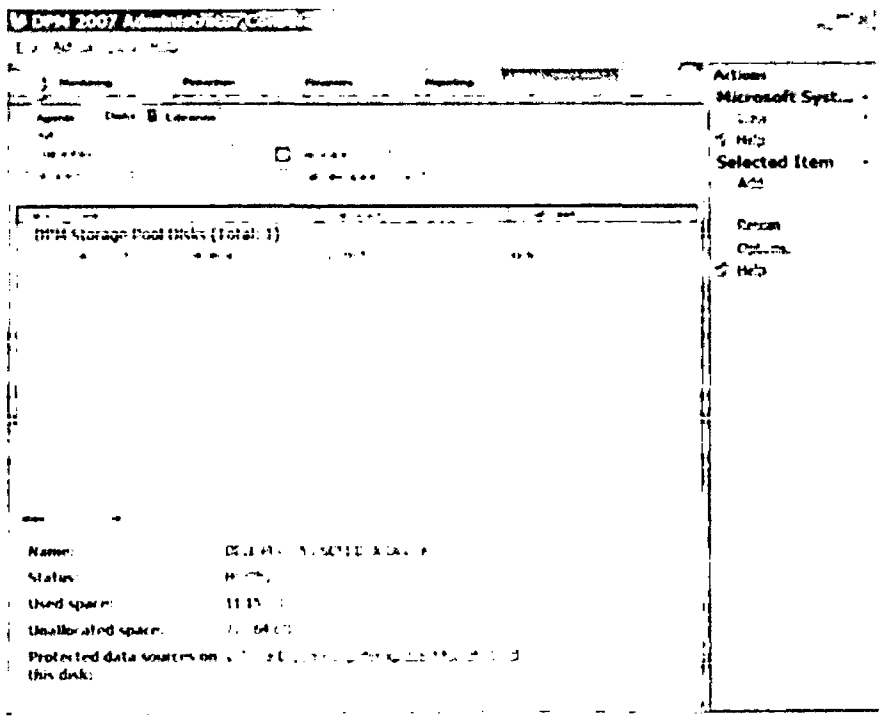


Grafico N° 31 Métodos de Administración: Data Protection Manager

4.3. COMPARATIVAS DE LAS HERRAMIENTAS

4.3.1. Principales diferencias y similitudes.

Característica	AMANDA SOURCE BACKUP	TIVOLI STORAGE MANAGER	DATA PROTECTION MANAGER
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.
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.
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.
***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.
Respaldos —ON-LINE soportados.	Soporte solo para MYSQL.	Soporta múltiples bases de datos, correos y sistemas operativos.	Soporta aplicaciones solo en Windows y como fabricante *Microsoft.*
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.
Deduplicación.	No soporta de-duplicación.	Soporte total para de-duplicación.	No soporta de-duplicación.
Soporte Técnico	Soporte técnico inexistente, se puede utilizar blogs, Wikipedia para solventar	Soporte especializado con un costo adicional, de parte del fabricante, por un canal asociado	Soporte especializado con costo adicional directamente con el fabricante, Wikipedia

	dudas o configuraciones existentes.	o por descarga de "RedBooks".	y blogs de información.
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.
Instalación y Configuración.	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.

Tabla N° 12 Principales diferencias y similitudes.

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 encripción 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 comprensión 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.

4.4. ELECCION DE LA HERRAMIENTA

Requisitos del Negocio	Amanda Source Backup	Tivoli Storage Manager	Data Protection Manager
Respaldos de Base de Datos Oracle 10i	X	X	
Calendarización para Respaldos Automáticos por Fecha		X	X
Calendarización para Respaldos Automáticos por Días	X	X	X
Calendarización para Respaldos Automáticos por Semanas Calendarizadas para Respaldos.		X	X
Calendarización para Respaldos Automáticos por Mes Calendarizadas para Respaldos.		X	X
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	**60%**	**100%**	**90%**

Tabla N° 13 Eleccion de la Herramienta.

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

4.5 BASE LEGAL

La Oficina General de Tecnologías de la Información conjuntamente con la Empresa Systems Support & Services a través de Gerencia de Proyectos presenta a la ZONA REGISTRAL N° VII la documentación correspondiente a la Implantación de Tivoli Storage Manager 6.3.4, desplegada como parte de la "Adquisición de un Servidor para la Oficina de Casma dela Zona Registral N° VII – Sede Huaraz, según Adjudicación Directa Selectiva No0004-2013 .R.NoVII/CE.

4.6 DESCRIPCIÓN DE TSM

Tivoli Storage Manager (TSM) es un producto de software IBM que permite realizar respaldos de información de manera periódica y automática. Provee además procedimientos de administración; así como mecanismos probados de restauración de la información en caso de desastres o requerimiento de información histórica.

La solución de respaldo implementada cuenta con los siguientes componentes:

- Un servidor de respaldo, que comprende los programas administrativa interfaz gráfica y una base de datos DB2.
- Una librería de respaldos marca IBM, modelo TS3100.
- Consola de monitoreo Operation Center.
- Clientes TSM, los que se instalan en cada servidor a respaldar y se encargan de lo siguiente:
    - Contactar al servidor TSM periódicamente y obtener del servidor TSM la fecha y horario del respaldo más próximo.
    - Ejecutar los respaldos de archivos conforme a la planificación.
    - Ejecutar el respaldo de virtuales.
- Agentes especializados para el respaldo de bases de datos y máquinas virtuales en caliente.

4.7 DESCRIPCION DE LA IMPLEMENTACION

El servidor TSM instalado es de la versión 6.3.4 y se implementó sobre un servidor físico con las siguientes características:

Nombre de host:	TSMSERVER
Nombre del sistema operativo:	Microsoft Windows Server 2008 R2
Fabricante del sistema operativo:	Microsoft Corporation
Configuración del sistema operativo:	Servidor miembro
Tipo de compilación del sistema operativo:	Multiprocessor Free
Propiedad de:	Usuario de Windows
Organización registrada:	IBM
Fabricante del sistema:	x64-based PC
Tipo de sistema:	C:\Windows
Directorio de sistema:	C:\Windows\system32
Dispositivo de arranque:	\Device\HarddiskVolume1
Configuración regional del sistema:	es-pe;Español (Perú)
Idioma de entrada:	N/D
Zona horaria:	(UTC-05:00) Bogotá, Lima, Quito
Cantidad total de memoria física:	

Ubicación(es) de archivo de paginación:	C:\pagefile.sys
Servidor de inicio de sesión:	\\TSMSERVER
Revisión(es):	2 revisión(es) instaladas. [01]: KB958488 [02]: KB976902

Tabla N° 14 Descripción de la Implementación.

4.7.1 Librería Robótica

La librería robótica es marca IBM, modelo TS2900 y cuenta con 1 drive LTO5.

La librería cuenta con 09 slots disponibles.

4.7.2 Consola de Monitoreo Operation Center

IBM TSM Operation Center es una consola grafica que permite lo siguiente:

- Gestionar la infraestructura de Respaldos
- Resolver problemas de respaldos
- Apoyar al equipo de administradores

El acceso a la consola es mediante el siguiente enlace:

http://TSMSERVER:11080/oc

Una vez abierto el enlace indicado aparecerá la siguiente interfaz:

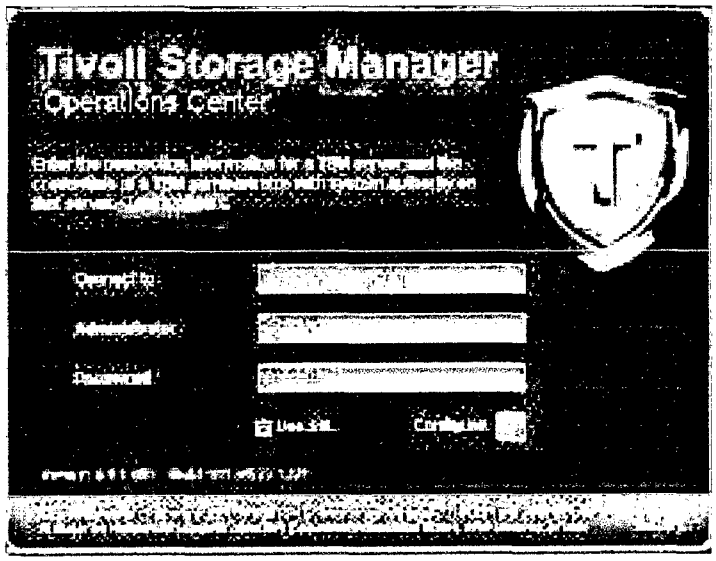


Grafico N° 32 Consola de Monitoreo Operation Center

Ingresar con las siguientes credenciales:

Administrator : ocadmin

Password : ocadmin

El siguiente enlace lleva a una demostración del producto:

http://ibmtvdemo.edgesuite.net/software/tivoli/demos/TSM_Ops_CenterFirst_Look/demo.html

4.7.3 Descripción de la Configuración

La implantación realizada se hizo conforme a la siguiente configuración:

4.7.3.1 Clientes de Respaldo

Los servidores a respaldar son los clientes de la solución de respaldo. Cada servidor a respaldar es representado en el servidor TSM por un nodo.

Un nodo es un elemento de TSM con un conjunto de características que lo identifican con el servidor al que representa. La data respaldada pertenece al nodo. Si borramos el nodo estamos eliminando los respaldos asociados a ese nodo. De igual forma los respaldos se programan para que sean ejecutados en nodos específicos.

En la implantación realizada, cada servidor está representado al menos por 2 nodos debido a que uno de ellos se utiliza solo programar los respaldos y se encarga de identificar los respaldos programados para cada servidor. Otro nodo se encarga de respaldar los datos a nivel de archivos.

Se establece el siguiente esquema de nombres:

Nombre Servidor	***Nombre Nodo***	***Descripción***
hostname	hostname	Nodo para programación de respaldos
hostname	hostname_bac	Nodo para respaldo de archivos
hostname	hostname_ora	Nodo para respaldo de Oracle

Tabla N° 15 Clientes de Respaldo

Por ejemplo, un servidor llamado server1, tendra 2 nodos:

server1, que será el nodo para programar los respaldos.

server1_bac, que será el nodo para respaldar los archivos del servidor.

Siguiendo con el mismo ejemplo, si en el mismo servidor hay una base de datos MS SQL, deberá contar con un tercer nodo llamado:

server1_sql para respaldar dicha base de datos.

4.7.3.2 Dominios

Conforme se indica en el acápite previo todo servidor a respaldar debe ser representado por un nodo. De igual forma, todo nodo que se registre

en el servidor TSM debe pertenecer a un dominio. Los dominios de TSM son agrupaciones de nodos que se rigen por una misma política.
La política determina hacia dónde van los respaldos (a disco, a cinta, a que cintas, etc.) y por cuánto tiempo se va a retener dicha información.

Nombre	***Descripción***
dom_files	Dominio para respaldar archivos a nivel de file system
dom_ora	Dominio para respaldar información de base de datos Oracle.
dom_sched	Dominio para programación de respaldos

Tabla N° 16 Dominios

En este sentido, se han creado los siguientes dominios:

4.7.3.3 Almacenamiento

El almacenamiento se refiere a los medios físicos para almacenar los respaldos de información.
En principio, un sistema de respaldo de información está preparado para respaldar a cinta, pero también es útil respaldar a disco debido a que ofrece una mayor velocidad, tanto respaldos como restauraciones. En este sentido, la configuración realizada está preparada para que los respaldos sean grabados primero en disco (del servidor TSM) y luego progresivamente vayan migrando a cinta.
La migración de disco a cinta es automática cuando el espacio utilizado del disco llega a cierto porcentaje definido por configuración y culmina cuando llega a cero. También se han programado tareas periódicas para migrar. En este caso el inicio del proceso de migración es de acuerdo al horario definido y no por el porcentaje de uso.
Los respaldos en disco se organizan físicamente en archivos de un tamaño definido por configuración. Cuando el archivo se llena, el sistema crea otro. Estos archivos son representados en el sistema con el nombre de volúmenes.

Los volúmenes se agrupan en Storage Pools y las políticas de dominio definen el Storage Pool a utilizar para todos los miembros del dominio.
Cuando los respaldos en disco migran a cinta, los archivos/volúmenes donde se almacenaban los datos migrados son eliminados, liberando espacio en el disco.

De igual forma, las cintas se representan como volúmenes en el sistema. Cada cinta pertenece a un Storage Pool de cintas. Cuando se produce una migración de disco a cinta, el sistema la información en una de las cintas disponibles. Al llenarse, coge una nueva cinta en blanco de las cintas disponibles en la librería.

El siguiente cuadro describe los Storage Pools creados y su asignación a dominios:

Dominio	***Storage Pool de Disco***	***Migra al Storage***	***Descripción***
dom_files	bkpdskfil_d	bkpltofil_d	Para respaldos diarios de archivos
dom_files	bkpdskfil_s	bkpltofil_s	Para respaldos semanales de archivos
dom_files	arcdskfil_m	arcltofil_m	Para archivados mensuales de archivos
dom_files	--	cpyltofil_s	Copia del respaldo semanal de archivos
dom_ora	bkpdskora_d	bkpltoora_d	Para respaldos diarios de Oracle
dom_ora	bkpdskora_s	bkpltoora_s	Para respaldos semanales de Oracle
dom_ora	arcdskfil_m	arcltofil_m	Para archivados mensuales de Oracle (como archivos)
dom_ora	--	cpyltoora_s	Copia del respaldo semanal de Oracle

Tabla N° 17 Almacenamiento

4.7.3.4 Tipos de Respaldo

Los respaldos de información pueden ser del tipo "backup" o del tipo "archive".

En el caso de los "backups", estos respaldos pueden ser completos (full) o incrementales. Un "backup full" respalda todos los archivos, mientras los incrementales solo respaldan los archivos que variaron o se agregaron después del último respaldo realizado. Por este motivo, los respaldos incrementales siempre están asociados al "full" más cercano y los incrementales sucesivos, hasta que se realice un nuevo "full".

Las políticas de retención para "backups" se configuran indicando el número de respaldos de una misma data (versiones) que el sistema va a retener y/o la antigüedad máxima de dichos respaldos.

Cuando llega al número máximo de versiones, la más antigua expira. Si un respaldo ha cumplido el tiempo máximo de retención también expira. Lo primero que suceda.

El otro tipo de respaldo es el "archive". Se parece al "full" en el sentido que respalda todos los archivos seleccionados, pero en este tipo de respaldo no hay incrementales. Por otro lado, los "archives" tienen sus propias políticas expresadas únicamente en número de días de retención y no en el número de versiones.

Los respaldos que atienden desastres y/o pérdidas de información son del tipo "backup". Se está empleando esta modalidad para los respaldos diarios y semanales.

Se definieron las siguientes frecuencias y tipos de respaldo a utilizar:

Frecuencia	**Tipo de Respaldo**
Diaria	Backup Incremental
Semanal	Backup Full
Mensual de Archivos	Archive
Mensual de Aplicaciones	Archive

Tabla N° 18 Tipos de respaldo

4.7.3.5 Políticas de Retención

Las políticas de retención permiten determinar por cuánto tiempo se va a retener en cinta un respaldo realizado. La retención también se puede expresar en número de versiones.

La implantación realizada en Sunarp Huaraz - Casma permite restaurar información ante un desastre (información "viva"), pero también permite recuperar datos históricos. Ambas situaciones, aunque similares difieren principalmente en la antigüedad de los datos; ello implica otra forma de respaldo, otros tiempos de retención y, finalmente, otro procedimiento de restauración. En este sentido, hay politicas de retención para restaurar información "viva" y otras politicas para información "histórica".

Cuando se trata de la pérdida de información vigente estamos hablando de información en producción, con una antigüedad máxima de 15 días (para el caso de Sunarp Huaraz - Casma), aunque este límite depende del requerimiento de cada organización o incluso del tipo de información.

Para simplificar el esquema de respaldos hemos definido que los respaldos se van regir únicamente por el tiempo de retención y no por el número de versiones que sera establecido como "nolimit" (sin límite).

Se establecieron los siguientes tiempos de retención para respaldos (backup full e incremental):

Dominio	Frecuencia	Versiones retenidas cuando el archivo existe	Versiones retenidas cuando el archivo fue eliminado	Días de retención de las versiones inactivas	Días de retención para la última versión retenida
dom_files	diaria	nolimit	2	15	30
dom_files	semanal	nolimit	2	15	30
dom_ora	diaria	1	0	7	7
dom_ora	semanal	1	0	7	7

Tabla N° 19 Políticas de Retención

Se establecieron los siguientes tiempos de retención para archivados (archives):

Dominio	Frecuencia	Días de retención
dom_files	mensual	365
dom_ora	mensual	365

Tabla N° 20 Tiempo de Retención

4.7.3.6 Programación de Respaldos

La programación de respaldos diarios y semanales se corresponde con el siguiente cuadro:

Domingo	*Lunes*	*Martes*	*Miércoles*	*Jueves*	*Viernes*
Semanal (Bkp full)	Diario (Bkp incr)	Diario (Bkp incr)	Diario (Bkp incr)	Diario (Bkp incr)	Diario (Bkp incr)

Tabla N° 21 Programación de respaldos diarios y semanales

La programación de los respaldos mensuales es la siguiente:

Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
1er Sab	1er Sab	1er Sab	1er Sab	1er Sab	1er Sab	1er Sab	1er Sab	1er Sab	1er Sab	1er Sab	1er Sab

Tabla N° 22 Programación de respaldos mensuales

4.7.3.7 Tareas Administrativas

La implantación comprende un conjunto de tareas administrativas que se realizan en forma automática conforme a una programación.

Se crearon las siguientes tareas administrativas:

Nombre	*Descripción*
bkp_dbtape	Backup de la base de datos TSM a cinta
rec_stgpoold	Reclamación de las cintas del respaldo diario
rec_stgpools	Reclamación de las cintas del respaldo semanal
rec_stgpoolm	Reclamación de las cintas del respaldo mensual, virtuales e histórico
exp_inventory	Expiración del inventario de respaldos conforme a los tiempos de retención
mig_stgpoold	Migración de los Storage Pools diarios
mig_stgpools	Migración de los Storage Pools semanales
mig_stgpoolm	Migración de los Storage Pools mensuales, virtuales e históricos
def_mcdiario	Asigna como default la Management Class de los respaldos diarios en los dominios dom_files y dom_ora
def_mcsemanal	Asigna como default la Management Class de los respaldos semanales en los dominios dom_files y dom_ora

Tabla N° 23 Tareas Administrativas

Se definieron los siguientes horarios y frecuencias de respaldo:

Tarea Administrativa	*Frecuencia*	*Horario*
bkp_dbtape	Lunes - Domingo	12:00
rec_stgpoold	Martes - Viernes	13:00
rec_stgpools	Lunes de la sem. 2,3,4 y 5	13:00
rec_stgpoolm	Lunes de la sem. 1	13:00
exp_inventory	Lunes - Domingo	09:00
mig_stgpoold	Martes - Viernes	09:00
mig_stgpools	Lunes de la sem. 2,3,4 y 5	09:00
mig_stgpoolm	Lunes de la sem. 1	09:00
def_mcdiario	Domingo	23:50
def_mcsemanal	Viernes	23:50

Tabla N° 24 Horarios y frecuencias de respaldo

4.7.4 Procedimientos y Comandos de Configuración

La implantación consta de los siguientes pasos en lo que se refiere a configuración del software:

4.7.4.1 Configuración de Librería y Drives

Se creó la librería de respaldos y su "path" correspondiente, así como drives y paths:

```
define library lib01 libtype=scsi shared=yes resetdrives=yes autolabel=yes
define path server1 lib01 srctype=server desttype=library device=lb2.1.0.1

define drive lib01 drv01 serial=autodetect online=yes
define path server1 drv01 srctype=server desttype=drive library=lib01 device=mt2.0.0.0
```

4.7.4.2 Configuración de Device Classes

Se creó el Device Class para respaldo de clientes a cinta:

```
define devclass lto5dev devtype=lto library=lib01 format=drive mountlimit=drives
```

Se creó el Device Class para respaldos de clientes a disco:

```
define devclass dskdev devtype=file mountlimit=12 maxcapacity=10G \ directory=G:\dskbkp
shared=no
```

Se creó el Device Class de disco para respaldo de la base de datos TSM:

```
define devclass dbback devtype=file mountlimit=4 maxcapacity=10G \ directory=G:\dbback
shared=yes
```

4.7.4.3 Configuración de Storage Pools

a. Respaldos Diarios

Se creó Storage Pool BKPLTOFIL_D para respaldos diarios a cinta de servidores de archivos:

```
define stgpool bkpltofil_d lto5dev pooltype=primary maxscratch=1000 colloc=no rec=100
```

Se creó Storage Pool BKPLTOORA_D para respaldos diarios a cinta de servidores Oracle:

```
define stgpool bkpltoora_d lto5dev pooltype=primary maxscratch=1000 colloc=no rec=100
```

Nota:

Los Storage Pool de cinta reciben la migración de datos de sus pares en disco.

Se creó Storage Pool BKPDSKFIL_D para respaldos diarios a disco de servidores "críticos":

```
define stgpool bkpdskfil_d dskdev pooltype=primary maxscratch=1000 colloc=no
nextstgpool=bkpltofil_d lowmig=0 highmig=20
```

Se creó Storage Pool BKPDSKORA_D para respaldos diarios a disco de servidores "no críticos":

```
define stgpool bkpdskora_d dskdev pooltype=primary maxscratch=1000 colloc=no
nextstgpool=bkpltoora_d lowmig=0 highmig=20
```

b. Respaldos Semanales

Se creó Storage Pool bkpltofil_s para respaldos semanales a cinta de servidores de archivos:

```
define stgpool bkpltofil_s lto5dev pooltype=primary maxscratch=1000 colloc=no rec=100
```

Se creó Storage Pool bkpltoora_s para respaldos semanales a cinta de servidores Oracle:

```
define stgpool bkpltoora_s lto5dev pooltype=primary maxscratch=1000 colloc=no rec=100
```

Nota:

Los Storage Pool de cinta reciben la migración de datos de sus pares en disco.

Se creó Storage Pool bkpdskfil_s para respaldos semanales a disco de servidores de archivos:

```
define stgpool bkpdskfil_s dskdev pooltype=primary maxscratch=1000 colloc=no
nextstgpool=bkpltofil_s lowmig=0 highmig=20
```

Se creó Storage Pool BKPDSKORA_S para respaldos semanales a disco de servidores Oracle:

```
define stgpool bkpdskora_s dskdev pooltype=primary maxscratch=1000 colloc=no
nextstgpool=bkpltoora_s lowmig=0 highmig=20
```

c. Respaldos Mensuales

Se creó Storage Pool ARCLTOFIL_M para respaldos mensuales de archivos a cinta:

```
define stgpool arcltofil_m lto5dev pooltype=primary maxscratch=1000 colloc=no rec=100
```

Se creó Storage Pool ARCLTOORA_M para respaldos mensuales de Oracle a cinta:

```
define stgpool arcltoora_m lto5dev pooltype=primary maxscratch=1000 colloc=no rec=100
```

Nota:

Los Storage Pool de cinta reciben la migración de datos de sus pares en disco.

Se creó Storage Pool bkpdskfil_s para respaldos semanales a disco de servidores de archivos:

```
define stgpool bkpdskfil_s dskdev pooltype=primary maxscratch=1000 colloc=no
nextstgpool=bkpltofil_s lowmig=0 highmig=20
```

Se creó Storage Pool BKPDSKORA_S para respaldos semanales a disco de servidores Oracle:

```
define stgpool bkpdskora_s dskdev pooltype=primary maxscratch=1000 colloc=no
nextstgpool=bkpltoora_s lowmig=0 highmig=20
```

d. Copia de los Respaldos Semanales

Se creó Storage Pool CPYLTOFIL_S para respaldo de Storage Pool Semanal BKPLTOFIL_S:

```
define stgpool bkpltofil_s lto5dev pooltype=copy maxscratch=1000 colloc=no rec=100
```

Se creó Storage Pool CPYLTOORA_S para respaldo de Storage Pool Semanal BKPLTOORA_S:

```
define stgpool cpyltoora_s lto5dev pooltype=copy maxscratch=1000 colloc=no rec=100
```

4.7.4.4 Configuración de Dominios

Se crearon los siguientes dominios:

a. Dominio de Servidores de Archivos

Se creó el dominio DOM_FILES para servidores de archivos:

```
define domain dom_files desc="Dominio Servidores de Archivos"
```

Se creó la política POL1 para el dominio DOM_FILES:

```
define policyset dom_files pol1
```

Se creó la management class DIA para la política POL1:

```
define mgmtclass dom_files pol1
```

Se creó el copygroup STANDARD para la management class DIA, tanto para backups como archives. Aquí se consigna tiempo de retención de 15 días para los respaldos diarios y 1 año para los archives mensuales. También se define BKPDSKFIL_D como Storage Pool de destino de

backups diarios y ARCDSKFIL_M como Storage Pool de destino de archives (mensuales):

```
define copygroup dom_files pol1 dia standard type=backup destination=bkpdskfil_d
verexists=nolimit verdeleted=2 retextra=15 retonly=30
define copygroup dom_files pol1 dia standard type=archive destination=arcdskfil_m retver=365
```

Se creó la management class SEM para la política POL1:

```
define mgmtclass dom_files pol1 sem
```

Se creó el copygroup STANDARD para la management class SEM, tanto para backups como archives. Aquí se consigna tiempo de retención de 15 días para los respaldos semanales y 1 año para los archives mensuales. También se define BKPDSKFIL_S como Storage Pool de destino de backups semanales y ARCDSKFIL_M como Storage Pool de destino de archives (mensuales):

```
define copygroup dom_files pol1 sem standard type=backup destination=bkpdskfil_s
verexists=nolimit verdeleted=2 retextra=15 retonly=30
define copygroup dom_files pol1 sem standard type=archive destination=arcdskfil_m retver=365
```

Se definió DIA como management class por defecto:

```
assign defmgmtclass dom_files pol1 dia
```

Se validó y activo la política POL1:

```
validate policyset dom_files pol1
activate policyset dom_files pol1
```

b. Dominio De Servidores Oracle

Se creó el dominio DOM_ORA para servidores Oracle:

```
define domain dom_ora desc="Dominio Servidores Oracle"
```

Se creó la politica POL1 para el dominio DOM_ORA:

```
define policyset dom_ora pol1
```

Se creó la management class DIA para la política POL1:

```
define mgmtclass dom_ora pol1 dia
```

Se creó el copygroup STANDARD para la management class DIA, tanto para backups como archives. Aqui se consigna tiempo de retencion de 7 días para los respaldos diarios y 1 año para los archives mensuales. Tambien se define BKPDSKORA_D como Storage Pool de destino de backups diarios y ARCDSKORA_M como Storage Pool de destino de archives (mensuales):

```
define copygroup dom_ora pol1 dia standard type=backup destination=bkpdskora_d
verexists=nolimit verdeleted=2 retextra=15 retonly=30
define copygroup dom_ora pol1 dia standard type=archive destination=arcdskora_m retver=365
```

Se creó la management class SEM para la política POL1: .

```
define mgmtclass dom_ora pol1 sem
```

Se creó el copygroup STANDARD para la management class SEM, tanto para backups como archives. Aquí se consigna tiempo de retención de 15 días para los respaldos semanales y 1 año para los archives mensuales. También se define BKPDSKORA_S como Storage Pool de destino de backups semanales y ARCDSKORA_M como Storage Pool de destino de archives (mensuales):

```
define copygroup dom_ora pol1 sem standard type=backup destination=bkpdskora_s
verexists=nolimit verdeleted=2 retextra=15 retonly=30
define copygroup dom_ora pol1 sem standard type=archive destination=arcdskora_m retver=365
```

Se definió DIA como management class por defecto:

```
assign defmgmtclass dom_ora pol1 dia
```

Se validó y activo la política POL1:

```
validate policyset dom_ora pol1
activate policyset dom_ora pol1
```

4.7.4.5 Programación de Respaldos

a. Respaldos Diarios

Nombre	Frecuencia	Horario	Acción
bkp_win_dia_bac	L-V	22:00	c:\tsmscripts\bkp_diario_bac.cmd

Descripción:
Respaldo diario de archivos en servidores Windows
Nodos asociados: --

Comandos:
define schedule dom_sched bkp_win_dia_bac \
desc='Diario Archivos - Windows' \
action=command obj='c:\tsmscripts\bkp_diario_bac.cmd' \
schedstyle=classic \
starttime=22:00 dayofweek=weekday
define association dom_sched bkp_win_dia_bac

Nombre	Frecuencia	Horario	Acción
bkp_win_dia_ora	L-V	03:00	c:\tsmscripts\bkp_diario_ora.cmd

Descripción:
Respaldo diario de base de datos Oracle en servidores Windows
Nodos asociados: --

Comandos:
define schedule dom_sched bkp_win_dia_ora \
desc='Diario Oracle - Windows' \
action=command obj='c:\tsmscripts\bkp_diario_ora.cmd' \
schedstyle=classic \
starttime=03:00 dayofweek=weekday
define association dom_sched bkp_lnx_dia_ora

b. Respaldos Semanales

Nombre	Frecuencia	Horario	Acción
bkp_win_sem_bac	Domingo	00:00	c:\tsmscripts\bkp_semanal_bac.cmd

Descripción:
Respaldo semanal de archivos en servidores Windows
Nodos asociados: --

Comandos:
def sched dom_sched bkp_win_sem_bac \
desc='Semanal Archivos - Windows' \
action=command obj='c:\tsmscripts\bkp_semanal_bac.cmd' \
schedstyle=classic \
starttime=00:00 dayofweek=sun
define association dom_sched bkp_win_sem_bac

Nombre	Frecuencia	Horario	Acción
bkp_win_sem_ora	L-V	07:00	c:\tsmscripts\bkp_semanal_ora.cmd

Descripción:
Respaldo semanal de base de datos Oracle en servidores Windows
Nodos asociados:
--

Comandos:
```
def sched dom_sched bkp_win_sem_ora \
desc='Semanal Oracle - Windows' \
action=command obj='c:\tsmscripts\bkp_semanal_ora.cmd' \
schedstyle=classic \
starttime=07:00 dayofweek=sun
define association dom_sched bkp_win_sem_ora
```

c. Respaldos Mensuales

Nombre	Frecuencia	Horario	Acción
bkp_win_men_bac	1er Sábado c/mes	00:00	c:\tsmscripts\bkp_mensual_bac.cmd

Descripción:
Respaldo mensual de archivos en servidores Windows
Nodos asociados:
srvdomain

Comandos:
```
define schedule dom_sched bkp_win_men_bac \
desc='Mensual Archivos - Windows' \
action=command obj='c:\tsmscripts\bkp_mensual_bac.cmd' \
schedstyle=enhanced \
starttime=00:00 weekofmonth=first dayofweek=sat

define association dom_sched bkp_win_men_bac srvdomain
```

Nombre	Frecuencia	Horario	Acción
bkp_lnx_men_ora	1er Sábado c/mes	00:00	c:\tsmscripts\bkp_mensual_ora.cmd

Descripción:
Respaldo mensual de base de datos Oracle en servidores Windows
Nodos asociados:
--

Comandos:

```
define schedule dom_sched bkp_win_men_ora \
desc='Mensual Oracle - Windows' \
action=command obj='c:\tsmscripts\bkp_mensual_ora.cmd' \
schedstyle=enhanced \
starttime=07:00 weekofmonth=first dayofweek=sat

define association dom_sched bkp_lnx_men_ora
```

4.7.4.7 Configuración de scripts

Se crearon los siguientes scripts:

a. Respaldo de la Base de Datos TSM

Nombre	Descripción
backupdbt	Este script permite hacer un respaldo de la base de datos TSM a cinta y de los archivos necesarios para una recuperación de desastre en el servidor TSM a disco

```
def script bkp_dbtape "backup db devclass=lto5dev
type=dbsnapshot wait=yes"
upd script bkp_dbtape "delete volhistory type=dbsnapshot
todate=today-2 wait=yes"
upd script bkp_dbtape "backup volhistory
filename=g:\dbback\volhist.out"
upd script bkp_dbtape "backup devconfig
filename=g:\dbback\devcnfg.out"
```

Nombre	Descripción
backupdbd	Este script permite hacer un respaldo de la base de datos TSM a disco y de los archivos necesarios para una recuperación de desastre en el servidor TSM a disco

```
def script bkp_dbdisk "backup db devclass=dbback type=full wait=yes"
upd script bkp_dbdisk "delete volhistory type=dbback todate=today-1
wait=yes"
upd script bkp_dbdisk "backup volhistory filename=g:\dbback\volhist.out"
upd script bkp_dbdisk "backup devconfig filename=g:\dbback\devcnfg.out"
```

b. Gestión de Cintas

Nombre	Descripción
ing_scratch	Este script permite ingresar cintas en blanco (scratch) a la librería robótica

```
def script ing_scratch "checkin libvolume lib01 status=scratch checlabel=barcode search=yes"
```

Nombre	Descripción
ing_private	Este script permite ingresar cintas con datos (private) a la librería robótica

```
def script ing_private "checkin libvolume lib01 status=private checlabel=barcode search=yes"
```

Nombre	Descripción
ing_cleaner	Este script permite ingresar cintas de limpieza (cleaner) a la libreria robotica

```
def script ing_cleaner "checkin libvolume lib01 status=cleaner cleanings=50 checlabel=barcode
search=yes"
```

Nombre	Descripción
ing_offsite_bulk	Este script permite ingresar una cinta (a través de la puerta de entrada/salida) que retorna del depósito externo de cintas (offsite) a la librería robótica

```
def script ing_offsite_bulk "checkin libvolume lib01 $1 status=private checlabel=barcode
search=bulk"
upd script ing_offsite_bulk "update volume $1 access=readwrite"
```

Nombre	Descripción
ret_cinta	Este script permite retirar una cinta de la librería robótica

```
def script ret_cinta "checkout libvolume lib01 $1 remove=bulk checklabel=no"
```

Nombre	Descripción
ret_offsite	Este script permite retirar una cinta de la librería robótica que será enviada al depósito externo (offsite)

```
def script ret_offsite "checkout libvolume lib01 $1 remove=bulk checklabel=no"
upd script ret_offsite "update volume $1 access=offsite"
```

c. Procesamiento de Datos

Nombre	Descripción
exp_inventory	exp_inventory permite iniciar el proceso de expiración de respaldos, conforme a los tiempos de retención definidos en las politicas de dominios

```
def script exp_inventory "expire inventory"
```

Nombre	Descripción
mig_stgpoold	mig_stgpoold permite iniciar el proceso de migración de disco a cinta para los Storage Pool en disco de los respaldos diarios
mig_stgpools	mig_stgpoold permite iniciar el proceso de migración de disco a cinta para los Storage Pool en disco de los respaldos semanales
mig_stgpoolm	mig_stgpoold permite iniciar el proceso de migración de disco a cinta para los Storage Pool en disco de los respaldos mensuales, virtuales e históricos

```
def script mig_stgpoold "migrate stgpool bkpdskfil_d wait=yes"
upd script mig_stgpoold "migrate stgpool bkpdskora_d wait=no"

def script mig_stgpools "migrate stgpool bkpdskfil_s wait=yes"
upd script mig_stgpools "migrate stgpool bkpdskora_s wait=no"

def script mig_stgpoolm "migrate stgpool arcdskfil_m wait=yes"
```

d. Misceláneas

Nombre	Descripción
def_mcdiario	def_mcdiario permite definir la management class diario (dia) como default, tanto en el dominio de servidores críticos (dom_files) como el dominio de servidores no críticos (dom_ora)
def_mcsemanal	def_mcsemanal permite definir la management class semanal (sem) como default, tanto en el dominio de servidores críticos (dom_files) como el dominio de servidores no críticos (dom_ora)

```
def script def_mcdiario "assign defmgmtclass dom_files pol1 dia"
upd script def_mcdiario "assign defmgmtclass dom_ora pol1 dia"

def script def_mcsemanal "assign defmgmtclass dom_files pol1 sem"
upd script def_mcsemanal "assign defmgmtclass dom_ora pol1 sem"
```

e. Consultas

Nombre	Descripción
qry_client	qry_client nos muestra la lista de servidores que son clientes dc TSM

```
def script qry_client "select distinct substr(tcp_name,1,35) as HOSTNAME,substr(tcp_address,1,15)
as IPADDRESS,substr(platform_name,1,16) as OS,substr(client_os_level,1,6) as
OS_LEVEL,concat(concat(concat(concat(client_version,'.'),client_release),'.'),client_level) as
VERSION
from nodes where length(client_version)>0 order by hostname,os,version asc"upd script
def_mcsemanal "assign defmgmtclass dom_ora pol1 sem"
```

Nombre	Descripción
qry_node	qry_node nos muestra la lista de nodos registrados en el servidor TSM

```
def script qry_node "select distinct substr(node_name,1,15) as NODO,substr(platform_name,1,16)
as OS,substr(client_os_level,1,6) as
OS_LEVEL,concat(concat(concat(concat(client_version,'.'),client_release),'.'),client_level) as
VERSION from nodes where length(client_version)>0 order by nodo,os,version ascdef_mcsemanal
"assign defmgmtclass dom_ora pol1 sem"
```

Nombre	Descripción
qry_summary	qry_summary nos muestra el resumen de los respaldos realizados en una fecha dada

```
def scr qry_summary "ISSUE MESSAGE I
'*********************************************************************************'"
upd scr qry_summary "ISSUE MESSAGE I ' REPORTE SUMARIO DE RESPALDOS'"
upd scr qry_summary "ISSUE MESSAGE I ' '"
upd scr qry_summary "ISSUE MESSAGE I
'*********************************************************************************'"
upd scr qry_summary "ISSUE MESSAGE I ' '"
upd scr qry_summary "ISSUE MESSAGE I '-----------------------------------'"
upd scr qry_summary "ISSUE MESSAGE I ' RESPALDOS ENTRE LAS 00:00 Y 06:00'"
upd scr qry_summary "ISSUE MESSAGE I '-----------------------------------'"
upd scr qry_summary "select distinct (select substr(to_char(min(start_time),'dd/mm/yy
HH24:MI'),1,18)
from summary where to_char(start_time,'DD-MM-YY HH24:MI') between
concat(to_char((current_date -
1 day),'DD-MM-YY'),' 00:00') and concat(to_char((current_date - 1 day),'DD-MM-YY'),' 06:00') and
entity=a.entity) as start,(select substr(to_char(max(end_time),'dd/mm/yy HH24:MI'),1,18) from
summary
where to_char(start_time,'DD-MM-YY HH24:MI') between concat(to_char((current_date - 1
day),'DDMM-
YY'),' 00:00') and concat(to_char((current_date - 1 day),'DD-MM-YY'),' 06:00') and entity=a.entity) as
end,substr(entity,1,15) as node,(select substr(sum(affected),1,12) from summary where
to_char(start_time,'DD-MM-YY HH24:MI') between concat(to_char((current_date - 1 day),'DD-MM-
YY'),'
00:00') and concat(to_char((current_date - 1 day),'DD-MM-YY'),' 06:00') and entity=a.entity) as
bkp_files,(select substr((sum(bytes)/1024/1024),1,12) from summary where to_char(start_time,'DD-
MMYY
HH24:MI') between concat(to_char((current_date - 1 day),'DD-MM-YY'),' 00:00') and
concat(to_char((current_date - 1 day),'DD-MM-YY'),' 06:00') and entity=a.entity) as MB from summary
as
a where activity='BACKUP' and to_char(start_time,'DD-MM-YY HH24:MI') between
concat(to_char((current_date - 1 day),'DD-MM-YY'),' 00:00') and concat(to_char((current_date - 1
day),'DD-MM-YY'),' 06:00') order by start"
upd scr qry_summary "ISSUE MESSAGE I '-----------------------------------'"
upd scr qry_summary "ISSUE MESSAGE I ' RESPALDOS ENTRE LAS 06:00 Y 13:00'"
upd scr qry_summary "ISSUE MESSAGE I '-----------------------------------'"
upd scr qry_summary "select distinct (select substr(to_char(min(start_time),'dd/mm/yy
HH24:MI'),1,18)
from summary where to_char(start_time,'DD-MM-YY HH24:MI') between
concat(to_char((current_date -
1 day),'DD-MM-YY'),' 06:00') and concat(to_char((current_date - 1 day),'DD-MM-YY'),' 13:00') and
entity=a.entity) as start,(select substr(to_char(max(end_time),'dd/mm/yy HH24:MI'),1,18) from
summary
where to_char(start_time,'DD-MM-YY HH24:MI') between concat(to_char((current_date - 1
day),'DDMM-
YY'),' 06:00') and concat(to_char((current_date - 1 day),'DD-MM-YY'),' 13:00') and entity=a.entity) as
end,substr(entity,1,15) as node,(select substr(sum(affected),1,12) from summary where
to_char(start_time,'DD-MM-YY HH24:MI') between concat(to_char((current_date - 1 day),'DD-MM-
YY'),'
06:00') and concat(to_char((current_date - 1 day),'DD-MM-YY'),' 13:00') and entity=a.entity) as
```

```
bkp_files,(select substr((sum(bytes)/1024/1024),1,12) from summary where to_char(start_time,'DD-
MMYY
HH24:MI') between concat(to_char((current_date - 1 day),'DD-MM-YY'),' 06:00') and
concat(to_char((current_date - 1 day),'DD-MM-YY'),' 13:00') and entity=a.entity) as MB from summary as
a where activity='BACKUP' and to_char(start_time,'DD-MM-YY HH24:MI') between
concat(to_char((current_date - 1 day),'DD-MM-YY'),' 06:00') and concat(to_char((current_date - 1
day),'DD-MM-YY'),' 13:00') order by start"
upd scr qry_summary "ISSUE MESSAGE I '----------'"
upd scr qry_summary "ISSUE MESSAGE I ' RESPALDOS ENTRE LAS 13:00 Y 18:00'"
upd scr qry_summary "ISSUE MESSAGE I '----------'"
upd scr qry_summary "select distinct (select substr(to_char(min(start_time),'dd/mm/yy HH24:MI'),1,18)
from summary where to_char(start_time,'DD-MM-YY HH24:MI') between concat(to_char((current_date -
1 day),'DD-MM-YY'),' 13:00') and concat(to_char((current_date - 1 day),'DD-MM-YY'),' 18:00') and
entity=a.entity) as start,(select substr(to_char(max(end_time),'dd/mm/yy HH24:MI'),1,18) from summary
where to_char(start_time,'DD-MM-YY HH24:MI') between concat(to_char((current_date - 1 day),'DD-MM-
YY'),' 13:00') and concat(to_char((current_date - 1 day),'DD-MM-YY'),' 18:00') and entity=a.entity) as
end,substr(entity,1,15) as node,(select substr(sum(affected),1,12) from summary where
to_char(start_time,'DD-MM-YY HH24:MI') between concat(to_char((current_date - 1 day),'DD-MM-YY'),'
13:00') and concat(to_char((current_date - 1 day),'DD-MM-YY'),' 18:00') and entity=a.entity) as
bkp_files,(select substr((sum(bytes)/1024/1024),1,12) from summary where to_char(start_time,'DD-
MMYY
HH24:MI') between concat(to_char((current_date - 1 day),'DD-MM-YY'),' 13:00') and
concat(to_char((current_date - 1 day),'DD-MM-YY'),' 18:00') and entity=a.entity) as MB from summary as
a where activity='BACKUP' and to_char(start_time,'DD-MM-YY HH24:MI') between
concat(to_char((current_date - 1 day),'DD-MM-YY'),' 13:00') and concat(to_char((current_date - 1
day),'DD-MM-YY'),' 18:00') order by start"
upd scr qry_summary "ISSUE MESSAGE I '----------'"
upd scr qry_summary "ISSUE MESSAGE I ' RESPALDOS ENTRE LAS 18:00 Y 23:59'"
upd scr qry_summary "ISSUE MESSAGE I '----------'"
upd scr qry_summary "select distinct (select substr(to_char(min(start_time),'dd/mm/yy HH24:MI'),1,18)
from summary where to_char(start_time,'DD-MM-YY HH24:MI') between concat(to_char((current_date -
1 day),'DD-MM-YY'),' 18:00') and concat(to_char((current_date - 1 day),'DD-MM-YY'),' 23:59') and
entity=a.entity) as start,(select substr(to_char(max(end_time),'dd/mm/yy HH24:MI'),1,18) from summary
where to_char(start_time,'DD-MM-YY HH24:MI') between concat(to_char((current_date - 1 day),'DD-MM-
YY'),' 18:00') and concat(to_char((current_date - 1 day),'DD-MM-YY'),' 23:59') and entity=a.entity) as
end,substr(entity,1,15) as node,(select substr(sum(affected),1,12) from summary where
to_char(start_time,'DD-MM-YY HH24:MI') between concat(to_char((current_date - 1 day),'DD-MM-YY'),'
18:00') and concat(to_char((current_date - 1 day),'DD-MM-YY'),' 23:59') and entity=a.entity) as
bkp_files,(select substr((sum(bytes)/1024/1024),1,12) from summary where to_char(start_time,'DD-
MMYY
HH24:MI') between concat(to_char((current_date - 1 day),'DD-MM-YY'),' 18:00') and
concat(to_char((current_date - 1 day),'DD-MM-YY'),' 23:59') and entity=a.entity) as MB from summary as
a where activity='BACKUP' and to_char(start_time,'DD-MM-YY HH24:MI') between
concat(to_char((current_date - 1 day),'DD-MM-YY'),' 18:00') and concat(to_char((current_date - 1
day),'DD-MM-YY'),' 23:59') order by start"
```

Nombre	Descripción
qry_event	qry_event nos muestra la lista de respaldos programados en una fecha dada, así como el estado final del evento. Este script y el anterior (qry_summary) permiten hacer seguimiento del resultado de los respaldos programados en el servidor TSM

```
def script qry_event "issue message i
'*********************************************************************************'"
upd script qry_event "issue message i ' REPORTE DE EVENTOS PROGRAMADOS'"
upd script qry_event "issue message i ' '"
upd script qry_event "issue message i
'*********************************************************************************'"
upd script qry_event "issue message i ' '"
upd script qry_event "issue message i '---------------------------------------------------------------------------'"
upd script qry_event "issue message i 'Eventos en Clientes'"
upd script qry_event "issue message i '---------------------------------------------------------------------------'"
upd script qry_event "query event * * begindate=$1 begintime=00:00"
upd script qry_event "issue message i '---------------------------------------------------------------------------'"
upd script qry_event "issue message i 'Eventos en Servidor TSM'"
upd script qry_event "issue message i '---------------------------------------------------------------------------'"
upd script qry_event "query event * type=admin begindate=$1 begintime=00:00"
upd script qry_event "issue message i '---------------------------------------------------------------------------'"
```

4.7.4.8 Programación De Tareas Administrativas

Se programaron las siguientes tareas administrativas:

a. Respaldo de la Base de Datos TSM

Nombre	Frecuencia	Horario	Acción
bkp_dbtape	Lunes - Domingo	12:00	run bkp_dbtape

Descripción:
Respaldo de la base de datos TSM

Comandos:

```
define schedule bkp_dbtape cmd="run bkp_dbtape" \
type=administrative \
active=yes \
schedstyle=enhanced \
starttime=12:00
```

b. Expiración de Datos

Nombre	Frecuencia	Horario	Acción
exp_inventory	Lunes - Domingo	12:30	run exp_inventory

Descripción:
Expiración de datos conforme a los parametros de tiempos de retencion

Comandos:
```
define schedule exp_inventory cmd="run exp_inventory" \
type=administrative \
active=yes \
schedstyle=enhanced \
starttime=12:30
```

c. Migración de Respaldos Diarios

Nombre	Frecuencia	Horario	Acción
mig_stgpoold	Martes - Viernes	09:00	run mig_stgpoold

Descripción:
Esta tarea migra los respaldos diarios, que originalmente van a disco, hacia cintas, de manera que los discos queden libres para futuros respaldos

Comandos:
```
define schedule mig_stgpoold cmd="run mig_stgpoold" \
type=administrative \
active=yes \
schedstyle=enhanced \
starttime=09:00 dayofweek=tu,we,th,fri
```

d. Migración de Respaldos Semanales

Nombre	Frecuencia	Horario	Acción
mig_stgpools	Lunes de las semanas 2,3,4 y 5	09:00	run mig_stgpools

Descripción:
Esta tarea migra los respaldos semanales, que originalmente van a disco, hacia cintas, de manera que los discos queden libres para futuros respaldos

Comandos:
define schedule mig_stgpools cmd="run mig_stgpools" \
type=administrative \
active=yes \
schedstyle=enhanced \
starttime=09:00 dayofweek=monday
weekofmonth=sec,third,fourth,last

e. Migración de Respaldos Mensuales

Nombre	Frecuencia	Horario	Acción
mig_stgpoolm	Lunes de la semana 1	09:00	run mig_stgpoolm

Descripción:
Esta tarea migra los respaldos mensuales, que originalmente van a disco, hacia cintas, de manera que los discos queden libres para futuros respaldos

Comandos:
define schedule mig_stgpoolm cmd="run mig_stgpoolm" \
type=administrative active=yes \
schedstyle=enhanced \
starttime=09:00 dayofweek=monday
weekofmonth=sec,third,fourth,last

f. Activación de Management Class para Respaldos Diarios

Nombre	Frecuencia	Horario	Acción
def_mcdiario	Domingo	23:50	run def_mcdiario

Descripción:
Esta tarea activa las politicas para respaldos diarios

Comandos:
define schedule def_mcdiario cmd="run def_mcdiario" \
type=administrative \
active=yes \
schedstyle=enhanced \
starttime=23:50 dayofweek=sunday

g. Activación de Management Class para Respaldos Semanales

Nombre	Frecuencia	Horario	Acción
def_mcsemanal	Viernes	23:50	run def_mcsemanal

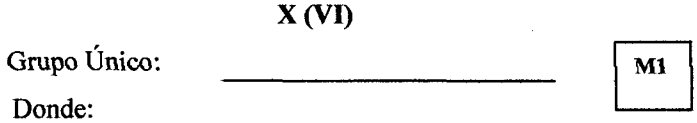
CAPÍTULO V

MATERIALES Y MÉTODOS

5.1 DISEÑO DE CONTRASTACIÓN DE LA HIPÓTESIS

El diseño de contrastación de la Hipótesis es no experimental, de tipo descriptivo de corte transversal **de Grupo Único con Medición Posterior.**

Esquema del Diseño:



Donde:

X = *Implementación de un Servidor Tivoli Storage Manager*

M1 = Descripción de la percepción u observación de la mejora del salvaguardo de la información en la Oficina Registral Casma de la Zona Registral VII Sede Huaraz (VI).

5.2 POBLACIÓN

Población es la totalidad del fenómeno a estudiar en donde las unidades de población poseen una característica común, la cual se estudia y da origen a los datos de la investigación, (Tamayo & Tamayo, 2000; Balestrini, 2002). En el caso de esta investigación, el universo objeto de estudio, es una población finita, que está constituida por todo el personal que labora en la Zona Registral VII – Sede Huaraz, distribuidas en las distintas áreas de producción: haciendo un total de 195 trabajadores.

Además se tomó en cuenta el criterio experimental de los Jefes de las Unidades de Tecnologías de la Información de otras Sedes (8 Sedes)

5.3 MUESTRA

Tamayo & Tamayo (2000), define la muestra como la selección de un grupo de elementos con la intención de averiguar algo sobre la población de la cual están tomados. Para conocer las características de las variables del estudio en la empresa Sima - Chimbote se calculó la muestra utilizando la formula para poblaciones finitas:

$$n = \frac{N * Z_c^2 * S^2}{e^2 (N - 1) + Z_c^2 * S^2}$$

Se utilizaron los siguientes parámetros para determinar la muestra:

Donde:

n : Tamaño de la muestra

N: Tamaño de la población

Zc: coeficiente de confianza

Nivel de Confianza 95% => Zc = ± 1,96

e: representará el error muestral o la diferencia entre la media muestral X y la población, (e: el error admisible debe ser a lo sumo 5% por encima o por debajo del valor real).

S: desviación típica Estándar, dada por:

S = p . q = 0.50 . 0.50 = 0.25

p: es la proporción poblacional. p puede ser estimada de experiencias anteriores de esta naturaleza.

q: La proporción complementaria a p. Se obtiene calculando 1 - p = q.

Determinación de la muestra para los Operadores, reemplazando los datos en la formula, se obtiene:

n = 65 trabajadores

Según el cuestionario (Anexo A), las preguntas se formularon de acuerdo a los aspectos a investigar y se utilizó una escala Likert de 5 puntos, siendo 1 el menor valor y 5 el mayor valor. Para facilitar la comprensión de todos los trabajadores la valoración Likert se expresa en su equivalente en porcentuales de la siguiente manera:

1= de 0% a 20%; 2= mayor que 20% y menor o igual que 40%; 3= mayor que 40% y menor o igual que 60%; 4= mayor que 60 % y menor o igual que 80%; 5= mayor que 80% y menor o igual que 100%.

5.4 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

5.4.1 TÉCNICAS

5.4.1.1 De Campo

Para determinar el nivel de la Implementación de un Servidor Tivoli Storage Manager de las unidades de la muestra, en la percepción posterior.

5.4.1.2 De Gabinete

Para hacer el análisis y evaluación homogénea de las unidades de la población y determinar las unidades de la muestra y sus correspondientes unidades de análisis, que conformarán el grupo único.

5.4.2 INSTRUMENTOS

5.4.2.1 Tablas de Referencia

Preparación de los cuadros para recoger la información en relación a la Implementación de un Servidor Tivoli Storage Manager de las unidades de análisis en la observación posterior.
Preparación de tablas para consolidar la información de los procesos antes mencionados.

5.4.2.2 Cuestionarios

Para registrar información requerida, impresiones y sugerencias en cuanto a la Implementación de un Servidor Tivoli Storage Manager de las unidades de análisis de la muestra.

5.4.2.3 Tablas de Calificación

Para recoger la información sobre el nivel de mejoras en el salvaguardo de la información logradas a través de las unidades de análisis de la muestra.

5.5 METODOLOGIA DE PASOS PARA EL DESARROLLO DEL TRABAJO

1. El método de investigación utilizado es el Inductivo – Deductivo. Ante esta realidad observable, la variable dependiente se pudo dividir en características o indicadores en cada uno de los procesos definidos, a efectos de contrastar la hipótesis, que es verdadera confirmada a través de la percepción de la veracidad de los indicadores, es decir, es suficiente que los indicadores de la variable dependiente sean verdaderos para que la hipótesis sea verdadera, cuyos resultados nos permitirá generalizar a la población.
2. Elaboración definitiva del Marco Teórico.

3. Identificar las unidades de la población del estudio y determinar las unidades de la muestra.
4. Preparación de las Técnicas, Instrumentos y Herramientas a utilizar en el estudio para la recogida de datos.
5. Desarrollar la Implementación, en función a la variable independiente, que permitan llevar a cabo la evaluación de los indicadores de la variable dependiente.
6. Capacitar a los involucrados de la muestra para el llenado de la encuesta
7. Elaboración del informe final de la investigación

CAPÍTULO VI

RESULTADOS Y DISCUSIÓN

Si bien el modelo a desarrollar en la Oficina Registral de Casma, ya ha sido evaluado e otras oficinas registrales, nos vemos en la necesidad de garantizar su utilidad. Para completar las medidas de seguridad que se han de tomar a la hora de guardar los soportes de almacenamiento es bueno recordar que no sólo vale con tener las copias en lugares seguros ante catástrofes naturales. También debemos proteger la información y no sólo la de los backup, sino toda, de personal no autorizado.

Cuando se habla de personal no autorizado no nos referimos a personas no relacionadas con el departamento de informática como pueda ser personal de mantenimiento, recursos humanos, comunicación o cualquier otro: en un plan de seguridad debe estar perfectamente indicado quiénes pueden acceder a las copias, quiénes deben encargarse de guardar los backup, quién puede restaurar información, etcétera.

Los backup los ha de guardar el personal indicado a tal efecto. Ellos son los encargados de seguir las pautas indicadas en la planificación y los responsables ante cualquier fallo. El acceso a cualquier copia debe estar autorizado por el responsable de seguridad y no por cualquier persona por muy alto directivo que pueda ser.
Pueden parecer reglas muy estrictas, pero se dan circunstancias en las que ciertas copias están en poder de personal ajeno al grupo de seguridad u ocasiones en las que personal de desarrollo solicita datos o restauraciones.

En la medida de lo posible hay que evitar esta situación, ya no por la maldad o el desconocimiento de la gente, sino por mantener el máximo control e intentar adaptarnos a lo establecido en el plan de contingencia y documento de seguridad.

El flexibilizar ciertos comportamientos lo único que conlleva es el aumento del riesgo a que suceda algo negativo o a que no se cumplan requisitos de cara a auditorías, certificaciones de calidad, cumplimiento de leyes, etc.

Una organización es un todo, como tal se debe tratar de conseguir la máxima interoperabilidad e integración entre las diferentes partes, pero todo ello sin descuidar las competencias y responsabilidades de cada departamento. Al fin y al cabo, tanto la

integración como las competencias de cada una de las partes de una organización buscan un objetivo común: la continuidad del negocio.

6.1 DISCUSIÓN

Existe una reflexión sobre seguridad que viene a decir que el esfuerzo que debemos dedicar a proteger algo debe ser directamente proporcional a su valor.

Esta reflexión es más que válida para el tema del que se ha hablado a lo largo de estas páginas. A pesar de que se ha intentado no hablar mucho de cuestiones económicas, ha sido inevitable citar el tema en alguna ocasión y podía haber sido una constante a lo largo de la mayoría de las secciones de este trabajo.

Ha quedado claro que debemos hacer todo lo posible para garantizar al máximo la continuidad de la organización para la que elaboramos un plan de contingencia y ha de quedar claro que esa garantía está estrechamente ligada al factor económico, cuanto más dinero invirtamos más seguros estaremos ante cualquier contingencia y/o interrupción.

Pero no debemos olvidar, y aquí viene algo que debemos tener muy claro, que hagamos lo que hagamos siempre deberemos asumir ciertos riesgos, no existe la seguridad total.

Cualquier organización debería estar preparada para hacer frente a ciertas situaciones que pusieran en jaque su continuidad. A pesar de que poco a poco las empresas van tomando conciencia de que hay que proteger la información, éste es un tema en el que todavía debemos insistir, y desde aquí pongemos un pequeño granito de arena para ello.

Algo que tampoco debemos olvidar es que la protección de nuestros sistemas, de la información, es un proceso vivo. Mientras exista la organización debe existir preocupación de hacer frente a los problemas que pongan en peligro su continuidad.

Cuántas veces habremos oído hablar de la sociedad de la información. Incluso puede que alguna vez nosotros mismos hayamos usado este término, no sé si con la suficiente propiedad, pero al fin y al cabo debemos tener muy claro que si hoy en día desapareciera toda la información almacenada en la infinidad de discos duros que existen, nuestra sociedad de la información' se iría a pique.

Sin ánimo de convertir estas conclusiones en apocalípticas, nos tomaremos la libertad de insistir en otro de los temas que se han tratado con cierta insistencia: debemos tener copias de seguridad de nuestros datos. No me quiero imaginar qué pasaría si ahora mismo se quemara el disco duro de mi ordenador y no tuviera ninguna copia de este documento.

A pesar de lo escrito en las últimas líneas hay que decir que no todo es dinero. Es importante, sí, pero no es lo único. Para que en nuestra empresa todo "vaya sobre ruedas" debemos contar con un personal cualificado y sobre todo (y esta es una opinión muy personal) comprometido con la empresa. Si hablamos únicamente de seguridad en SI nos

pasa lo mismo. El personal encargado de la seguridad debe estar debidamente preparado, pero es muy importante que el usuario esté comprometido con esta labor y para ello el responsable y su grupo deben ser los primeros en dar ejemplo y tomar unas decisiones lógicas con la situación a la que se enfrenten.

Ahí entramos en un gasto personal por parte de los encargados: tiempo y ganas y en esos casos la inversión económica pasa a un segundo plano.

Políticas de respaldo, ciclos de copias de seguridad, protección de la información, documento de seguridad, planes de contingencia... Estoy seguro de que cualquiera que pueda leer estas líneas, volverá a oír hablar de estos términos, puede que incluso sean objeto de trabajos o vida laboral. Y ahora, escribiendo estas líneas, recuerdo mis conversaciones con expertos en la materia y qué razón tienen cuando dicen que una de las máximas de este mundo es que te pasas una vida elaborando un buen plan de contingencia y deseando nunca tener que usarlo.

6.2 MODELO DE EVALUACIÓN DE LA IMPLEMENTACIÓN DE UN SERVIDOR TIVOLI STORAGE MANAGER

El modelo propuesto, permite evaluar los resultados de la Implementación de un Servidor Tivoli Storage Manager en los procesos básicos tradicionales en la Oficina Registral de Casma.

Esta evaluación no solo permite demostrar el impacto de la implementación, si no contribuye a aumentar la seguridad e integración de la información por medio de la copias de seguridad que serán el producto final de nuestro trabajo, además de la optimización de las copias de seguridad a disco.

6.2.1 Nivel de Confianza por parte de los usuarios externos/internos

Sunarp, para cumplir su misión, que es la de brindar seguridad jurídica al ciudadano, brindado los servicios de inscripción de bienes muebles, inmuebles, personas jurídicas y propiedad vehicular, incluyéndose adicionalmente los servicios de asesoría jurídica, defensoría del usuario, servicios en la plataforma Web de forma productiva y sostenible para generar confianza, bienestar y compromiso social en los trabajadores para con los clientes para así contribuir a fomentar una cultura registral, teniendo como visión ser una institución referente a nivel internacional, altamente tecnificada, proactiva confiable y con presencia efectiva en todo el territorio nacional, con trabajadores formados y capacitados

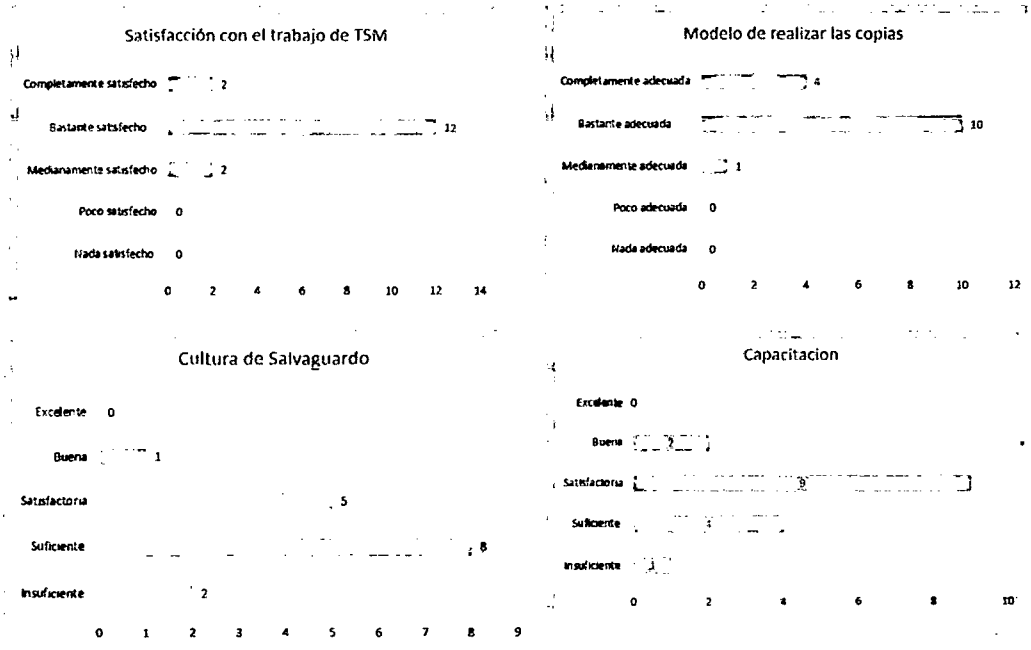
en un ambiente de bienestar y compromiso social, fomentando el desarrollo y la economía de la región y el país.

Usuarios Internos:

Se conversó y realizo una encuesta con los Jefes de UTI y especialistas de Base de Datos de otras Sedes que utilizan Tivoli Storage Manager como solución como:

- Zona Registral N° I Piura.
- Zona Registral N° II Chiclayo
- Zona Registra N° III Moyobamba
- Zona Registral N° IX Lima
- Zona Registral N° X Cusco
- Zona Registral N° XI Ica
- Zona Registral N° XII Arequipa
- Zona Registral N° XIII Tacna

Los resultados obtenidos en el aspecto de Nivel de Confianza por parte de los Usuarios internos pueden observarse en la Figura N° 001, que persigue en general determinar el grado de Satisfacción con la herramienta.



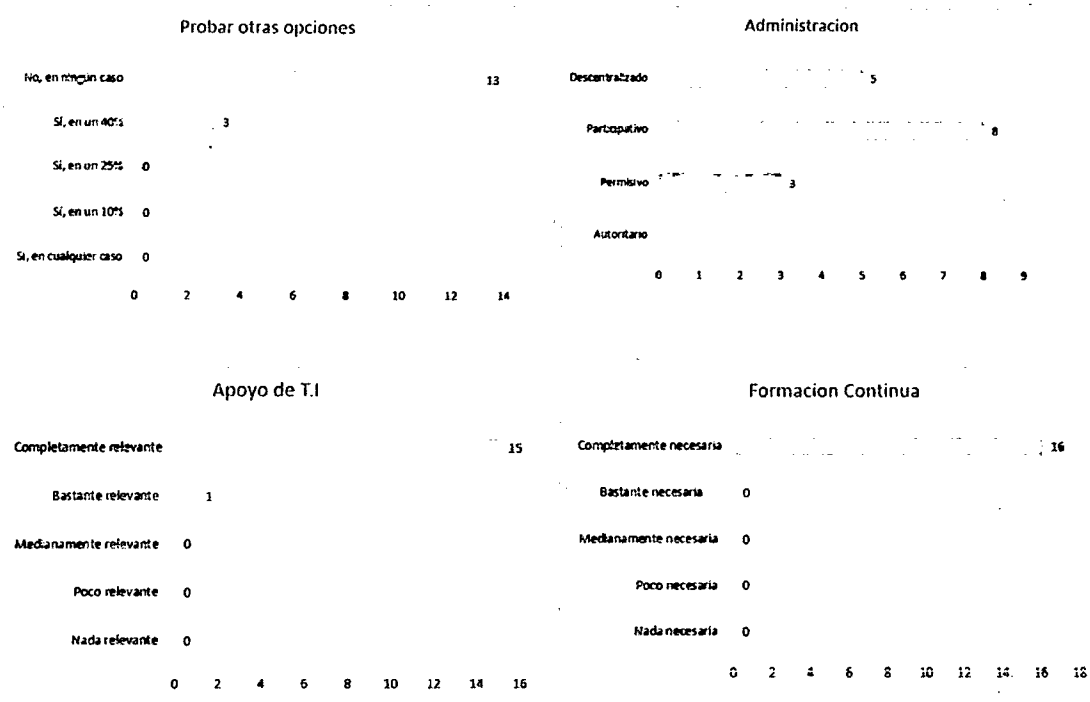


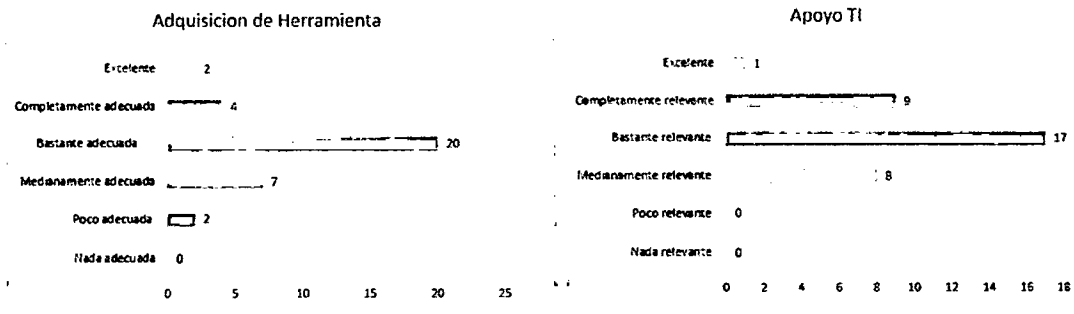
Figura N° 01 - Usuarios Internos

Con lo cual podemos apreciar que las Zonas Registrales evaluadas, están conformes con la utilización de la herramienta.

Podemos inferir entonces que dicha utilidad nos resulta ***factible***.

Usuarios Externos:

Asimismo se realizó una encuesta con los demás usuarios en este caso, el personal de la Zona Registral VII, especialmente a las áreas usuarias (Publicidad, Caja, Informes, Archivo, Administración y Catastro), a las cuales se les mostró la utilidad llegando a las siguientes conclusiones que se detallan en la Figura N° 02.



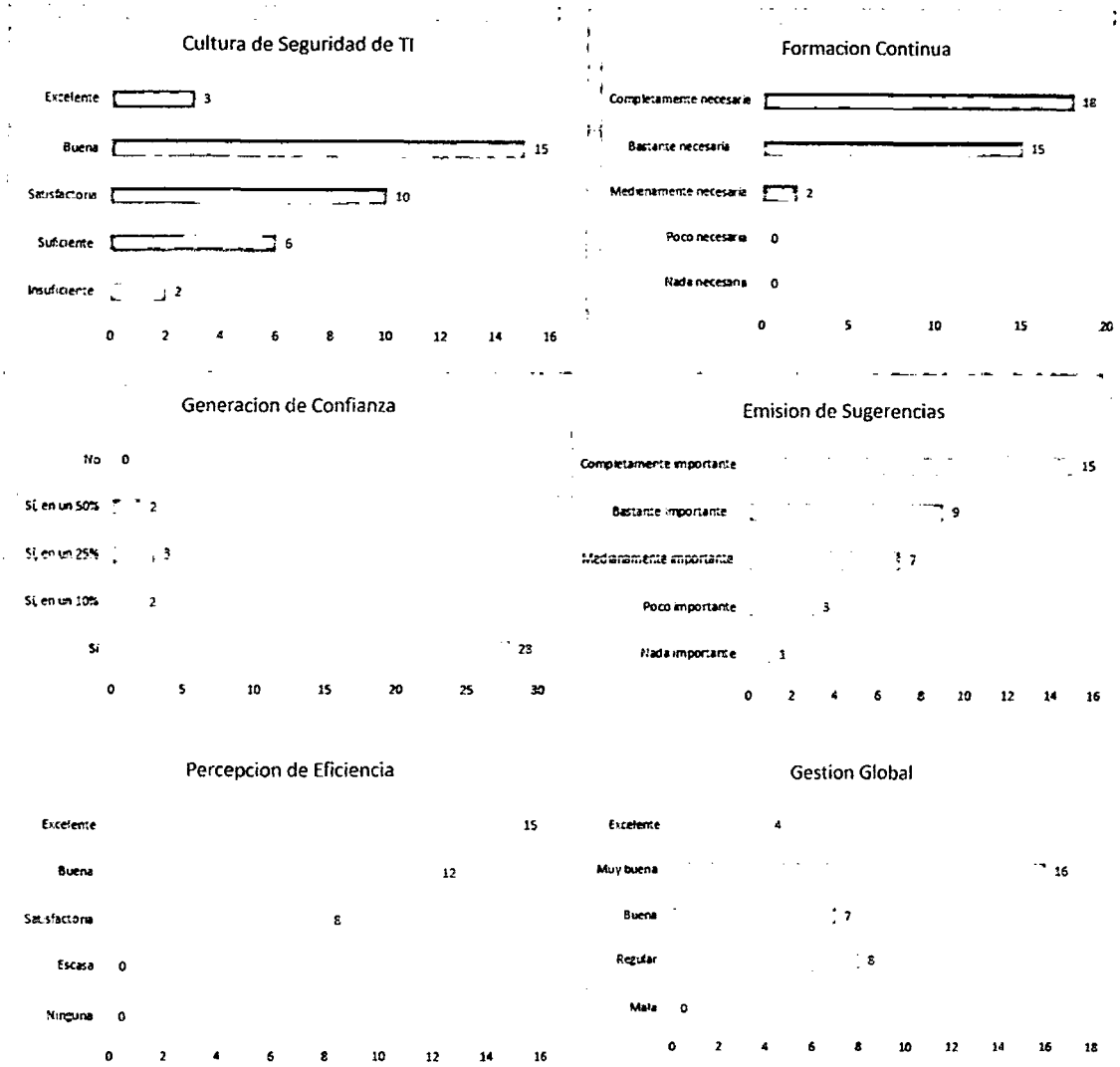


Figura N° 02 - Usuarios Internos

Podemos determinar entonces que la utilidad nos resulta ***factible***.

6.2.2 Análisis de Costo Beneficio de la Implementación

Para una institución publica como SUNARP, lo principal es el ahorro Dinero-tiempo en cuanto a sus diversos procedimientos, es por ello que se detalla una comparativa en general algunos de los alcances de la solución:

Antes	Ahora
Compra de 2 Cintas LTO 5 (IBM) cada mes ($ 95.00 c/u)	Ahorro, pues ahora, con el concepto de De-Duplicación, se compra, 1 cada 6 meses.

El riesgo de pérdida de Datos estaba inminente.	El Riesgo de pérdida de datos esta minimizado ya que se guardan copias Diarias, Semanales y Mensuales.
No había un lugar donde almacenar físicamente estas copias	Actualmente, a parte de los Magazines que sirven para alojar estos discos, también se cuenta con un armario ignifugo, donde se guardan periódicamente las copias de seguridad.
El Backup de Datos se guardaba en cintas Ópticas	El Backup de Datos de hace mediante TSM
La Búsqueda de Archivos (Tomos y/o Folios, antiguos) demoraba hasta 3 horas.	La búsqueda de Archivos Digitalizado, demora aproximadamente de 3 a 5 minutos.
La estadística de Datos, requería un gran esfuerzo al buscar la data, al buscar las comparativas de años pasados	La estadística se tiene en tiempo real, no requiriendo un esfuerzo grande para acceder a la información requerida.
No había protección de ningún tipo.	Protege hasta diez veces más datos de usuario al día por servidor de copia de seguridad.

Todos estos ítems, en beneficios y costos, generan un ahorro y promueven la imagen de institución, en vista de los cumplimientos de estándares de calidad y protección de datos, por lo tanto el proyecto es ***factible.***

6.3 MODELO DE EVALUACIÓN DEL SALVAGUARDO DE LA INFORMACION

6.3.1 Análisis de la Evaluación de la funcionalidad de la Solución

La implementación de Tivoli Storage Manager atrae muchos beneficios funcionales tiempo para la Oficina Registral de Casma. Entre ellos podemos mencionar:

- **Administración**: Ofrece mayor visualización y productividad de administrador
- **Adquisición:** Debido a la compra, se tiene un solo fabricante, un tipo de hardware exclusivo para la solución brindada, y sobre todo la certificación de

los técnicos que al momento de la adquisición se validó en los términos de referencia.

- **Implementación:** Con los niveles de preparación de los técnicos capacitados, la herramienta esta lista en poco tiempo para su utilización para beneficio de la Oficina.
- **Soporte:** Conforme al estudio, el soporte de IBM se comunica constantemente para el soporte de garantía y el extendido.
- **Beneficios WAN**: Acelera el backup al reducir la cantidad de datos transferida.
- **Beneficios de la De-duplicación:** TSM rentabiliza el backup a Disco, optimizando el espacio utilizado y generando menos conste en la adquisición de las cintas.

Todos estos ítems, que antes no se habían implementado, apuntan al cambio tecnológico y proyecta a SUNARP hacia los adelantos emergentes, haciendo una comparativa:

	ANTES	AHORA
Administración	No	Si
Adquisición	No	Si
Implementación	No	Si
Soporte	No	Si
Beneficios WAN	No	Si
Beneficios de la De-Duplicación	No	Si

El indicador de Funcionalidad de la Solución indica que ahora el proyecto es ***factible***, dado que antes no se contaba con dichos beneficios para la Institución

6.4 CONSTRASTACIÓN DE LA HIPÓTESIS EN FUNCIÓN A LA IMPLEMENTACION DEL SERVIDOR TIVOLI STORAGE MANAGER

HIPÓTESIS NULA (Ho)

La propuesta de la Implementación de un Servidor Tivoli Storage Manager No Genera Positivamente el salvaguardo de la Información en la Oficina Registral de Casma de la Zona Registral VII Sede Huaraz

HIPÓTESIS ALTERNATIVA (Ha)

La propuesta de la Implementación de un Servidor Tivoli Storage Manager SI Genera Positivamente el salvaguardo de la Información en la Oficina Registral de Casma de la Zona Registral VII Sede Huaraz.

Para ir concluyendo cabe citar algunos aspectos a tener en cuenta antes de llevar a cabo una restauración, como por ejemplo:

- Tener una debida autorización por parte del responsable principalmente cuando lo que se va a restaurar es algún fichero suelto a petición de cualquier usuario. Esta autorización también se ha de tener cuando la restauración afecta a algún sistema que esté en producción y funcionando con datos reales.
- Versión del sistema operativo en la que fue guardada la información y versión de la máquina que recibe los datos ya que puede darse el caso de que no sea la misma.
- Comprobar que la información que vamos a restaurar corresponde realmente a lo que queremos, esto es comprobar la etiqueta del soporte para no confundirnos de fecha o de sistema.
- Comprobar que el soporte está debidamente protegido contra grabación, cualquier error humano podría hacernos perder la información.
- Inmediatamente después de la restauración volver a introducir el o los soportes en el ciclo que corresponda. Si se ha traído de sede remota, se volverá a trasladar y si estaba en las propias instalaciones se volverá a guardar bajo las medidas de seguridad adecuadas.
- A posteriori de la restauración, comprobar la integridad de los datos y el correcto funcionamiento de la máquina ya que es algo que no hay que dar por supuesto.

Después de discutir la utilidad propuesta en este Proyecto, percibimos cuantitativamente que su implementación como una herramienta de soporte tiende a generar solides en lo que respecta a la Seguridad en la información que son positivas para la Superintendencia Nacional de los Registros Públicos, específicamente en la Oficina Registral de Casma, lo que demuestra que se cumple la hipótesis alternativo por lo tanto se confirma la hipótesis de la investigación, pues su implementación cubre la mayor cantidad de elementos evaluativos relacionados con la Integridad de la información y sobre todo, la seguridad de la misma.

CAPÍTULO VII

CONCLUSIONES Y RECOMENDACIONES

7.1 CONCLUSIONES

Luego de la implementación se llegaron a las siguientes conclusiones, las mismas que aportaron a la demostración de la validez de nuestro Objetivo General:

- Se demostró que a través de una planificación previa (calendarización) se puede administrar de una manera mucho más óptima el entorno de seguridad de la información, esto hizo ver a la gerencia cuán importante es la necesidad de estar a la vanguardia en tecnología para protección del activo más preciado.

- Se generó un registro de acciones realizadas. Esta especie de reporte es de vital importancia al momento de evaluar el comportamiento del servidor bajo la configuración actual, dadas las circunstancias también puede llevar a ajustarse las especificaciones iniciales con las que se configuró TSM. Gracias a la implementación ahora se tiene un registro periódico de todos los backups, restores y fallas suscitadas.

- Se demostró que la fácil administración hace que se pueda monitorear desde cualquier punto de la Red Sunarp. Debido a las restricciones de Seguridad, esta administración web es posible desde cualquier oficina, y si asi lo solicita Sede Central poder observar el comportamiento del flujo de backups de nuestra Zona Registral N° VII.

- Se implementó TSM, y se adecuó a las normas exigentes del SGSI que actualmente se viene plasmando en todos los procesos (administrativos y colaborativo) que SUNARP está estableciendo, por lo que, conjuntamente con la implementación realizada se elaboraron las políticas de respaldos que nuestra Zona debe manejar a fin de estar de acuerdo con el estándar que se viene aplicando en otras Zonas Registrales.

- Se realizó este documento lo que 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 demostró 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 el personal de la UTI de la Zona Registral N° VII genero un material de practica para que éste sea revisado como material de estudio y compartido con las demás Zonas Registrales que actualmente están trabajando bajo la arquitectura TSM.

7.2 RECOMENDACIONES

Se presentan las siguientes recomendaciones:

- SUNARP, debe tomar en cuenta el presente estudio como base de la implementación con el propósito de mejorar el salvaguardo de la información en la Oficina Registral de Casma de la Zona Registral N° VII - Sede Huaraz, a fin de darle la seguridad jurídica que proclama brindar a sus usuarios.

- Tomar como base el estudio de la implementación y aplicarlo a cualquier Zona Registral que posea o no posea TSM para verificar su eficiencia y funcionalidad en este tipo de rubro de negocio

- Tomar como base la metodología empleada en esta investigación con el objetivo de ampliar el modelo teórico, incorporando nuevas variables o bien profundizando en algunas partes del modelo incluyendo un cuadro de mando y aplicarlo para evaluar su eficiencia y funcionalidad en la implementación de servidores TSM.

REFERENCIAS BIBLIOGRAFICAS

[1] Max Alonso Huamán (2009) Fundamentos de Sistemas de Respaldo de Información

[2] Xavier Mauricio Rea Peñafiel (2012) "Implementación de una de las Herramientas de Salvaguardo de Información para Sinergy Team Cia. Ltda."

[3] López López, Isvel (2010) "Implementación de una solución de respaldos de información en la empresa Uniplex Systems en Quito"

[4] Manual de TSM (2014) IBM Tivoli Redbooks.

[5] Charlotte Brooks, Peter McFarlane, Norbert Pott, Martin Trcka, Eduardo Tomaz. (2006). IBM Tivoli Storage Manager Implementation Guide

[6] Charlotte Brooks, Peter McFarlane, Norbert Pott, Martin Trcka, Eduardo Tomaz. (2006). IBM Tivoli Storage Manager Implementation Concepts.

[7] Ryan Femling. (2006). Mastering System Center Data Protection Manager 2007

[8] Steve Buchanan. (2006). Microsoft Data Protection Manager 2010.

[9] Jason Buffington. (2006). Data Protection for Virtual Data Centers.

DIRECCIONES ELECTRONICAS

[URL 01] http://www-01.ibm.com/support/docview.wss?uid=swg24036718
IBM Tivoli Storage Manager (TSM) Client 6.3.2 Downloads and READMEs

[URL 02] http://es.slideshare.net/maxalonzohuaman/sistemas-de-respaldo-de-informacion-presentation
Fundamentos de Sistemas de Respaldos de Información

[URL 03] www.uteq.edu.mx/tesis/telematica
Telematica y Seguridad de information

[URL 04] http://searchdatabackup.techtarget.com/definition/IBM-TSM-IBM-Tivoli-Storage-Manager
What is IBM TSM (IBM Tivoli Storage Manager)?

[URL 05] http://www.zcom.cl/servicios.php?servicio=8

Amanda Source Backup

[URL 06] http://amanda.zmanda.com/

Amanda Source Backup

[URL 07] http://www-01.ibm.com/software/tivoli/products/storage-mgr/features.html

IBM patrtnerworld

[URL 08] http://publib.boulder.ibm.com/tividd/td/ITSML/GC23-4690-02/es_ES/HTML/anrlgd52218.htm

IBM Redbook Web

[URL 09] http://prcerda.blogspot.com/2010/04/system-center-data-protection-manager.html

Tecnologías Aplicadas

[URL 10] http://scug.be/mike/tag/dpm-scdpm-backup/

Microsoft Data Protection Manager.

[URL11] http://richfrombechtle.wordpress.com/2008/10/07/microsoft-system-center-data-protection-manager-dpm/

Amanda Source Backup

Anexo A

CUESTIONARIO PARA JEFES DE UTI Y ESPECIALISTAS DE BASE DE DATOS

El siguiente cuestionario pretende conocer algunos aspectos sobre la Implementación de un Servidor Tivoli Storage Manager en su Zona Registral. No existen respuestas correctas o incorrectas. Por esto, le pedimos trate de responder de manera objetiva. **Los resultados son confidenciales. Muchas gracias por sus respuestas**

Instrucciones:
1. Lea cuidadosamente cada Ítem formulado.
2. Cada pregunta tiene diferentes opciones seleccione **sola una**, marcando con una (X) a la opción que a su juicio considera más adecuada.
3. Las preguntas se valoran del 1 al 5, están en función de menor a mayor conformidad con la respuesta.
4. Se le agradece responder todos los Ítems.

Calificación: Escala de Likert y porcentual.
1= de 0% a 20%; 2= mayor que 20% y menor o igual que 40%; 3= mayor que 40% y menor o igual que 60%; 4= mayor que 60 % y menor o igual que 80%; 5= mayor que 80% y menor o igual que 100%

---

1. ¿Está usted satisfecho con el trabajo que realiza Tivoli Storage Manager?

Nada satisfecho	Poco satisfecho	Medianamente satisfecho	Bastante satisfecho	Completamente satisfecho
1( )	2( )	3( )	4( )	5( )

2. ¿Cómo juzgaría el modo de realizar las copias de Seguridad con Tivoli Storage Manager?

Nada adecuada	Poco adecuada	Medianamente adecuada	Bastante adecuada	Completamente adecuada
1( )	2( )	3( )	4( )	5( )

3. ¿Cómo calificaría la cultura de Seguridad de la Información en su Zona Registral?

Insuficiente	Suficiente	Satisfactoria	Buena	Excelente
1( )	2( )	3( )	4( )	5( )

4. ¿El personal cuenta con la capacitación correspondiente en comandos TSM?

Insuficiente	Suficiente	Satisfactoria	Buena	Excelente
1( )	2( )	3( )	4( )	5( )

5. ¿Estaría usted dispuesto a cambiar de tecnología si encuentra una alternativa que le brinde mejores opciones?

1. ( ) Sí, en cualquier caso
2. ( ) Sí, en un 10%
3. ( ) Sí, en un 25%
4. ( ) Sí, en un 40%
5. ( ) No, en ningún caso

6. La administración de TSM en su Zona Registral se da de manera:

a. ( ) Autoritario
b. ( ) Permisivo
c. ( ) Participativo
d. ( ) Descentralizado

7.- El apoyo de la tecnología de la información es relevante para desarrollar su trabajo

Nada relevante	Poco relevante	Medianamente relevante	Bastante relevante	Completamente relevante
1( )	2( )	3( )	4( )	5( )

8.- ¿Piensa Ud. que la formación continua es necesaria para el desarrollo del trabajo que desempeña?

Nada necesaria	Poco necesaria	Medianamente necesaria	Bastante necesaria	Completamente necesaria
1( )	2( )	3( )	4( )	5( )

Anexo B

CUESTIONARIO PARA AREAS USUARIAS

El siguiente cuestionario pretende conocer algunos aspectos sobre la Implementación de un Servidor de Salvaguardo de Información en su Zona Registral. No existen respuestas correctas o incorrectas. Por esto, le pedimos trate de responder de manera objetiva. **Los resultados son confidenciales. Muchas gracias por sus respuestas**

Instrucciones:
1. Lea cuidadosamente cada Ítem formulado.
2. Cada pregunta tiene diferentes opciones seleccione **sola una**, marcando con una (X) a la opción que a su juicio considera más adecuada.
3. Las preguntas se valoran del 1 al 5, están en función de menor a mayor conformidad con la respuesta.
4. Se le agradece responder todos los Ítems.

Calificación: Escala de Likert y porcentual.
1= de 0% a 20%; 2= mayor que 20% y menor o igual que 40%; 3= mayor que 40% y menor o igual que 60%; 4= mayor que 60 % y menor o igual que 80%; 5= mayor que 80% y menor o igual que 100%

1.- ¿Cómo valoraría la adquisición de herramientas para la seguridad de la Información?

Nada adecuada	Poco adecuada	Medianamente adecuada	Bastante adecuada	Completamente adecuada
1( )	2( )	3( )	4( )	5( )

2.- El apoyo de la tecnología de la información es relevante para desarrollar su trabajo

Nada relevante	Poco relevante	Medianamente relevante	Bastante relevante	Completamente relevante
1( )	2( )	3( )	4( )	5( )

3. ¿Cómo calificaría la cultura de Seguridad de la Información en su Zona Registral?

Insuficiente	Suficiente	Satisfactoria	Buena	Excelente
1( )	2( )	3( )	4( )	5( )

4.- ¿Piensa Ud. que la formación continua es necesaria para el desarrollo del trabajo que desempeña?

Nada necesaria	Poco necesaria	Medianamente necesaria	Bastante necesaria	Completamente necesaria
1( )	2( )	3( )	4( )	5( )

5. ¿Le genera confianza conocer que la institución cuenta con herramientas para la protección de datos/información?

1. ( ) Sí
2. ( ) Sí, en un 10%
3. ( ) Sí, en un 25%
4. ( ) Sí, en un 50%
5. ( ) No.

6.- ¿Cómo valoraría la posibilidad de emitir sugerencias respecto al funcionamiento de la herramienta de salvaguardo de la Información?

Nada importante	Poco importante	Medianamente importante	Bastante importante	Completamente importante
1( )	2( )	3( )	4( )	5( )

7.- ¿Qué percepción tiene sobre la eficiencia de la herramienta de salvaguardo de la Información en su empresa y las políticas que se desarrolla para aumentarla?

Ninguna	Escasa	Satisfactoria	Buena	Excelente
1( )	2( )	3( )	4( )	5( )

8.- Como calificaría de manera global la gestión de la Seguridad de la Informacion de su empresa.

Mala	Regular	Buena	Muy buena	Excelente
1( )	2( )	3( )	4( )	5( )

"Año de la Diversificación Productiva y del Fortalecimiento de la Educación"

UNIVERSIDAD NACIONAL DEL SANTA

OFICINA CENTRAL DE INVESTIGACIÓN

"CATÁLOGO DE TRABAJOS DE INVESTIGACIÓN - TRIPOS"

Resolución N° 1562-2006-ANR

REGISTRO DEL TRABAJO DE INVESTIGACIÓN

I. DATOS GENERALES (PRE GRADO)

- **UNIVERSIDAD:**
  UNIVERSIDAD NACIONAL DEL SANTA

- **ESCUELA O CARRERA PROFESIONAL**
  E.A.P. DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

- **TÍTULO DEL TRABAJO:**
  "IMPLEMENTACIÓN DE UN SERVIDOR TIVOLI STORAGE MANAGER PARA MEJORAR EL SALVAGUARDO DE LA INFORMACION EN LA OFICINA REGISTRAL CASMA DE LA ZONA REGISTRAL VII SEDE HUARAZ."

- **ÁREA DE INVESTIGACIÓN**
  OFICINA REGISTRAL CASMA DE LA ZONA REGISTRAL VII SEDE HUARAZ
- **AUTOR(ES)**
  DNI: 42440732
  APELLIDOS Y NOMBRES: TORRES ESPINOZA GERSON JULIO

- **TÍTULO PROFESIONAL A QUE CONDUCE:**
  Tesis Para Optar El Título Profesional de Ingeniero de Sistemas e Informática

- **AÑO DE APROBACIÓN DE LA SUSTENTACIÓN**
  2015

II. CONTENIDO DEL RESUMEN

- **PLANTEAMIENTO DEL PROBLEMA**

  La Oficina Registral de Casma que pertenece a la Zona Registral N° VII – Sede Huaraz, tiene como necesidad la acción de generar diaria, semanal y mensualmente respaldos de sus servidores presentes en el Centro de Datos, con respecto a base de datos y servidores de archivos, y 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 ha 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 cuentas 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.
- Perdida 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 institución.

- **OBJETIVOS**

  - **Objetivo General**
    Implementar un Servidor Tivoli Storage Manager para mejorar el salvaguardo la Información en la Oficina Registral Casma de la Zona Registral VII Sede Huaraz
  - **Objetivos Específicos**
    - Crear calendarios diarios, semanales y mensuales 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.
    - Administrar la herramienta haciendo que sea accesible desde la red interna a través de un acceso web y si lo solicita la Institución 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 crear sinergia.
    - Generar material de entrenamiento para que sea objeto de estudio y práctica dentro de la Oficina Registral de Casma.

- **HIPÓTESIS**
  "La Implementación de un Servidor Tivoli Storage Manager mejora el salvaguardo de la información en la Oficina Registral Casma de la Zona Registral VII Sede Huaraz

- **BREVE REFERENCIA AL MARCO TEÓRICO (10 A 20 LÍNEAS)**

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.

Características de TSM.
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
- Protección de aplicaciones
- Backup y recuperación
- Continuidad del negocio de nivel de servicio de Protección
- Reducción de datos
- Prepararse para una catástrofe
- Virtualización del almacenamiento
- Administrador de "Archives"
- Protección de los datos de oficinas remotas
- Gestión de Almacenamiento de Recursos
- Gestión Unificada de Recuperación.

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.

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.

- **CONCLUSIONES Y RECOMENDACIONES**

CONCLUSIONES

- Se demostró que a través de una planificación previa (calendarización) se puede administrar de una manera mucho más óptima el entorno de seguridad de la información, esto hizo ver a la gerencia cuán importante es la necesidad de estar a la vanguardia en tecnología para protección del activo más preciado.

- Se generó un registro de acciones realizadas. Esta especie de reporte es de vital importancia al momento de evaluar el comportamiento del servidor bajo la configuración actual, dadas las circunstancias también puede llevar a ajustarse las especificaciones iniciales con las que se configuró TSM. Gracias a la implementación ahora se tiene un registro periódico de todos los backups, restores y fallas suscitadas.

- Se demostró que la fácil administración hace que se pueda monitorear desde cualquier punto de la Red Sunarp. Debido a las restricciones de Seguridad, esta administración web es posible desde cualquier oficina, y si asi lo solicita Sede Central poder observar el comportamiento del flujo de backups de nuestra Zona Registral N° VII.

- Se implementó TSM, y se adecuó a las normas exigentes del SGSI que actualmente se viene plasmando en todos los procesos (administrativos y colaborativo) que SUNARP está estableciendo, por lo que, conjuntamente con la implementación realizada se elaboraron las políticas de respaldos que nuestra Zona debe manejar a fin de estar de acuerdo con el estándar que se viene aplicando en otras Zonas Registrales.

- Se realizó este documento lo que 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 demostró 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 el personal de la UTI de la Zona Registral N° VII genero un material de practica para que éste sea revisado como material de estudio y compartido con las demás Zonas Registrales que actualmente están trabajando bajo la arquitectura TSM.

RECOMENDACIONES

Al término del presente informe se recomienda lo siguiente:

- SUNARP, debe tomar en cuenta el presente estudio como base de la implementación con el propósito de mejorar el salvaguardo de la información en la Oficina Registral de Casma de la Zona Registral N° VII - Sede Huaraz, a fin de darle la seguridad jurídica que proclama brindar a sus usuarios.

- Tomar como base el estudio de la implementación y aplicarlo a cualquier Zona Registral que posea o no posea TSM para verificar su eficiencia y funcionalidad en este tipo de rubro de negocio

- Tomar como base la metodología empleada en esta investigación con el objetivo de ampliar el modelo teórico, incorporando nuevas variables o bien profundizando en algunas partes del modelo incluyendo un cuadro de mando y aplicarlo para evaluar su eficiencia y funcionalidad en la implementación de servidores TSM.

- **BIBLIOGRAFÍA**

- MAX ALONSO HUAMÁN (2009) Fundamentos de Sistemas de Respaldo de Información

- XAVIER MAURICIO REA PEÑAFIEL (2012) "Implementación de una de las Herramientas de Salvaguardo de Información para Sinergy Team Cia. Ltda."

- LÓPEZ LÓPEZ, ISVEL (2010) "Implementación de una solución de respaldos de información en la empresa Uniplex Systems en Quito"

- Manual de TSM (2014) IBM Tivoli Redbooks.

- 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.

- 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.