Universidad Nacional Autónoma de Nicaragua

Recinto Universitario Rubén Darío

Facultad de Ciencias e Ingenierías

Departamento de Tecnología

Ingeniería en Electrónica

Título

Optimización de los servicios telemáticos.

Subtítulo

Propuesta de implementación de respaldo en nube privada para data center de UNAN-MANAGUA.

Seminario de graduación para optar al título de Ingeniero en Electrónica.

Autor

- Br. Moisés Humberto Castellón Martínez.

Tutor: MSc. Ing. Edwing Quintero.

Managua, Nicaragua

Enero, 2013

Dedicatoria

Dedico este trabajo a mi familia por brindarme su apoyo incondicional estando presente en todo momento y enseñarme con su ejemplo, la necesidad de superación en todo momento.

A mis amigos por haber compartido todos estos años de estudio y a maestros por enseñarme todos los conocimientos necesarios a lo largo de estos últimos años.

Agradecimientos

Expreso mi agradecimiento a DIOS por dotarme de inteligencia y sabiduría necesaria para adaptarme y transformar tanto a nivel material como espiritual el mundo que me rodea, para beneficio mismo de la sociedad en que todos vivimos.

Así mismo, manifiesto gran agradecimiento a mi tutor de seminario de graduación y al asesor tecnológico, por sus acertadas orientaciones y su encomiable pasión por la enseñanza, necesarias para la exitosa culminación de este trabajo.

TABLA DE CONTENIDOS

INDICE DE FIGURAS Y CUADROS

Resumen

En los últimos años la explosión de aplicaciones, datos y servicios que manejan las instituciones obligan al centro de datos a adaptarse para responder a las necesidades ya que la mayoría de ellos no se construyeron para soportar el actual entorno de sistemas y servidores. Los cambios en los centros de datos son imparables y continuarán produciéndose para proporcionar flexibilidad.

El presente trabajo de seminario de graduación está orientado a proponer una implementación de respaldo en nube privada para el centro de datos de la Universidad Nacional Autónoma de Nicaragua (UNAN-MANAGUA) que mejore radicalmente la infraestructura de TI y así pueda adaptarse a las necesidades cambiantes de dicho data center.

Para iniciar el trabajo se realizó un análisis y diagnóstico de la situación actual de la tecnología y dispositivos implementados en el data center que permitió identificar los puntos más vulnerables los cuales reforzaría y mejoraría, de forma gradual, nuestra propuesta.

Se revisaron materiales de diversa índole (documentos, artículos científicos, libros electrónicos, *whitepapers*) con el objetivo de hacer un análisis y búsqueda de información. Con todo ello se procedió a la realización de entrevistas-Véase Anexo A- dirigidas al personal de los centros de datos (TIC y Ciencias Médicas), con las que se completó la gama de informaciones necesarias.

Se eligió, como propuesta, una solución de replicación de datos factible de acuerdo a las condiciones, y que permitiría sentar los fundamentos para que los servicios de nube privada sean adaptados. Finalmente se planteó la propuesta de nube privada y todos los componentes esenciales que conllevaría su implementación. Se destacan sus principales características y beneficios basadas en la infraestructura como servicio IaaS (enfoque de la propuesta), uno de los dos modelos de cómo puede implementarse una nube privada, con las que concluye el presente informe.

CAPITULO I. PLANTEAMIENTO DE LA PROPUESTA

1.1. Introducción

Un data center, centro de procesamiento de datos o centro de cómputos es una sala de procesamiento que aloja equipos activos montados en *racks* ó gabinetes interconectados con sistemas de procesamiento de datos, de almacenamiento y de comunicaciones y por supuesto, un sistema de cableado estructurado para interconectarlos. El propósito general de los data centers es alojar los equipos activos de datos en un entorno que satisface sus necesidades por potencia, telecomunicaciones, redundancia y copias de seguridad. Además, proporciona un entorno controlado respecto al manejo de la energía y la temperatura, posibilitando así que los equipos funcionen en un nivel óptimo con la máxima disponibilidad del sistema.

La capacidad de almacenamiento de información de un data center, relacionada con el almacenamiento basado en archivos, crece año con año a una tasa altísima. Para optimizar los costos de éste crecimiento de datos, manejándolos con adecuada prioridad y acorde clasificación, se hace necesario contar con un sistema de respaldo que satisfaga las necesidades de almacenamiento.

Un componente esencial de un data center son los servidores. El alto rendimiento de servidores se garantiza cuando la carga de trabajo se encuentra balanceada, esto permitirá asegurar que los recursos y las aplicaciones de importancia decisiva permanezcan disponibles. Es entonces cuando un clúster cumple un papel importante, un clúster es un grupo de sistemas independientes, conocidos como nodos, que trabajan como un sistema único para garantizarle al usuario la disponibilidad. La organización en clústeres permite a los usuarios y administradores tener acceso a los nodos y administrarlos como un sistema único en lugar de cómo equipos independientes. Claro está, llega un momento que servidores en clúster interno no es suficiente para proporcionar la alta disponibilidad que hoy en día requieren los centros de datos que están evolucionando y creciendo de manera agigantada.

La información es uno de los activos más importantes para la mayoría de empresas e instituciones. Y cada una de ellas tiene una necesidad fundamental de proteger los datos y mantenerlos disponibles, la UNAN-Managua no es una excepción. Un

pequeño fallo, algunas veces inesperado, puede destruir el esfuerzo de años de trabajo en un solo instante y una vez perdida ésta información es casi imposible recuperarla. Allí radica la importancia de tener respaldo, con estrategias cada vez más confiables, de toda la información y aplicaciones que posee gran valor y que esté expuesta a fallos informáticos, robos y hasta fallas en los dispositivos de almacenamiento.

Por todo lo mencionado anteriormente, se plantea en el siguiente trabajo la propuesta de respaldo en nube privada para el data center de la UNAN-MANAGUA, con el objetivo de ofrecer beneficios y servicios orientados a satisfacer grandes necesidades permitiendo optimizar procesos, disminuir costos de adquisición de nuevo hardware y aumentar la productividad. Para formular la propuesta se evaluarán tres productos de replicación de datos, tecnologías basadas en host (servidor), con el objetivo de seleccionar la solución más factible para el data center institucional.

1.2. Justificación

Con los recientes avances en tecnologías de información, se han presentado también nuevas aplicaciones para la Internet, en éste caso del modelo llamado computación en la nube. Esta resulta conveniente y rentable, el poder trabajar en la ¨nube¨ permite ahorros en licencias y administración de servicios, esto se debe, a la arquitectura conformada por capas con las cual trabaja, que corresponden al software, plataforma e infraestructura como servicios.

La infraestructura tecnológica del sector de tecnologías de información (TI) de la UNAN-MANAGUA está basada en servidores independientes constituida por un conjunto de equipos heterogéneos tanto en tecnología como en prestaciones.

El centro de datos informático existente está conformado por dos arquitecturas de almacenamiento de datos:

Almacenamiento DAS (almacenamiento de conexión directa) encontrada en los discos locales de cada servidor; almacenamiento SAN (red de área de almacenamiento) que conecta a los servidores y equipos de almacenamiento utilizando tecnología iSCSI (*internet small computer system interface*), que es una familia de protocolos para comunicaciones con dispositivos de almacenamiento.

La infraestructura actual no realiza respaldo de la información ni bases de datos de los estudiantes o mejor de dicho de la información crítica a la cual se debe tener acceso en todo momento por razones de continuidad servicios y por la vitalidad de la misma. Más aún, no se practica alguna estrategia de replicación de datos que aseguren alta disponibilidad de todos los servicios telemáticos y que permita la recuperación casi inmediata de la información y aplicaciones en caso de que sucedan fallos informáticos o de alguna otra índole.

Con todo lo anterior, se hace una propuesta de implementación de respaldo en nube privada que es un modelo para permitir el acceso por medio de redes de manera conveniente y según demanda a un pool compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con un mínimo esfuerzo de administración.

Este modelo de nube privada, permitiría que la UNAN-MANAGUA por medio de su data center gestione archivos y utilice nuevas aplicaciones sin necesidad de ser instaladas ni incrementar recursos de hardware obteniendo beneficios como tolerancia a fallos, continuidad de servicios, administración mejorada y reducción de costos porque con la virtualización del hardware se pueden controlar los flujos de trabajo de máquinas virtuales y distribuir el trabajo.

Además, en el centro de datos se ve la necesidad de almacenar, organizar y depurar toda la información generada por los servicios, bases de datos y aplicaciones y sobre todo que se pueda mantener y controlar el flujo de datos. Por ende, deben establecerse herramientas que permitan mantener actualizada de manera permanente, ágil y oportuna toda esa información.

Por último, se evaluarán tres estrategias de replicación de datos con el fin de seleccionar la estrategia de mejor rendimiento, económicamente viable, que cumpla los requisitos técnicos y que proporcione continuidad de los servicios informáticos entre el centro de datos institucional y el de la Facultad de Ciencias Médicas.

1.3. Objetivos

1.3.1. General

1) Proponer el respaldo en nube privada para garantizar la disponibilidad de datos y servicios telemáticos en la UNAN-MANAGUA.

1.3.2. Específicos

1. Hacer un diagnóstico de infraestructura de almacenamiento actual implementada en el centro de datos institucional del proyecto TIC.
2. Evaluar tres estrategias de replicación de datos entre el data center del centro informático y el data center de la Facultad de Ciencias Médicas que garantice la continuidad de los servicios informáticos.
3. Seleccionar la estrategia de replicación más fiable y compatible para la infraestructura de nube privada del centro de datos institucional del proyecto TIC.

1.4. Marco Metodológico

El tipo de investigación utilizada en el desarrollo de este trabajo de seminario de graduación es la de investigación y desarrollo.

A continuación se presentan las etapas que se siguieron para alcanzar los objetivos específicos de presente trabajo y que contribuyeron a alcanzar el objetivo general del mismo.

1. Identificar y analizar las tecnologías y dispositivos que permitan hacer un diagnóstico de la situación actual del centro de datos institucional.
    a. Se consultó bibliografía y artículos de internet para determinar cuáles son los dispositivos básicos que debe poseer un centro de datos.
    b. Se hizo una revisión e inventario sobre los equipos de telecomunicaciones existentes que permitieran hacer un diagnóstico.
    c. Se prepararon dos guiones de entrevistas con preguntas abiertas (que permitieron profundizar en los temas consultados), dirigidas a las personas que poseen alta relación a los centros de datos TIC y facultad de Ciencias Médicas.
    d. Se aplicaron las entrevistas y una vez obtenidos los resultados se analizaron y se realizó el tratamiento de variables.
2. Hacer evaluaciones de productos de replicación.
    a. Se consultó artículos de internet y revistas para ubicar herramientas de replicación más adecuadas para ser evaluadas.
    b. Aplicación de las herramientas.
    c. Análisis de los resultados obtenidos de acuerdo a las métricas de evaluación.
3. Proponer un producto de replicación.
    a. Según el análisis de resultados se eligió un producto de replicación que por sus características se adapte mejor al modelo de nube que se propone.
4. Formular propuesta de nube privada.
    a. Presentar los elementos esenciales para montar la nube privada.
    b. Consistencia del modelo de nube IaaS y beneficios para el centro de datos.

CAPITULO 2. DESARROLLO

2.1. Generalidades

Este acápite estará estructurado de forma que presente las bases de la propuesta, a medida que contempla todo el proceso que conllevó la elaboración del presente trabajo.

El siguiente diagrama mostrará la distribución del capítulo:

El siguiente trabajo de seminario de graduación se desarrolló en la UNAN-MANAGUA, universidad de referencia nacional que brinda ofertas académicas de un sinnúmero de carreras y cuenta con 14 de facultades en el Recinto Universitario Rubén Darío. El sector de tecnologías de información es clave fundamental en cuanto a implementaciones e innovaciones tecnológicas que ayudan a mejorar los procesos y servicios académicos, su mal funcionamiento podría comprometer la integridad de tales servicios.

El centro de datos ubicado en el sector de tecnologías de información y comunicaciones (TIC) se encarga de almacenar todos los datos de los servicios académicos que presta la universidad, sistema de información universitario (SIU), postgrado, normativas, informe de calificaciones en línea, correo electrónico universitario, bases de datos que almacenan toda la información de todos los estudiantes de todas las carreras, sitio web y plataforma virtual para cursos de diferentes materias.

El almacenamiento recibe una especial atención en el funcionamiento del data center, por lo tanto se hace necesario distinguir las formas de almacenamiento. La red de área de almacenamiento (SAN) es una red dedicada para interconectar servidores, arreglos de discos y equipos de respaldo. Una SAN se diferencia de

otros modos de almacenamiento en red porque realiza el acceso a los archivos a bajo nivel por medio de comandos SCSI.

La implementación de una red SAN proporciona la manera más racional de gestionar y administrar los dispositivos de almacenamiento de forma dedicada y especializada, tanto en plataformas homogéneas como heterogéneas, de forma escalable y segura.

Las peticiones de entrada/salida (I/O) hacen referencia a bloques o sectores de un dispositivo determinado. Los dispositivos de altas prestaciones son SCSI por lo que cualquier red que haya bajo una SAN deberá tener un protocolo que transporte los comandos SCSI entre clientes y dispositivos de almacenamiento. Para redes Ethernet se ha definido el protocolo iSCSI (internet SCSI).

En SCSI se definen dos términos importantes: *initiators* (clientes) y *targets* (servidores). Los *targets* están compuestos por unidades lógicas (LUN´s) que son las que ejecutan los comandos. Tanto clientes como servidores usan bloques descriptores de comandos para comunicarse.

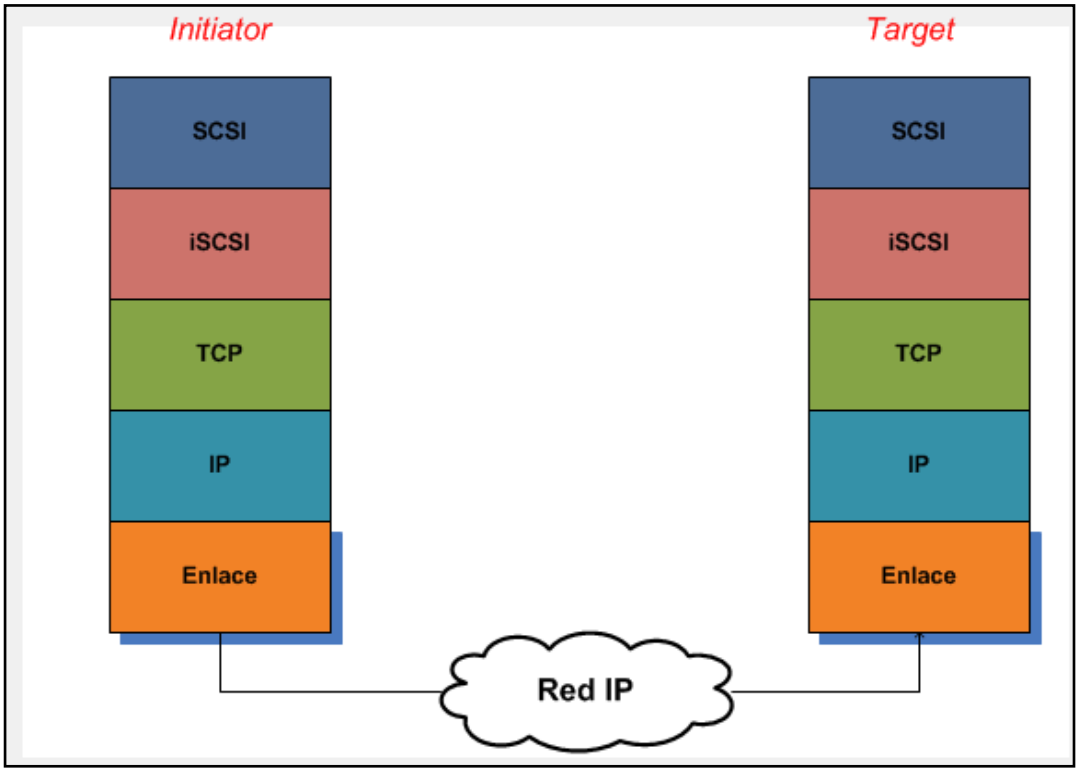

Figura 1. Modelo de capas con la inclusión de la familia de protocolos SCSI e iSCSI.

El almacenamiento es el proceso de guardar información en memorias de servidores o discos. Del almacenamiento de datos surgen dos modos: el respaldo (*backup*) y replicación. Se diferencian en que el respaldo son copias de seguridad (secundarias) de datos que por lo general se actualizan o sobre-escriben en base a

una programación periódica que puede ser una o dos semanas, según la frecuencia de cambios de la información. Mientras que replicación es la técnica de mantener las copias actualizadas de los datos y comúnmente se implementa para la recuperación ante desastres y asegurar la continuidad. Constituye una aproximación a las copias de seguridad. Además, es un mecanismo utilizado para propagar y diseminar datos en un ambiente distribuido, con el objetivo de tener mejor *performance* y confiabilidad, mediante la reducción de dependencia de un sistema de base de datos centralizado.

2.2. Diagnóstico de la situación actual del data center, dispositivos y la tecnología utilizada

Primero encontramos una de las partes fundamentales, los servidores. Contiene dos servidores HP *Proliant* DL380 G5. Es un conjunto de almacenamiento, memoria y herramientas de administración. Estos servidores se encuentran en inminente deterioro en relación con el tiempo de vida útil del mismo.

Tres servidores de almacenamiento *Dell PowerEdge serie 2950* denominados como Hyper-V2, Hyper-V3 y Hyper-V4, utilizados por su excelente disponibilidad y flexibilidad para gestión de base de datos. Aún con todo esto, proporcionan una capacidad de almacenamiento interno reducido en lugar de un sistema de almacenamiento externo. Posee seis compartimentos internos de unidad de disco duro proporcionando hasta 1,8 TB de almacenamiento interno que ayudan a ahorrar espacio en dicho centro de datos.

Todos los servidores se administran remotamente. Si son sistemas UNIX se administran mediante protocolo de órdenes seguras SSH (*Secure Shell*). Como todos los servidores son sistemas Windows entonces se administran por medio de escritorio remoto (*remote desktop*). Son operados con Windows Server 2008R2, por eso se denotan como hyper-V, que es una tecnología de virtualización basado en un *hypervisor* para los sistemas de 64-bits creado por Microsoft y que viene integrado en sistema operativo.

Figura 2. Modelo de servidores DELL PowerEdge serie 2950.

A continuación se presenta la tabla de direccionamiento de los servidores físicos que componen una de las partes esenciales de los equipos de telecomunicaciones del centro de datos institucional:

Tabla 1. Direccionamiento de los servidores del data center institucional.

Nombre	Modelo	O.S	Dirección IP	Máscara de subred	DNS	Nº de VMs
HYPER-V1.unan.edu.ni	ProLiant DL380 G5	Microsoft Windows Server 2008 R2	165.98.8.109 169.254.204.178 10.1.120.120	255.255.255.0 255.255.0.0 255.255.255.0	10.1.120.121	4
HYPER-V2.unan.edu.ni	PowerEdge R710	Microsoft Windows Server 2008 R2	10.1.120.129 192.168.131.1 172.16.0.2 169.254.3.92 169.254.247.78	255.255.255.0 255.255.255.0 255.255.255.0 255.255.0.0 255.255.0.0	10.1.120.121	13
HYPER-V3.unan.edu.ni	PowerEdge 2950	Microsoft Windows Server 2008 R2	10.1.120.135 192.168.132.1 172.16.0.3 169.254.1.14	255.255.255.0 255.255.255.0 255.255.255.0 255.255.0.0	10.1.120.121	4
HYPER-V4.unan.edu.ni	PowerEdge 2950	Microsoft Windows Server 2008 R2	10.1.120.140 10.1.120.71 192.168.133.1 172.16.0.4 169.254.2.245	255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.0.0	10.1.120.121; 10.1.120.2	5
Actasonline.unan.edu.ni	ProLiant DL380 G5	WS2008R2	10.1.120.141	255.255.255.0	10.1.120.2	-
DNS	PowerEdge 1850	OpenSuse 11.3	10.1.120.2	255.255.255.0	-	-

Tabla 2. Máquinas virtuales creadas en los servidores del centro de datos.

Nombre	S.O	Dir. IP	Máscara	DNS	Servidor físico	Descripción
Ads1.unan.edu.ni	WS2008R2	5.182.210.59 10.1.120.121	255.0.0.0 255.255.255.0	127.0.0.1	Hyper-V1	Controlador de dominio para unan.edu.ni y Active Directory
AVS.unan.edu.ni	WS2008R2	10.1.120.130	255.255.255.0	10.1.120.121 10.1.120.2	Hyper-V2	Servidor antivirus
DB1.unan.edu.ni	WS2008R2	10.1.120.126	255.255.255.0	10.1.120.121	Hyper-V1	Servidor web
DBS.unan.edu.ni	WS2008R2	10.1.93.254 5.179.125.253	255.255.0.0 255.0.0.0	10.1.120.121	Hyper-V2	Servidor de base de datos de producción
Mailbox1.unan.edu.ni	WS2008R2	10.1.120.106	255.255.255.0	10.1.120.121	Hyper-V4	Plantilla de VMs de servidor de correo Exchange
OWA.unan.edu.ni	WS2008R2	10.1.120.127 165.98.8.200	255.255.255.0 255.255.255.0	10.1.120.121	Hyper-V2	Plantilla de VM de servidor de correo Exchange
RDG.unan.edu.ni	WS2008R2	10.1.120.133 165.98.8.201	255.255.255.0 255.255.255.0	10.1.120.121	Hyper-V4	Servidor de *terminal services*
RDSH.unan.edu.ni	WS2008R2	10.1.120.122 165.98.8.152	255.255.255.0 255.255.255.0	10.1.120.121	Hyper-V2	Servidor de *remote desktop sesión host*
RDWA.unan.edu.ni	WS2008R2	10.1.120.128 165.98.8.151	255.255.255.0 255.255.255.0	10.1.120.121	Hyper-V2	Servidor de escritorio remoto acceso web
RS.unan.edu.ni	WS2008R2	10.1.120.211	255.255.255.0	10.1.120.121	Hyper-V4	Servidor de reporte de servicios
SP2010.unan.edu.ni	WS2008R2	10.1.120.224	255.255.255.0	10.1.120.121	Hyper-V3	Servidor de aplicaciones
EXHUB.unan.edu.ni	WS2008R2	10.1.120.132 165.98.8.202	255.255.255.0 255.255.255.0	10.1.120.121	Hyper-V2	Plantilla de VMs
unanvirtual.unan.edu.ni	Opensuse 11.3	10.1.120.33	255.255.255.0	10.1.120.121	PowerEdge	Servidor de UNAN-virtual

Para completar el conjunto de servidores solo se encuentra el servidor DNS (servidor de nombres de dominio) tal como se mostró en la tabla anterior. Con el servidor DNS sucede algo interesante, todas sus zonas configuradas y almacenadas se replican propiamente en dicho servidor local, además que se replican hacia el servidor remoto ubicado en el proveedor de servicios.

Después encontramos la SAN (red de área de almacenamiento) iSCSI *Powervault* MD3200i cuya característica principal es su diseño de almacenamiento para el rendimiento, alta disponibilidad y expansión accesible a través de la red Ethernet. La SAN del centro de datos se utiliza para conectar los servidores y los arreglos de discos basado en la tecnología iSCSI.

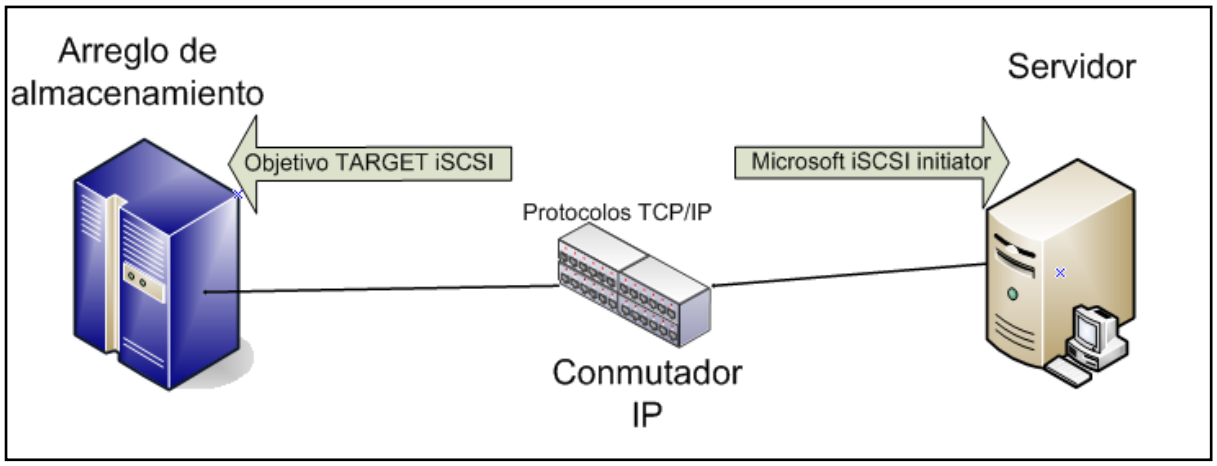

Figura 3. Componentes iSCSI cliente/host. Muestra el proceso de cómo se administra el almacenamiento desde el servidor por medio del protocolo internet SCSI integrado como un rol en Windows Server 2008 R2.

Es posible configurarla en niveles RAID 0, 1, 10, 5 y 6. En el centro de datos se encuentra configurada en nivel RAID 10. La SAN posee compartimentos (bahías) de más de 10 discos SAS (*serial attached SCSI*) de 3.5" que pueden ser de diferentes capacidades:

Cuatro espacios para discos de capacidad de 1 TB con velocidades de 7200 rpm, un espacio para disco de 6GB de RAM con 500 GB de capacidad a 7200 rpm y 5 espacios para discos de 600 GB a 15000 rpm. Esto indica que posee una amplia variedad de accionamiento de disco. El uso y distribución de la SAN se resume en la siguiente tabla:

Tabla 3. Descripción de la distribución de los discos de almacenamiento de la SAN.

Grupo de discos	Tamaño (GB)	Velocidad disco	N° disco
Diskgroup1	1862.03	7K RPM	Discos 2,3,4
Diskgroup2	465.26	7K RPM	-
Diskgroup3	1116.824	15 RPM	Discos 1,5,6

Es notable decir que es compatible con varios sistemas operativos; Windows, Linux, VMware e Hyper-V, siendo este último el que emplea la SAN del centro de datos institucional.

El rendimiento de la SAN está directamente relacionado con el tipo de red que utiliza, entonces entre mayor sea el ancho de banda mayor será la cantidad de conexiones de acceso. Se le denomina SAN Gigabit porque trabaja con una red Gigabit Ethernet.

La SAN iSCSI MD 3200i está diseñada para compañías que están en el espacio de empresa pequeña/media (SME, del inglés *small & medium enterprises*), para lo cual la replicación de datos (DR) en grandes volúmenes no es posible, es más que un desafío y aunque acompañado de virtualización (que reduce costos) pero la falta de replicación todavía estará allí.

Figura 4. Vista frontal de un arreglo SAN iSCSI MD 3200i.

A continuación se muestra el esquema de la red SAN y los equipos y dispositivos que la acompañan para completar el proceso de almacenamiento y acceso a la información que se lleva a cabo en el centro de datos.

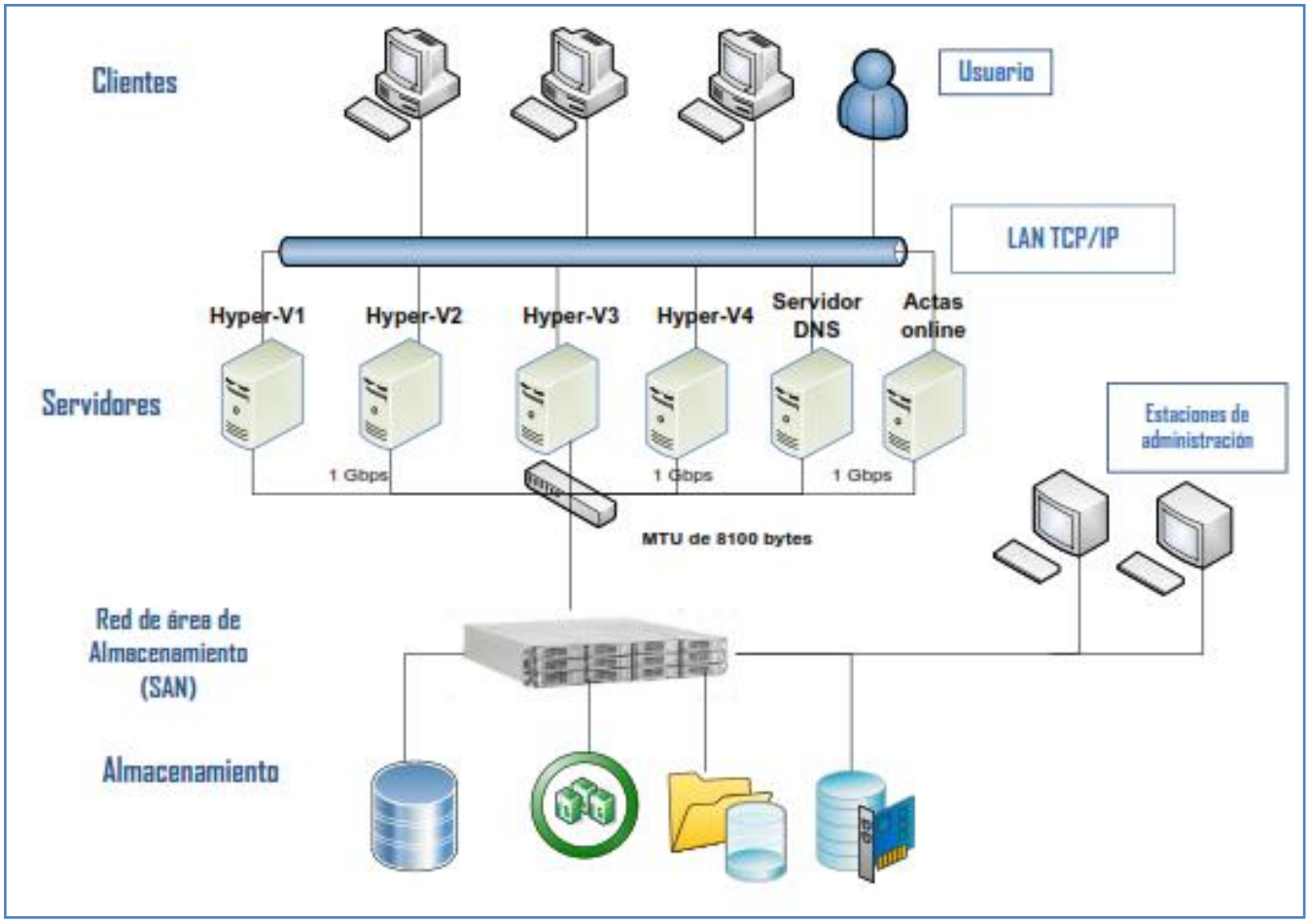

Figura 5. Esquema de la red SAN implementada en el data center y dispositivos de almacenamiento e interconexión.

En el esquema se puede observar los elementos que componen a la red SAN del data center: una red de alta velocidad (Gigabit Ethernet), equipo de interconexión dedicado (*switch* que realiza la conexión entre los servidores y la SAN) y los elementos de almacenamiento de red. La SAN juega un rol importante y es el de liberar a la red de la carga de almacenamiento al mismo tiempo que permite compartir los datos entre varios equipos de la red. Es importante saber que esto no afecta el rendimiento de dicha red porque el tráfico SAN está totalmente separado del tráfico de usuario. Son los servidores de aplicaciones (capa servidor) que funcionan como interfaz entre la red de datos y la red de usuario.

La comunicación cliente/servidor se hace por medio de la red IP (LAN TCP/IP). En la parte de comunicación SAN/servidores, denominada subred, en la capa 2 (capa de red) se eleva el valor de MTU (del inglés *maximum transmission unit*) a 8100[1] bytes para garantizar mayor acceso y evitar la fragmentación de paquetes. Este valor MTU se define tanto en la SAN como en los servidores. Todo esto es permitido por los enlaces de conexión de 1 Gbps.

[1] Normalmente se configura con un valor de 1500 bytes por defecto.

Como segundo punto encontramos la parte de red del centro de datos. Estos son los equipos de interconexión dedicados. Está conformada por cinco switches Catalyst 2970 series. Proveen configuraciones FastEthernet y Gigabit Ethernet con servicios inteligentes tales como seguridad para proteger información confidencial, alta disponibilidad, escalabilidad para adaptarse a crecimiento futuro y control de flujos de tráfico.

Figura 6. Vista trasera de switch 2970 catalyst series.

Luego se tiene un enrutador de servicios integrados cisco 800 series que provee conexión al ISP (proveedor de servicios de internet, en dicho caso es AMNET) y otro enrutador cisco 2800 series que provee servicio para acceso inalámbrico (Wi-Fi).

En ésta parte de red se da la distribución a otros sectores del recinto por medio de fibra óptica que permite altas velocidades de transmisión. Todas las conexiones se hacen desde un bastidor de distribución de Ethernet.

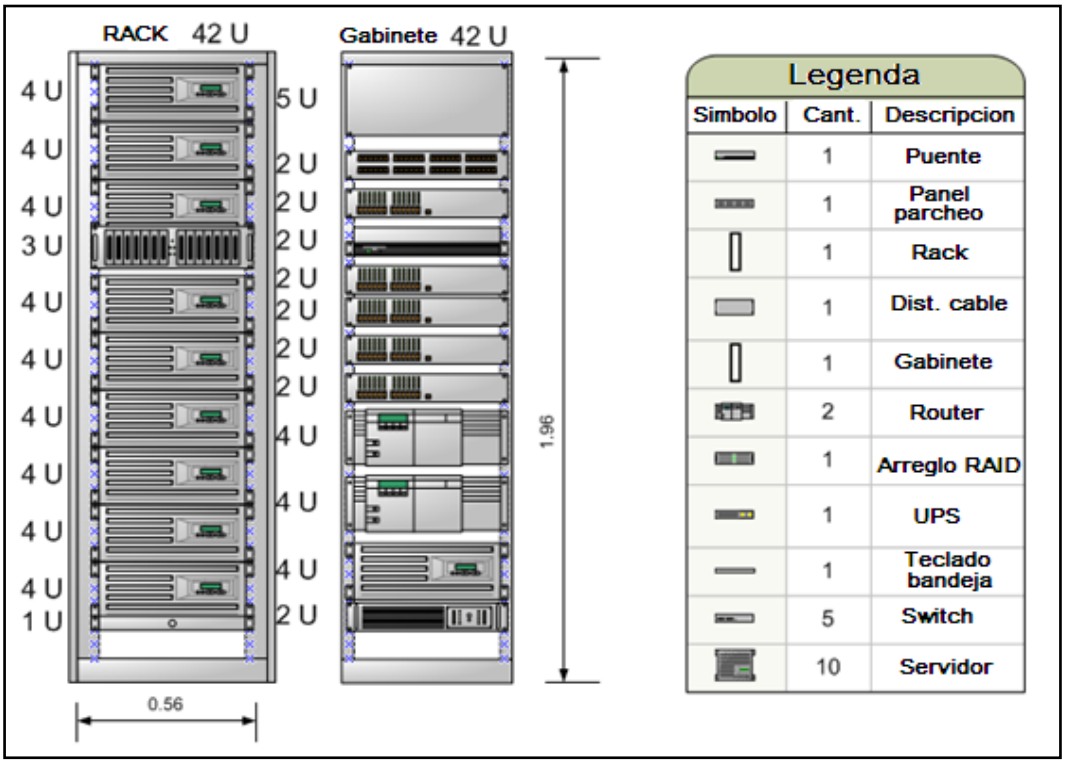

Figura 7. Diagrama de bastidor de los equipos existentes en el centro de datos.

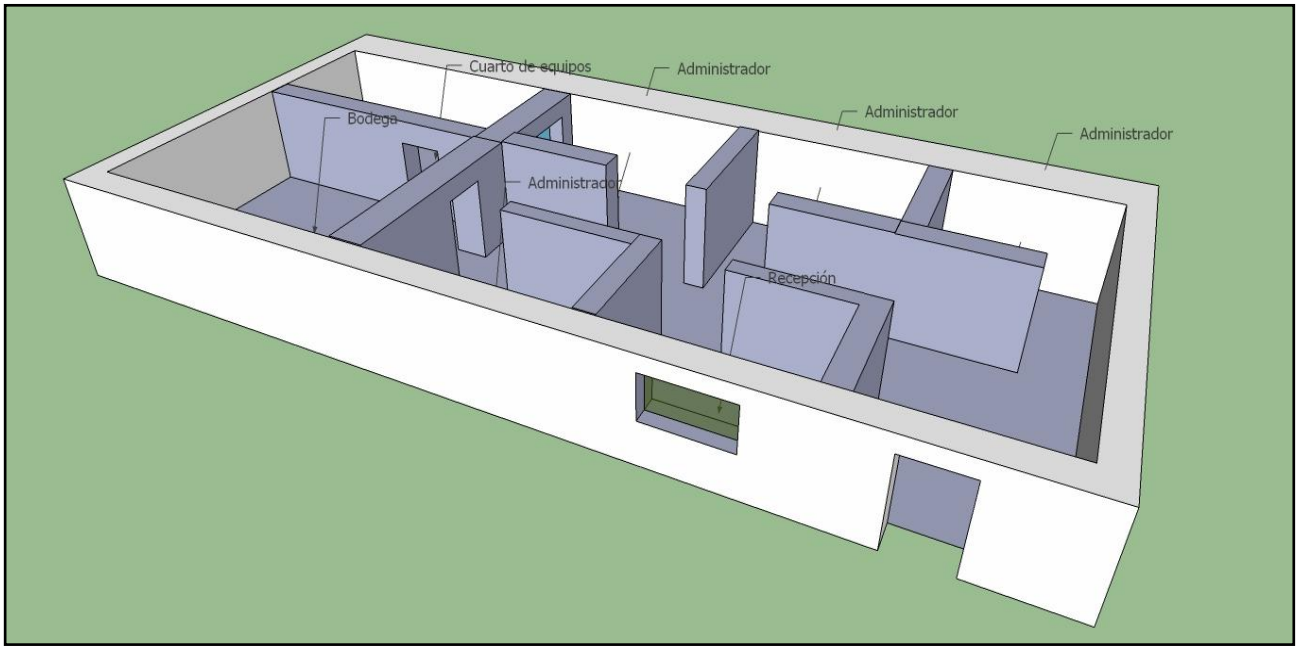

Figura 8. Vista interna/externa del centro de datos institucional.

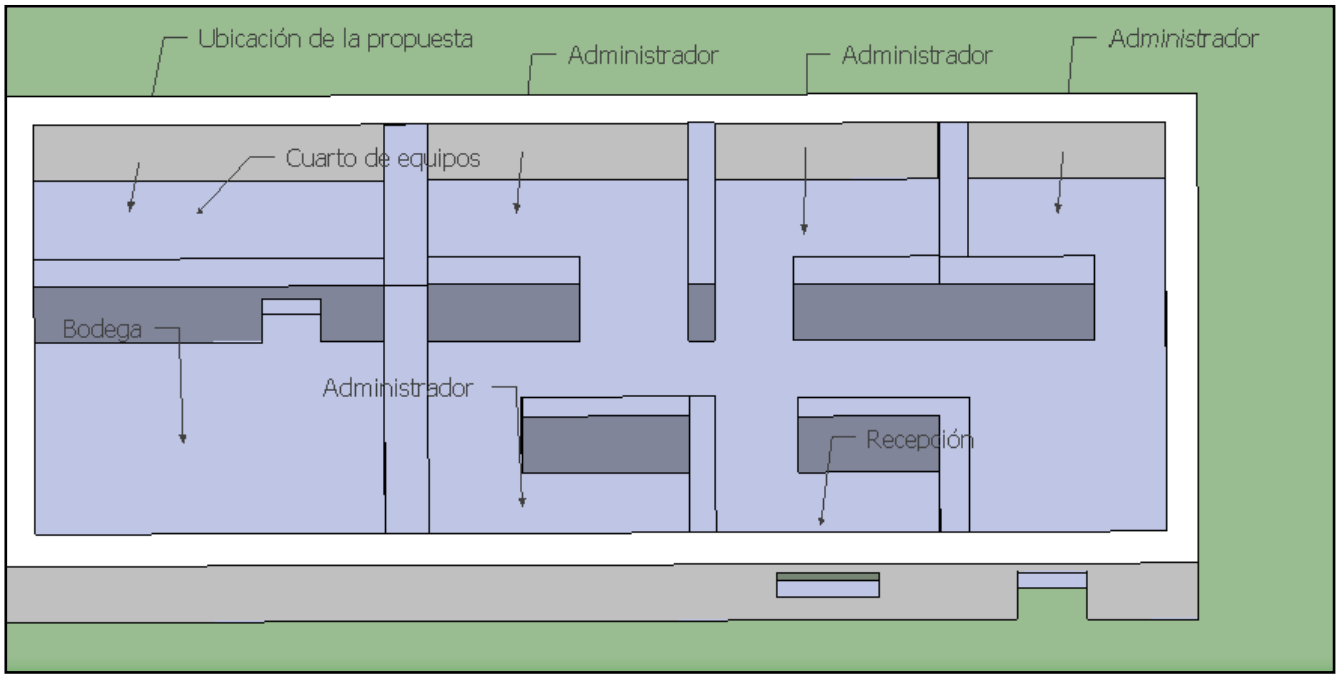

Figura 9. Vista superior con la distribución de cuartos del data center de UNAN-MANAGUA.

Otro aspecto importante es la calificación del centro de datos según los estándares establecidos a nivel internacional.

El estándar TIA-942, aprobado por TIA [2] y ANSI, brinda los requerimientos y lineamientos necesarios para el diseño e instalación de centro de datos, es decir, ofrece una norma de infraestructura de telecomunicaciones para centros de datos que orienta sobre el diagrama de distribución del centro. Entre los requerimientos que se definen en éste estándar se encuentran: estructura, ubicación, acceso, protección contra incendios, equipos y redundancia. Según todo esto, se define un modo de clasificar a los centros de datos de acuerdo a su desempeño, disponibilidad y confiabilidad en cuatro niveles denominados TIER´s que se mencionan a continuación:

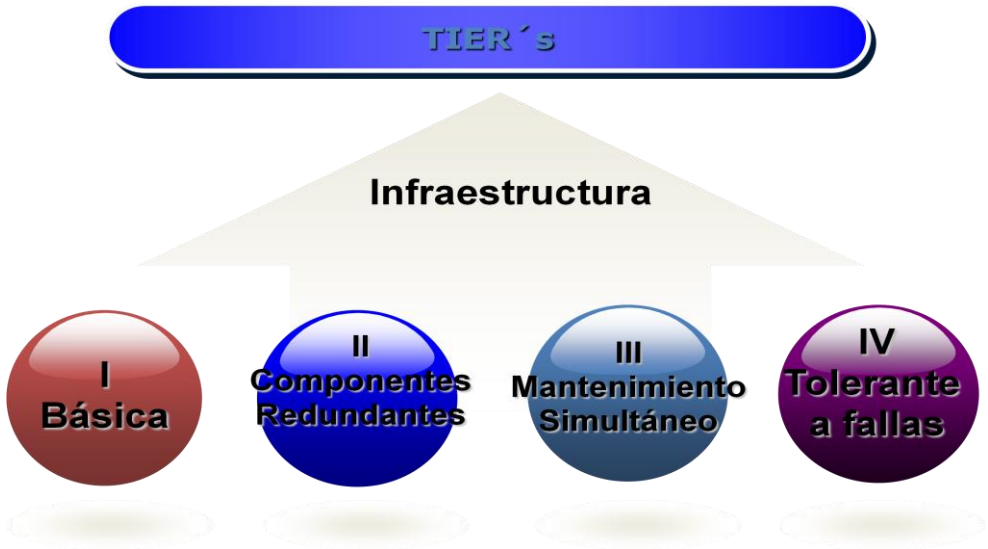

Ilustración 1. Niveles TIER´s elaborados por *uptime institute, Inc.* que definen el desempeño de acuerdo a la disponibilidad y confiabilidad de los centros de datos.

Podemos ver que según ésta clasificación, entre mayor es el numero más confiable es el sistema.

A continuación se presenta las áreas funcionales claves del diagrama de distribución según la norma:

- Uno o más cuartos de entrada.
- Área de distribución principal (MDA, de *main distribution area*).
- Una o más áreas de distribución horizontal (HDA).
- Un área de distribución de zona (ZDA).

[2] *Telecommunications Industry Association,* asociación líder representante de fabricantes y suministradores de redes globales.

- Un área de distribución de equipos.

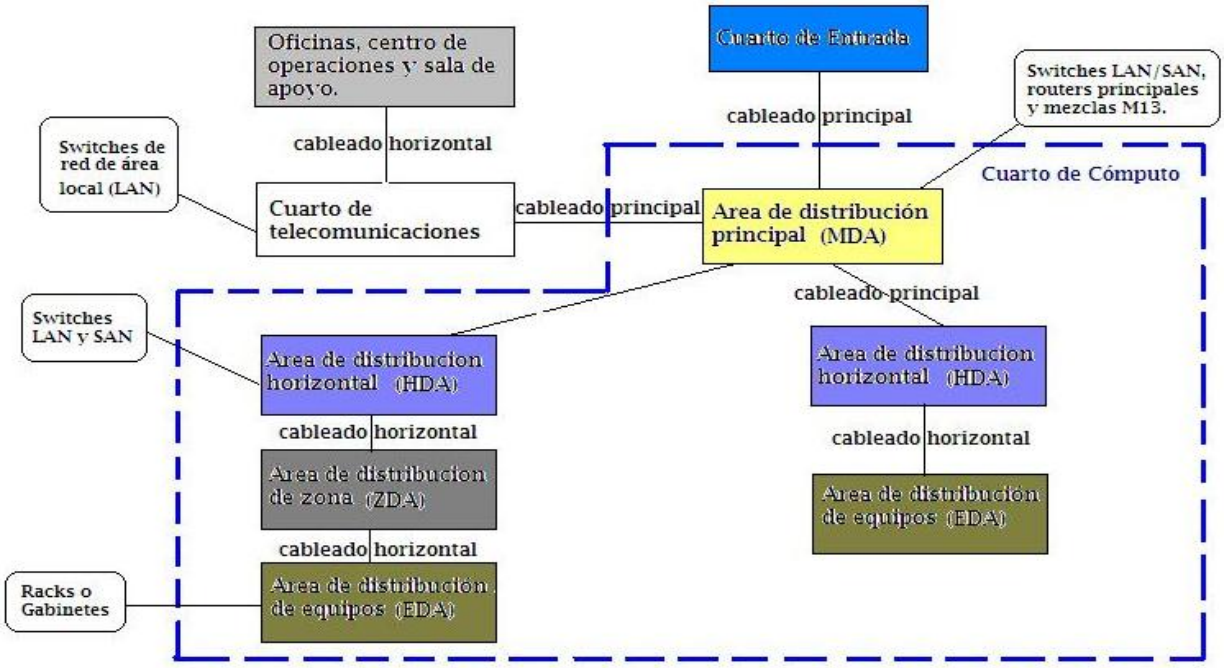

Figura 10. Diagrama de distribución y estructura de centro de datos según TIA-942.

Si bien no se trata este complejo tema en su totalidad, a grandes rasgos existen muchos aspectos que deben abordarse para que un centro de datos entre en la calificación de niveles. No obstante, cuatro son los aspectos principales: arquitectónico, telecomunicaciones, eléctrico y mecánico. El aspecto de telecomunicaciones es el de más interés para nuestro tema.

En el aspecto de telecomunicaciones existe algo muy importante denominado tolerancia a fallos, lo cual es posible al tener redundancia de equipos y dispositivos en el centro de datos. Dicha tolerancia requiere para su implementación que el sistema de almacenamiento guarde la misma información en más de un componente de hardware o en una máquina o dispositivos externos a modo de respaldo. A continuación se muestra un esquema de tolerancia a fallos si se practicara en el data center institucional:

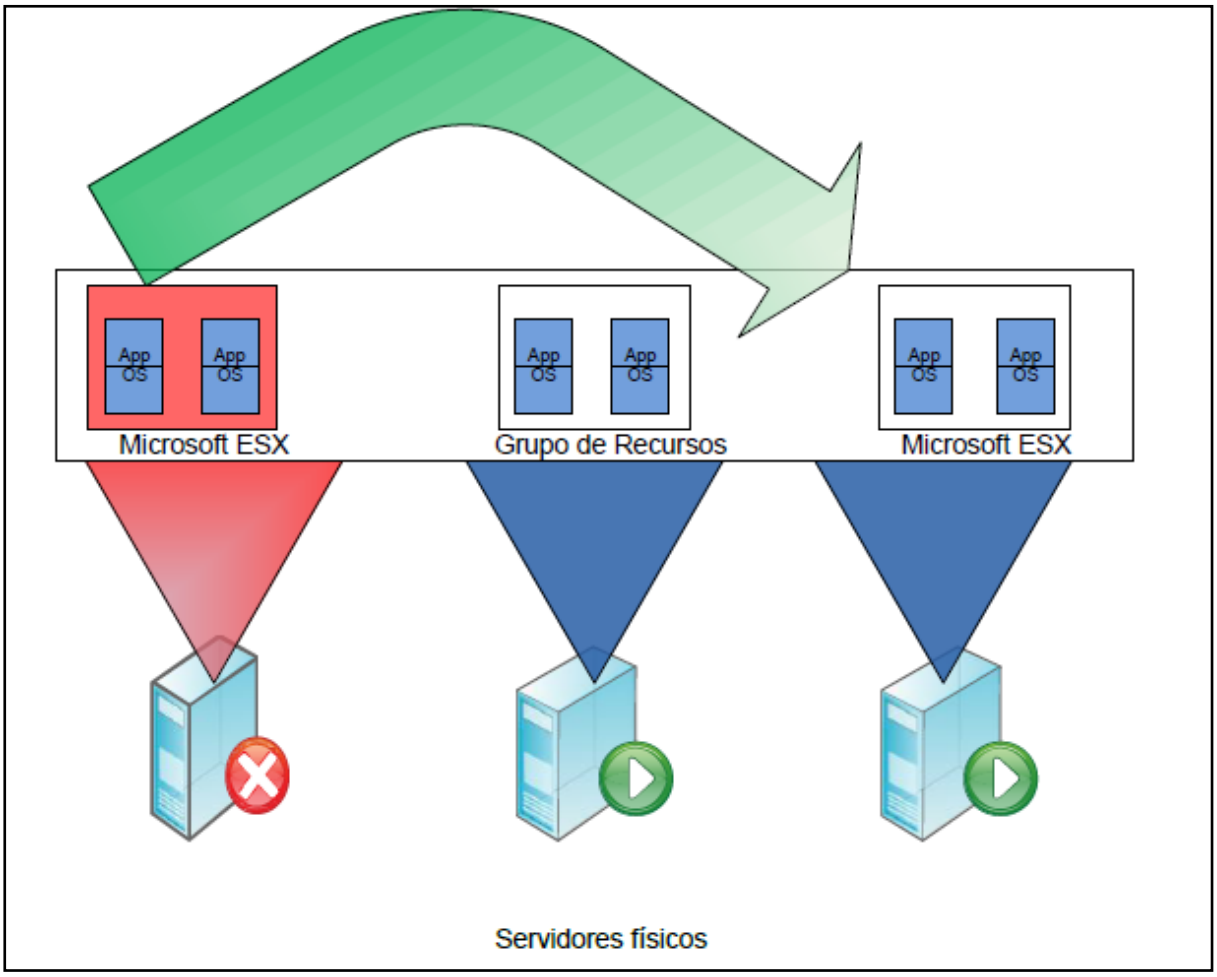

Figura 11. Esquema de trabajo con tolerancia a fallos por la redundancia de equipos.

2.2.1. Resultados y observaciones

Así, al realizar una inspección específica en el centro de datos se encontró que está calificado en el nivel de **TIER I** por los aspectos que se mencionan a continuación:

1. No posee componentes redundantes.
2. Única vía de distribución no redundante y una sola ruta de cableado.
3. En caso de que se produce una falla en un componente o en la distribución impacta el funcionamiento de los sistemas de cómputo.
4. Se cuenta con una infraestructura susceptible por cualquier evento (mantenimiento) planeado o no planeado.
5. Buena administración de cables, al utilizar rack y gabinete que brinda un amplio control de cables, tanto horizontales como verticales.
6. Sin protección de datos e información ante eventos físicos, naturales o accidentales. Es decir:
    a. No existe tecnología de replicación de datos (DR), que permiten asegurar la continuidad de la organización, específicamente del centro de datos.

b. No realiza respaldo local (*backup-on-site*) ni fuera de él (*cloud backup*) lo que no garantiza la disponibilidad de los servicios telemáticos brindados por la universidad. Este es un punto muy vulnerable teniendo en cuenta el grado de importancia que el almacenamiento de datos e información representan para la institución.
c. En cuanto a dispositivos de almacenamiento, la SAN existente en el centro de datos no permite replicar más de cuatro máquinas virtuales, lo que reduce la capacidad de establecer una tecnología de replicación basada en la red de área de almacenamiento. Es decir, no tiene replicación en grandes volúmenes de datos. Además posee una escalabilidad modesta que consecuentemente disminuye ambos, el desempeño *(performance*) y capacidad en el rendimiento de la red.

Se identificaron riesgos de tipo tecnológico y ambiental. Esto se traduce como un potencial de que un incidente no deseado pueda producir daños en la información. Es decir, en el caso de que el centro sufriera un accidente natural (desastres o fenómenos naturales) o accidental (fallo de los dispositivos de almacenamiento, corrupción del sistema u error operacional) sería imposible la recuperación de los datos o bien llamado en el campo *disaster recovery.*

Cabe mencionar que al establecer una tecnología de replicación y realizar respaldo en sitios externos, propuestas principales de este trabajo, se lograría que el data center institucional ascienda al nivel **TIER II** porque se brindaría protección de datos e información a eventos de mediana escala, alta disponibilidad y tolerancia a fallos, tal como se describió antes y que son los aspectos más relevantes y destacables del nivel II.

2.3. Soluciones de replicación entre el centro de datos institucional y Facultad de ciencias Médicas.

En éste inciso se tratará sobre la replicación de datos para asegurar la continuidad ante desastres, ya sean estos accidentales o naturales, se evaluarán tres productos de replicación de datos con el objetivo de brindar alternativas de solución ante la falta de replicación de datos del data center institucional.

Como se dio a conocer en el subcapítulo anterior, el centro de datos no posee un plan de contingencia o plan de continuidad del negocio (BCP, del inglés *business continuity plan*). Dicho plan se entiende como un conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los procesos que se realizan en el data center generando un impacto mínimo ante un incidente o desastre.

El plan BCP debe responder a preguntas como:

a) ¿Cuál es el impacto asociado a un desastre?
b) ¿Cuánta pérdida información puede ser tolerada?
c) ¿Cuáles son las alternativas?
d) ¿Cómo restablecer las funciones de los servicios?
e) ¿Contra qué tipo de "desastre" de pérdida de datos se necesita proteger los datos?

Todos estos cuestionamientos aún están sin responder lógicamente. Pero la última pregunta nos permite valorar cuáles son las causas más frecuentes de pérdidas de datos. Podemos observarlo en el siguiente cuadro:

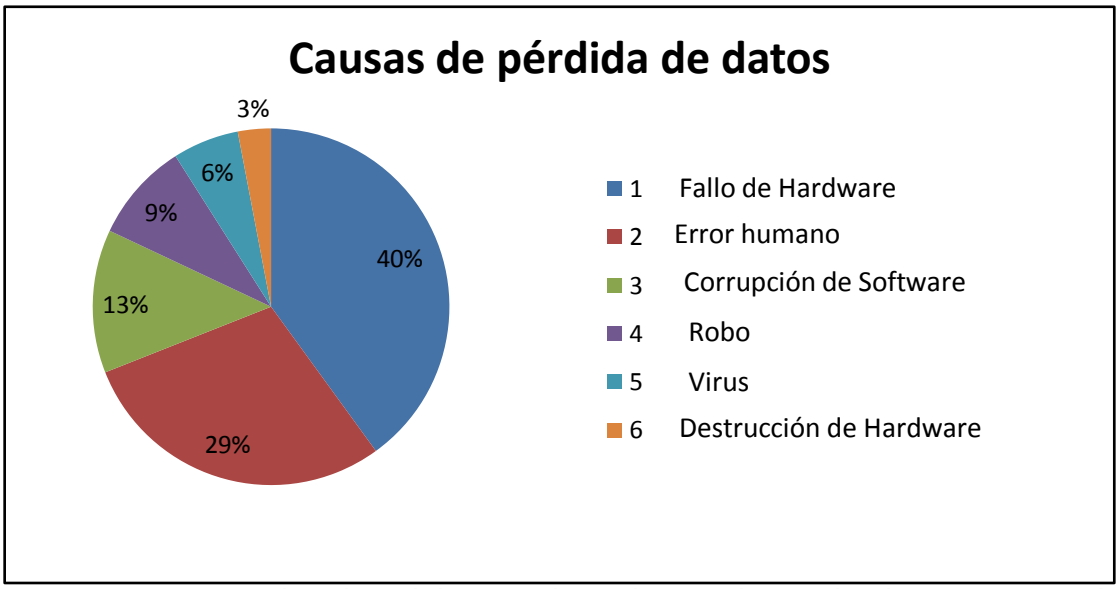

Figura 12. Fuente: Estimados del autor basado en datos desde Safeware, the insurance agency, Inc, "2000 safeware loss study," 2001; y ONTRACK Data International, Inc; "Understanding Data Loss," 2003.

Para evaluar una estrategia de continuidad (replicación) es necesario hacer un análisis de impacto (BIA) que contempla los siguientes aspectos: objetivo tiempo de recuperación (RTO), objetivo punto de recuperación (RPO) y recursos mínimos para operar. A saber, la replicación es la técnica más eficiente para reducir el RTO y el RPO para lograr la recuperación en caso de desastre o algún incidente que pueda presentarse.

Con el RPO debemos estar claros qué tan actualizados necesitan estar los datos y el RTO nos permite valorar cual es la tolerancia a la no disponibilidad.

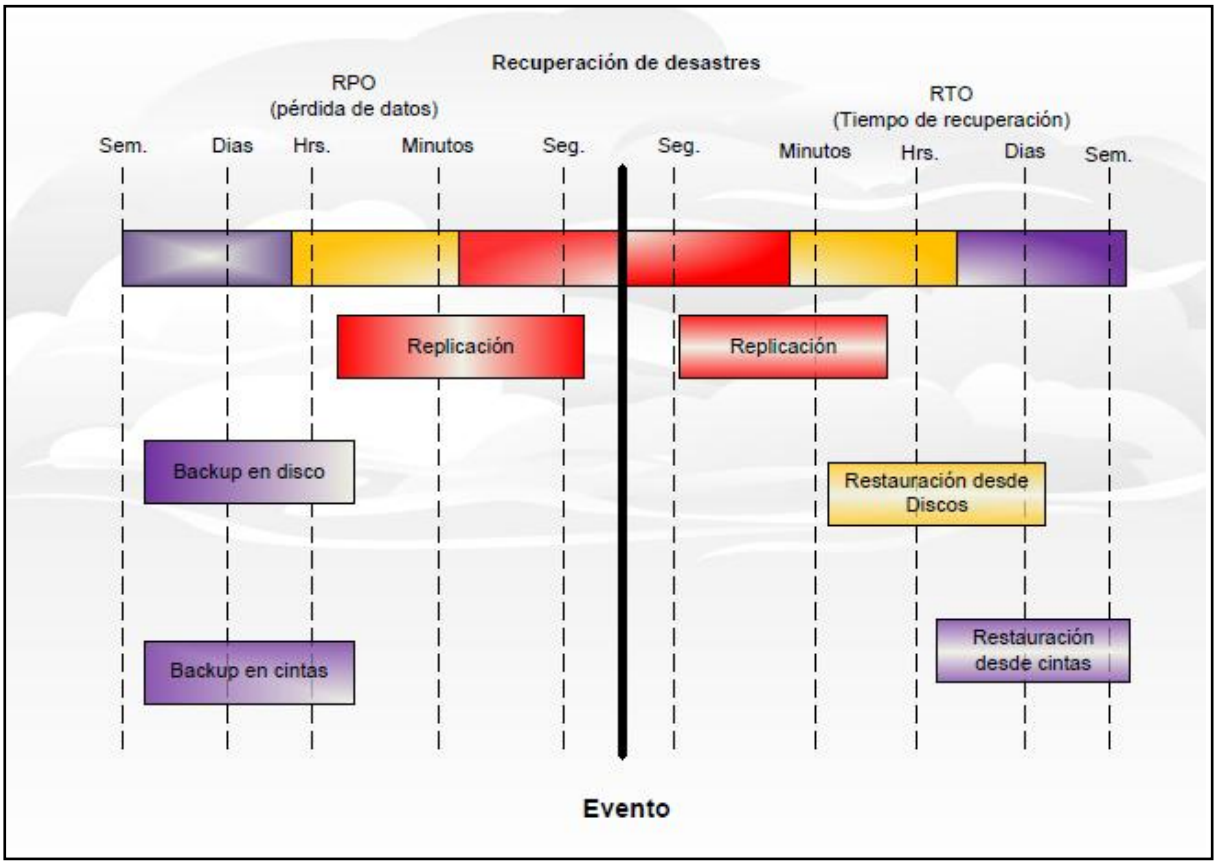

Figura 13. Cuadro comparativo de RPO y RTO para diferentes técnicas de recuperación.

Como se pudo observar en la figura anterior, se ilustra diferentes técnicas de recuperación de datos. La variable a medir es el tiempo y la técnica más efectiva es la replicación tanto para RPO como para RTO.

Así, la replicación es una tecnología clave y normalmente trabaja con la virtualización de servidores y la "nube" para desempeñar su función de recuperación ante desastres. Esto es importante porque la ejecución de una tecnología de replicación sienta las bases para que pueda implementarse el respaldo en la nube privada. La estrategia de replicación se debe producir entre una ubicación de

almacenaje primario y una segunda ubicación externa. Es por ésta razón, que se propone la replicación entre el centro de datos del TIC y el centro de datos de la Facultad de Ciencias Médicas.

El centro de datos de la Facultad de Ciencias Médicas posee una infraestructura de equipos similares al data center institucional. En general y de forma básica, su infraestructura está conformada por los siguientes dispositivos:

- ☑ Servidores de virtualización Dell PowerEdge R720.
- ☑ Arreglo de almacenamiento SAN iSCSI 3220i.
- ☑ Servidor Dell PowerEdge R310 II.
- ☑ Almacenamiento NAS NX 3500.

Este hardware, como veremos más adelante, es independiente de las tecnologías de replicación que se evaluarán, lo cual no se traduce como una limitante.

2.3.1. Productos y tecnologías de replicación

Existen varios factores para determinar y evaluar que producto de replicación de datos es mejor para el entorno en el que se desea implementar. Primero, se presentan dos tipos de producto o "modos" de replicación: los síncronos y asíncronos.

Vamos a profundizar un poco en replicación asíncrona y síncrona puesto que es esencial conocer la diferencia monumental de estos dos modos de replicación. Cuando los datos se replican sincrónicamente, los hosts sólo reciben una respuesta de escritura completa del almacenamiento cuando se ha validado la escritura de E/S (entrada/salida) en las ubicaciones locales y remotas. Es decir, el almacenamiento local y el remoto deben implementar el cambio antes de que se confirme que la escritura se ha realizado correctamente en el host. Por el contrario, en el modo asincrónico, el host recibe una escritura completa del almacenamiento cuando la escritura se ha validado en el sitio de almacenamiento local, sin que sea necesario esperar la confirmación de que la réplica también se ha actualizado en el sitio de almacenamiento remoto.

Así, cuando se implementa replicación asincrónica se deben tener los siguientes cuestionamientos:

i. Pérdida de datos, que depende de la frecuencia de la replicación de datos.
ii. Integridad de los datos. Tiene que ver con el mantenimiento del orden de la escritura.
iii. Impacto en el rendimiento, se debe evaluar cuanta degradación se produce en el rendimiento.

Con la replicación sincrónica se reduce en gran manera la latencia de escritura y se debe valorar el rendimiento en dependencia de la distancia de la replicación, el ancho de banda del vínculo de replicación y por supuesto, la utilización.

Luego tenemos el tipo de tecnología de replicación, se debe utilizar de acuerdo a las necesidades y características. Así, encontramos tres tecnologías: replicación basada en host (servidor), replicación basada en SAN (red) y por último la basada en arreglo de discos (*disk-array based*). De éstas, las mejores son las basadas en hardware pero son las más costosas para medianas y pequeñas empresas.

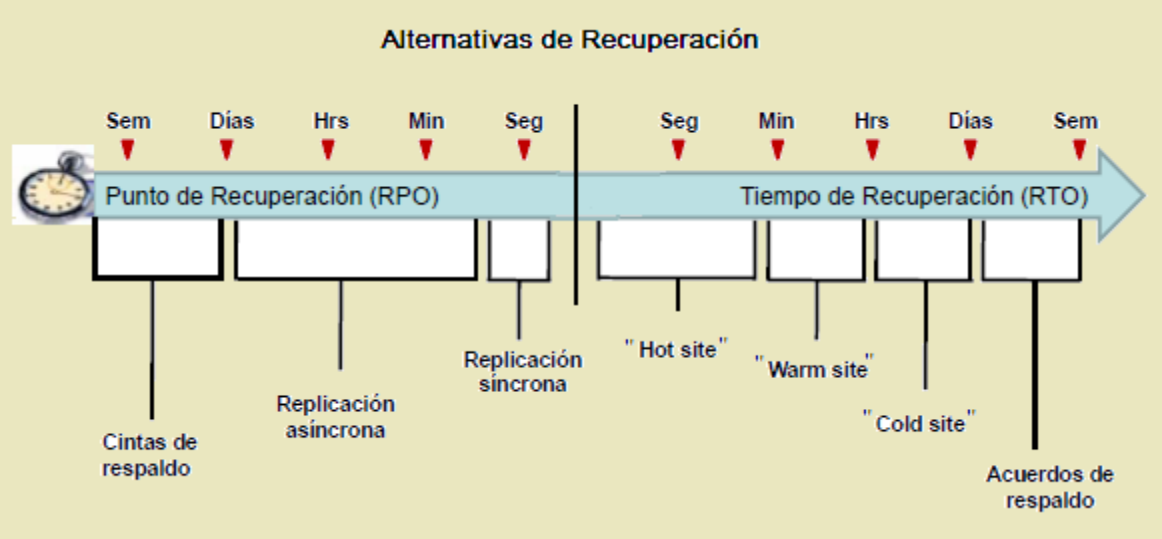

Figura 14. Característica del RPO y RTO de acuerdo al tipo de producto de replicación y sitios de recuperación externos.

Asunto crítico

El área metropolitana de Managua, sede de los campus principales de la UNAN-Managua tales como el Recinto Universitario Rubén Darío (RURD y otros recintos, se encuentra en una zona sísmica. Además la institución también tiene que prepararse para la gama completa de los riesgos de desastres (naturales-accidentales) como las que ya se han mencionado con anterioridad.

Por lo tanto, las preocupaciones de continuidad del "negocio" son fundamentales para esta institución universitaria. Obviamente, protegiendo la disponibilidad de los datos críticos y las aplicaciones que los gestionan es un componente importante para los planes de recuperación de desastres.

A pesar de aún no haber tenido que hacer frente a un desastre, no es necesario tener que esperar a que un desastre suceda antes de actuar. En particular, la institución necesita garantizar la recuperación de sus activos de información críticos, incluidos los recursos humanos y datos de los estudiantes.

2.3.2. Solución de replicación con *Hyperoo Software*

Hyperoo es una herramienta/aplicación orientada para sistemas basados en plataforma Microsoft y creado para resolver todos los problemas de respaldo de Hyper-V. Su funcionamiento es sencillo. Este software toma un *snapshot* [3] programado de los hosts virtuales corriendo hyper-V de Windows Server 2008 R2, encripta los datos y transfiere los hosts virtuales de forma segura sobre la conexión de red. Hyperoo es muy rápido, puede respaldar una máquina virtual de 100 GB en tan solo minutos.

Hyperoo es una forma económica pero efectiva ya que realiza respaldos diferenciales y también suporta ambos, restauración de datos completa (*full*) y diferencial.

2.3.2.1. Escenario de prueba con Hyperoo

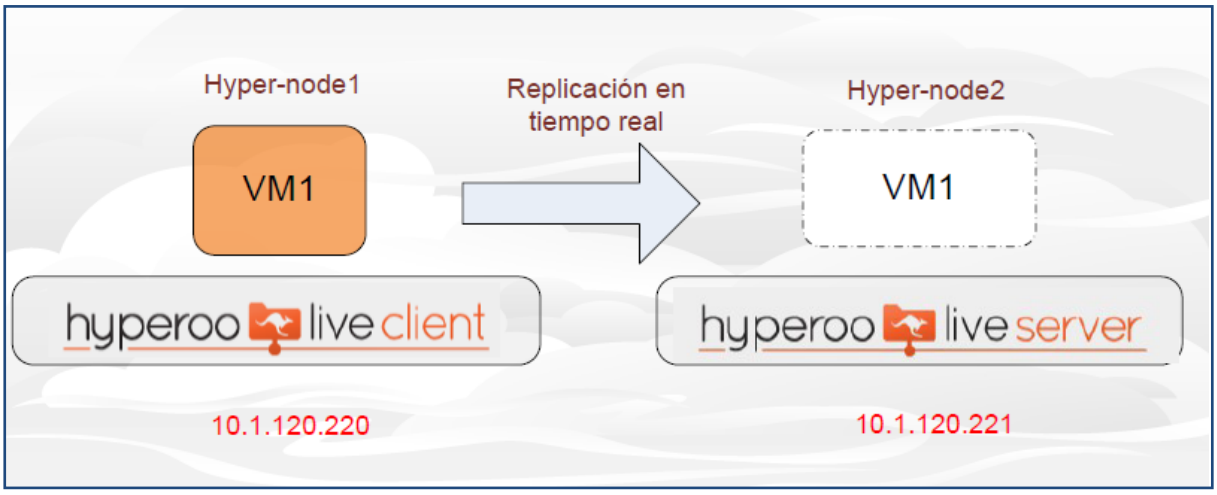

Figura 15. Escenario montado para realizar replicación con software Hyperoo.

La figura representa el escenario que se montó con dos nodos utilizando Windows server 2008 R2 y el rol Hyper-V para la creación de máquinas virtuales. Los componentes de Hyperoo son los siguientes: *Hyperoo managment console, Hyperoo client, Hyperoo server y Hyperoo restore*. Los componentes a instalar son opcionales y depende de los objetivos que se quieren lograr. Para nuestras pruebas se instalaron los *client/server* y la consola de administración con una versión de prueba ya que es un software licenciado.

Una vez instalados los componentes seleccionados se procede a la configuración de un respaldo, esto es crear una arreglo de respaldo (*backup array*) en el Hyperoo server. Se crea un nuevo arreglo haciendo click en “add array” en la ventana de la consola de administración de Hyperoo como se muestra en la siguiente figura:

[3] Snapshot o *copia instantánea de volumen*. Es una función de algunos sistemas que realizan copias de seguridad de ficheros almacenándolos tal y como fueron capturados en el pasado.

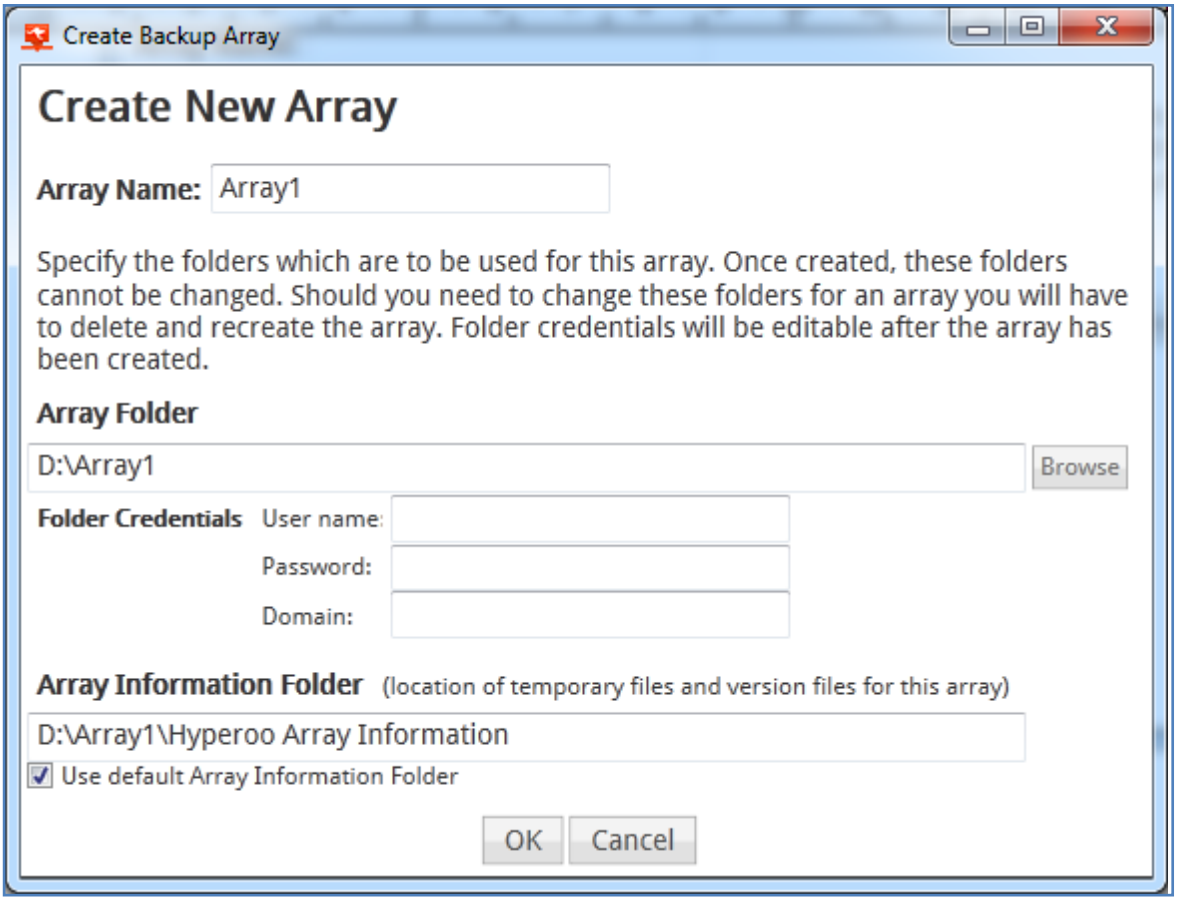

Figura 16. Ventana utilizada para la creación del arreglo de respaldo en la consola Hyperoo.

Los arreglos de respaldo de Hyperoo consistieron de dos archivos por separado. El "array folder", es donde los archivos de respaldo fueron almacenados y el "array information folder" que es donde temporalmente los archivos fueron retenidos.

Lo siguiente fue editar todas las configuraciones del arreglo. La siguiente pantalla muestra la ubicación de los folders de respaldo.

Usando la pestaña **network & security** se puede configurar un arreglo para requerir una contraseña y/o una conexión con autenticación.

Con **Versions and Deleted File Retention** el Hyperoo server puede sobreescribir archives por un período de tiempo determinado. Para respaldo en vivo (live backup) se puede especificar el período de tiempo en el que se creen nuevas versiones de de archivos que estén siendo usados por el arreglo en tiempo real.

La pestaña **array status** muestra cualquier respaldo actualmente conectado.

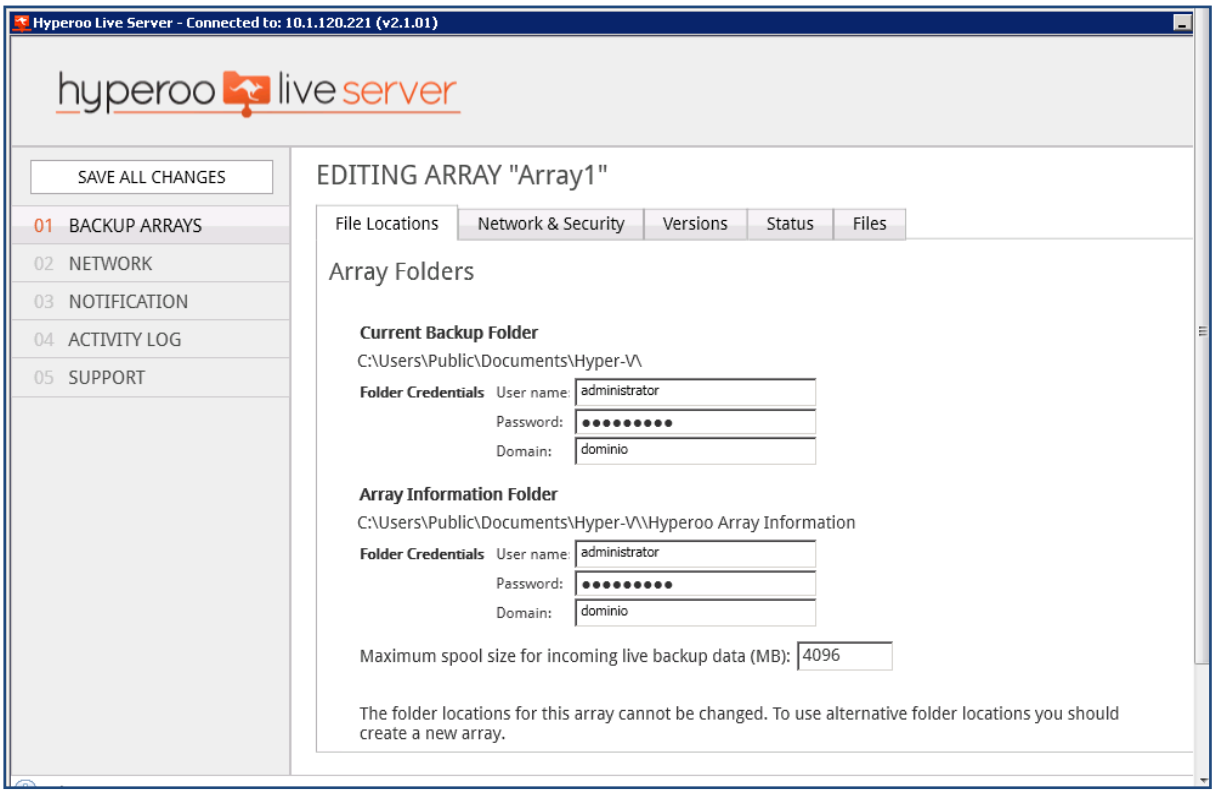

Figura 17. Edición del arreglo “array1”creado con variedad de configuraciones para el respaldo.

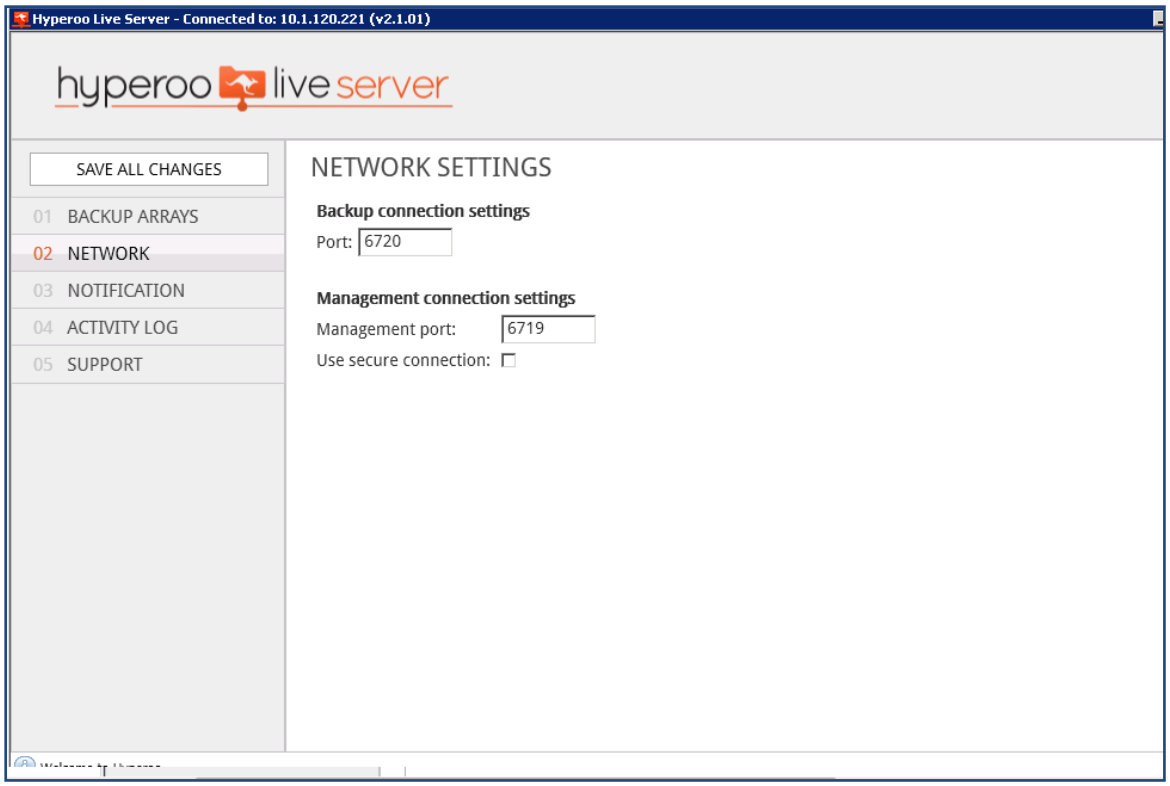

Figura 18. Configuración de red mostrando los puertos de conexión de respaldo y de consola respectivamente.

Una vez finalizada las configuraciones pertinentes para el arreglo de respaldo se procedió a crear una tarea de respaldo (*backup task*). Se abre la consola de administración de Hyperoo y se conecta con el Hyperoo client, una vez conectado se presiona el botón "**Add task**" y se crea la nueva tarea de respaldo.

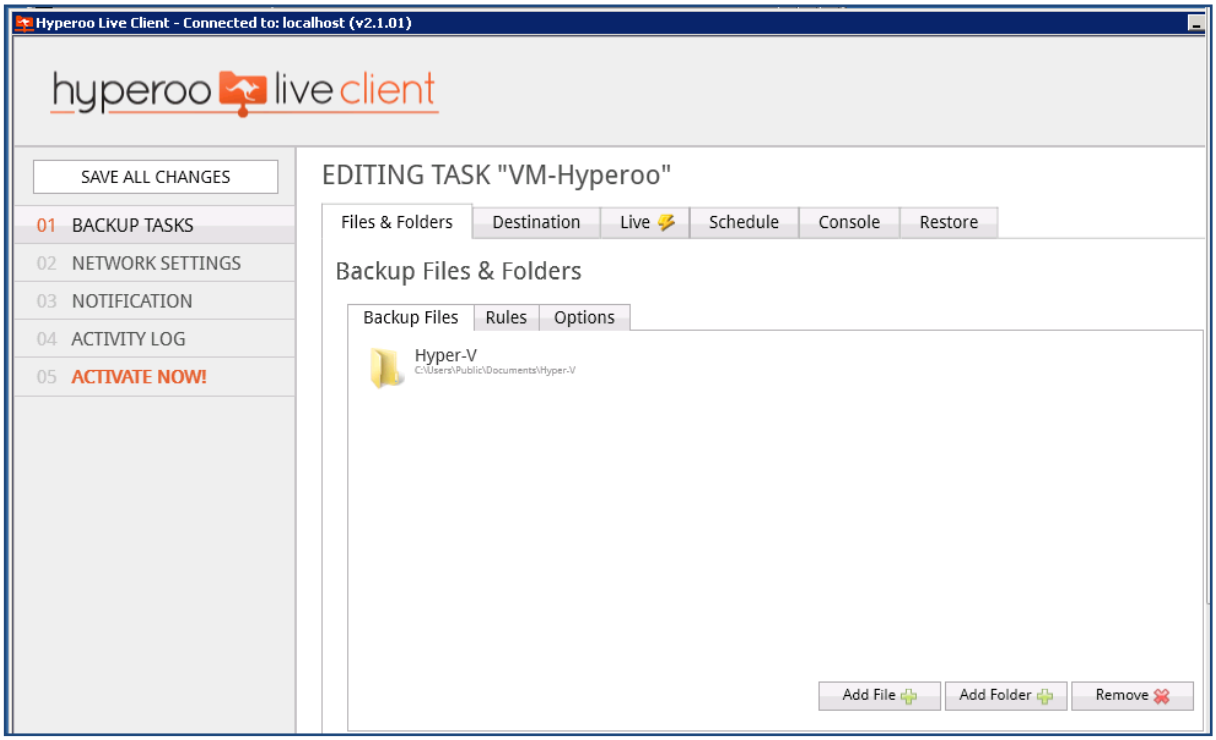

Figura 19. Creación de una tarea de respaldo en el Hyperoo client.

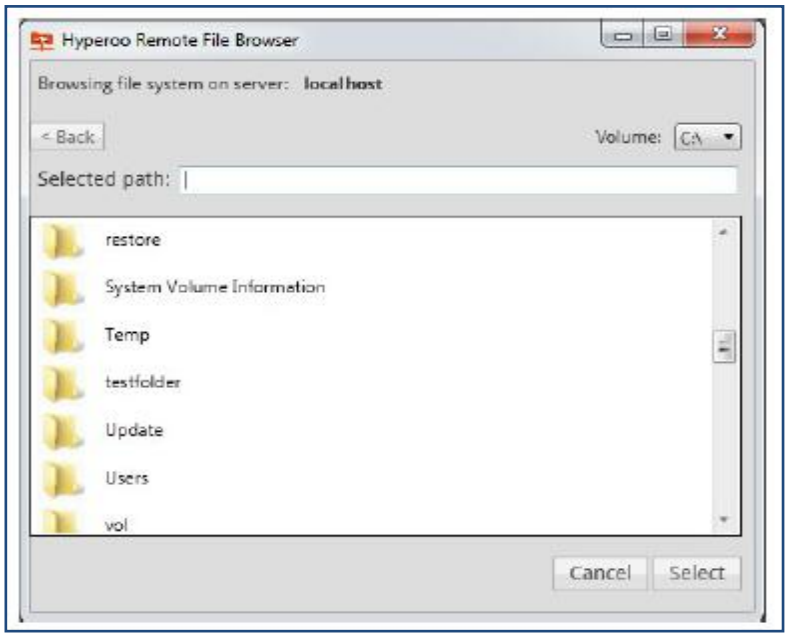

Figura 20. Ventana del navegador para la selección de la carpeta del Hyperoo server.

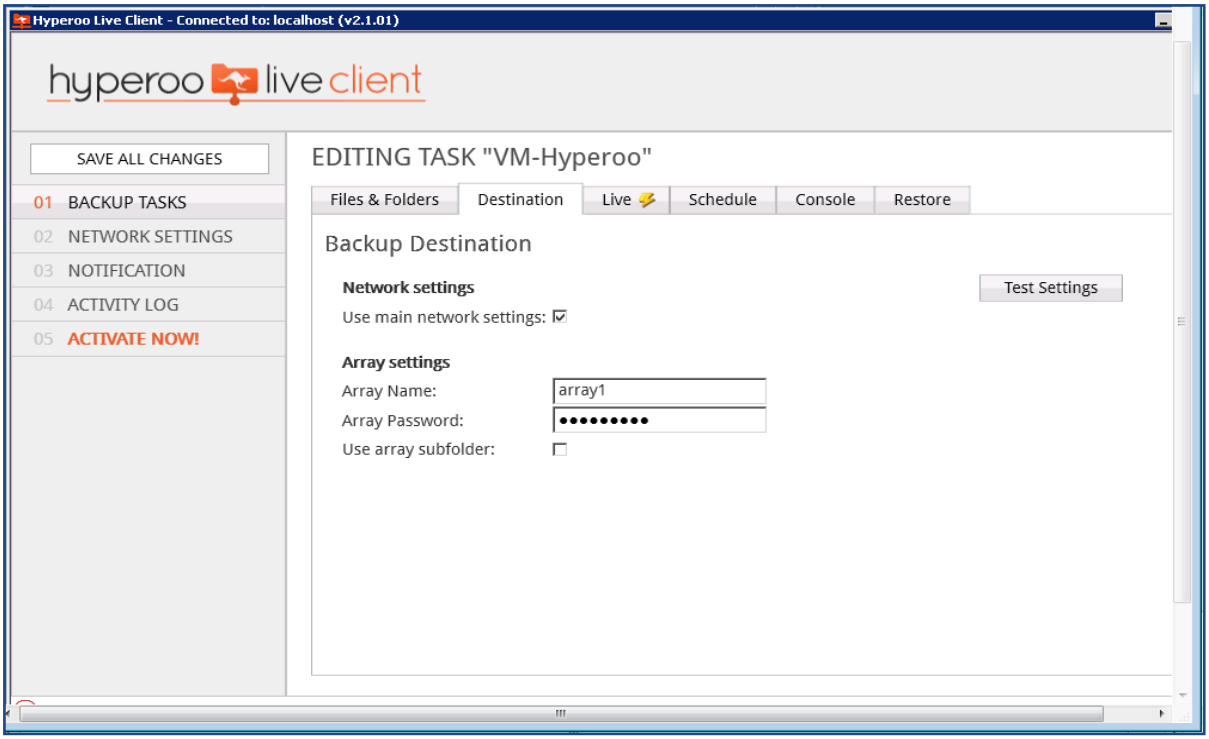

Figura 21. Ventana de especificación del nombre y contraseña del arreglo de respaldo.

A nuestra tarea de respaldo la llamamos VM-Hyperoo y a la almacenamos en una carpeta creada Hyper-V. Aquí debemos especificar el destino (destination) del Hyperoo server. Además si queremos hacerlo como respaldo en vivo (live backup), programación (schedule), entre otras. Por último se hicieron las especificaciones de las configuraciones de red tales como la dirección del servidor Hyperoo y su puerto de trabajo.

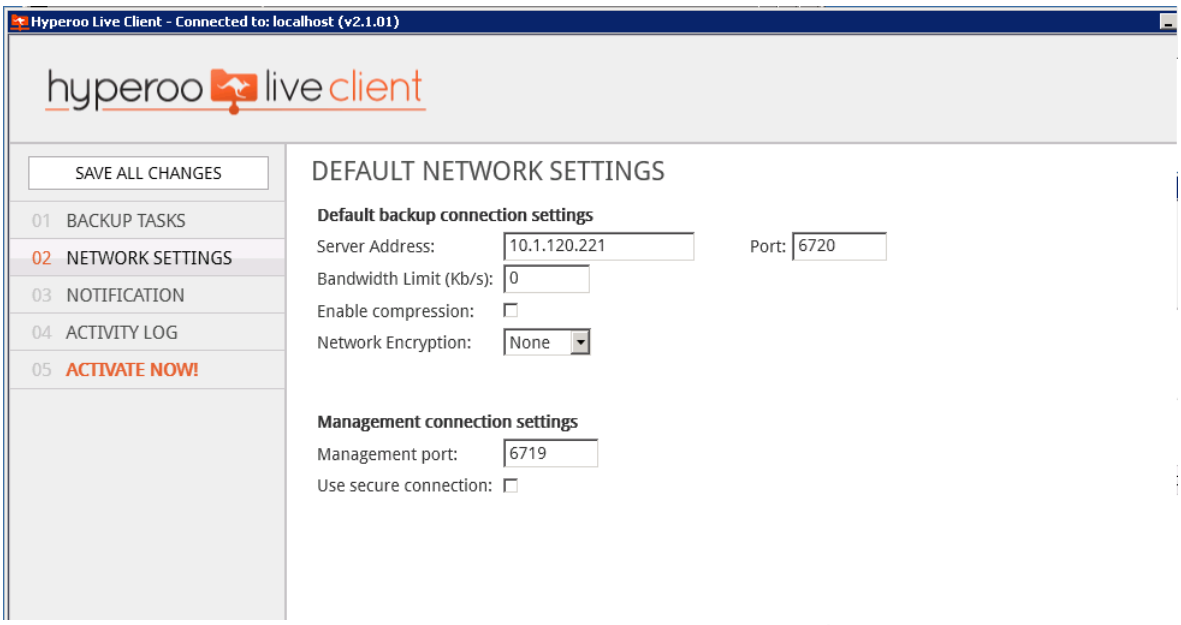

Figura 22. Configuraciones de red mostrando la dirección del servidor Hyperoo con su respectivo puerto.

Una vez finalizado las configuraciones básicas se replico la máquina virtual como tarea “VM-Hyperoo” del Hyperoo client hacia el arreglo de respaldo “Array1” en el Hyperoo server. Así, cualquier cambio que se hiciera en el Hyperoo client se hacía en término de segundos en el arreglo de respaldo.

2.3.3. Solución de replicación con Starwind iSCSI SAN & NAS V6

Producto que lleva el nombre de su empresa creadora Starwind Software Inc. Es un supervisor de almacenamiento que provee disponibilidad continua. Starwind ofrece reflexión (*mirroring)* sincrónico entre dos o tres nodos de un clúster de alta disponibilidad (HA). Esto hace resiliente contra los fallos de hardware o software, y asegura 50% más de desempeño (*performance*). Está diseñado para trabajar con *Windows server 2008 R2* y entre sus mayores beneficios tenemos replicación asíncrona sobre enlaces WAN, redundancia ante fallos de nodo, TCO minimizado y ROI acelerado.

2.3.3.1. Escenario de prueba con Starwind Software

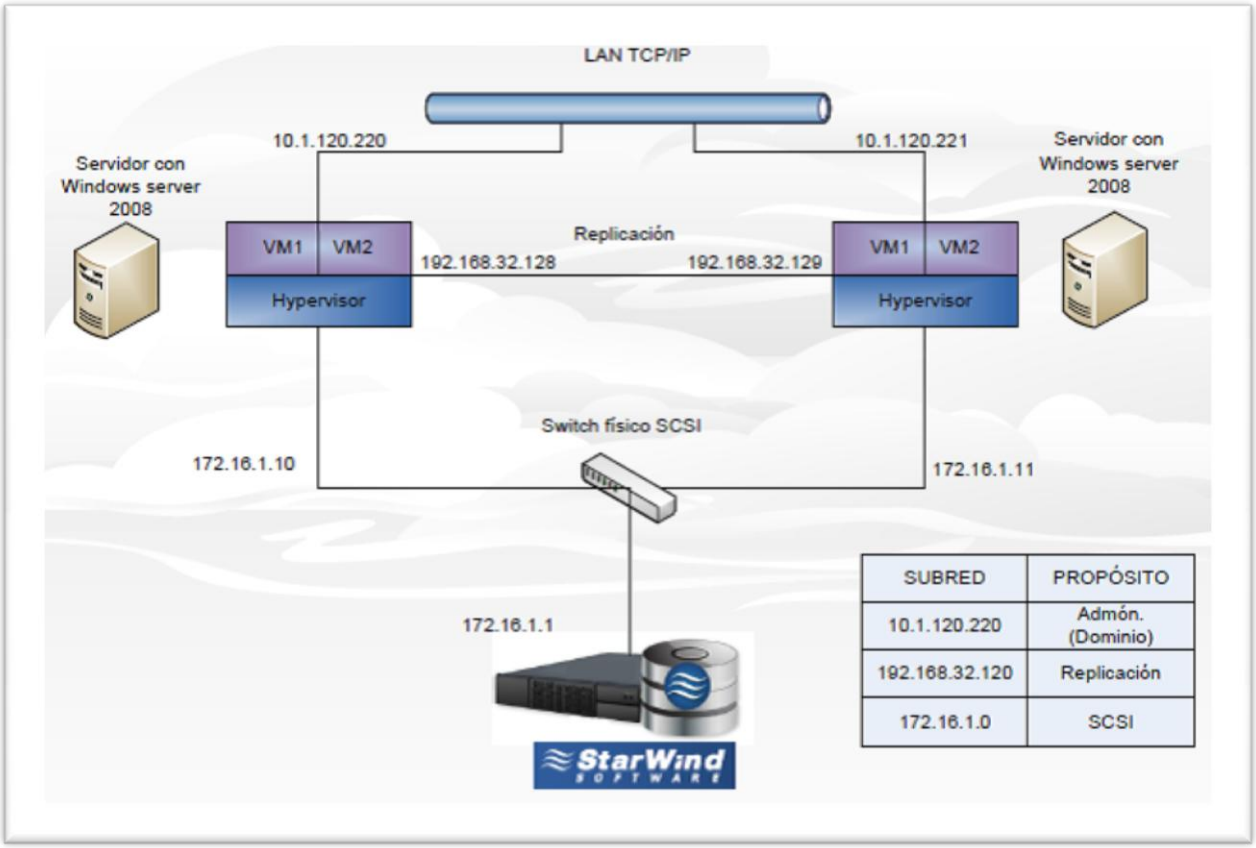

Figura 23. Escenario montado para realizar pruebas de replicación y storage con Starwind Software.

La figura anterior contiene el escenario que se utilizó para realizar evaluación de replicación con el software Starwind iSCSI SAN. Los dos servidores utilizan Windows server 2008 R2 y su respectivo hypervisor es Hyper-V que viene integrado en dicho sistema operativo.

En cada servidor, nombrado como hyper-node1 e hyper-node2 respectivamente, se crearon tres tarjetas de red (virtuales) con los siguientes propósitos: una establece la comunicación con la red LAN, la otra que permite la conexión iSCSI con el switch físico, necesario cuando se establece una red SAN y por último la que se utilizó para la replicación.

Las máquinas virtuales (VM) se crearon en cada servidor por medio de Hyper-V Manager. Cada disco duro virtual (VHD) perteneciente a su respectiva VM se almacena en la Starwind iSCSI SAN. Lo anterior permite que todas las máquinas virtuales puedan ser vistas y administradas por ambos Hipervisores, llegando a lo que se denomina clúster de servidores. Para realizar este clúster fue necesario crear un dominio de prueba (dominio.test) puesto que es un requisito, cada servidor debe estar unido a un dominio.

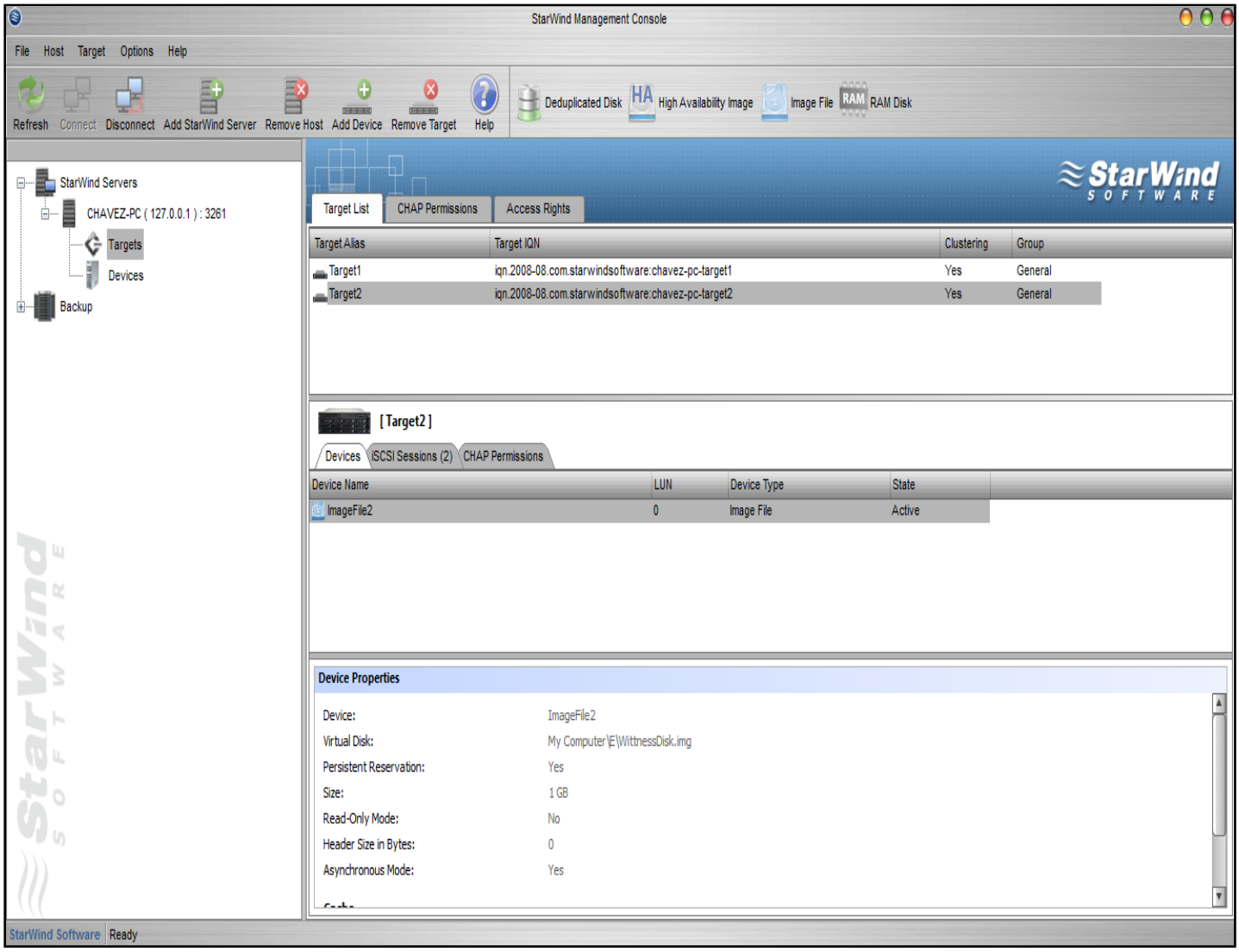

Figura 24. Ventana principal que muestra la consola de administración Starwind.

Así, por medio de *cluster shared volumes* (CSV) cada VHD se encuentra alojado en la SAN pero cada vez que estas inicien se cargarán en la RAM de cada hyper-node.

El *localhost* (127.0.0.1) funcionó como el Starwind server. En este servidor se crearon *devices* (dispositivos) y *targets* (objetivos). Los dispositivos son discos virtuales que se crearon para que sirvieran como almacenamiento compartido. Para nuestro escenario se crearon dos dispositivos: un disco virtual *high availability* (HA) de tamaño de 200 GB para el almacenamiento de las máquinas virtuales se creadas en los hyper-nodes y el otro fue un disco testigo (*witness disk*) de 1 GB necesario para validar el estado de servicio y es un recurso compartido que determina el número de nodos.

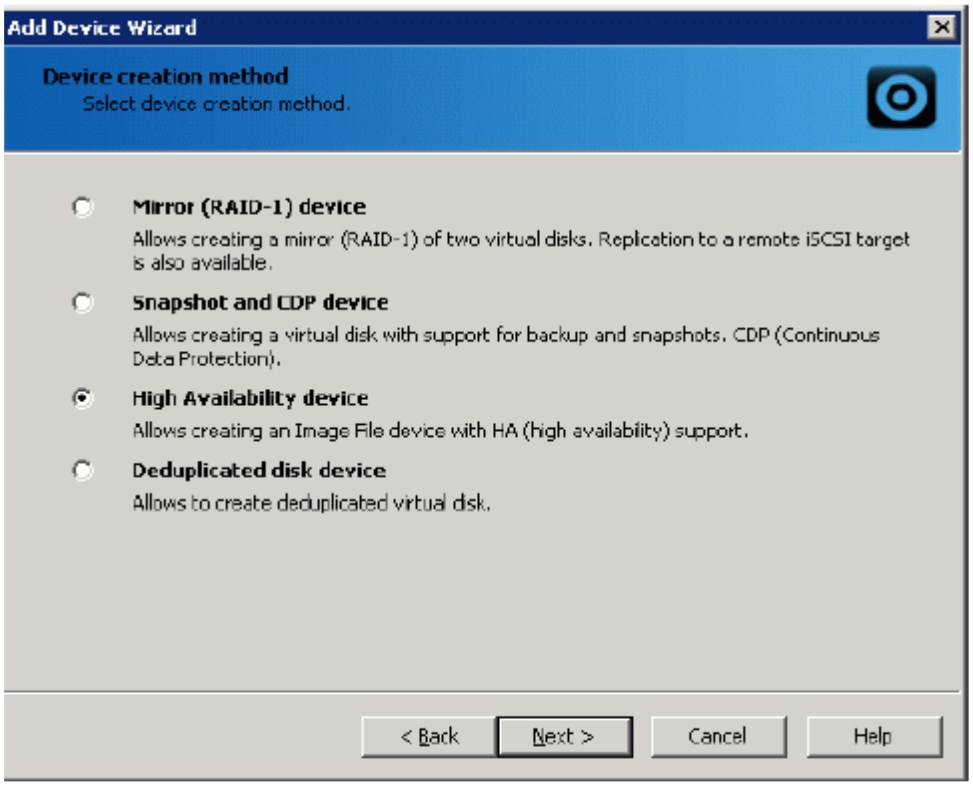

Figura 25. Ventana de elección del tipo de dispositivo de almacenamiento a crear.

En el caso de los objetivos se utilizaron para conectar a los nodos que forman en el clúster y deben crearse tantos objetivos como nodos tengamos. Como se tienen dos nodos entonces se crearon dos objetivos, “target1” y “target2” respectivamente. Bajo estos nombres se declaran ante los Microsoft SCSI initiators en cada servidor al servicio de Starwind sobre una red IP.

Una vez creado los dispositivos y objetivos se hicieron las conexiones. Para que los servidores tuvieran acceso a los discos virtuales y almacenaran sus respectivas máquinas virtuales solo restó en cada servidor ingresar al *server manager* y en la pestaña de *storage* dar el formato a ambos volúmenes creados. Para los objetivos se ingresa a los Microsoft iSCSI initiators en cada servidor para descubrirlos y conectarlos y así quedan ya establecidas las sesiones iSCSI.

2.3.4. Solución de replicación con *Double-take avalaibility* software

La última estrategia fue un producto de replicación asíncrono (a nivel de bytes) que utiliza también tecnología basada en host (*host-based software*). El producto es distribuido por varios proveedores encargados de implementaciones críticas de tecnologías de información y comunicaciones y es un software licenciado, lo que indica que es un producto calificado para muchos fines. Por ende, para evaluar este producto se utilizó una versión de prueba (*trial*). Es un software impulsado por Microsoft garantizando la máxima disponibilidad para los clústeres de Windows server, como lo es en nuestro caso. Sin embargo, puede trabajar en el entorno VMware como lo es vSphere.

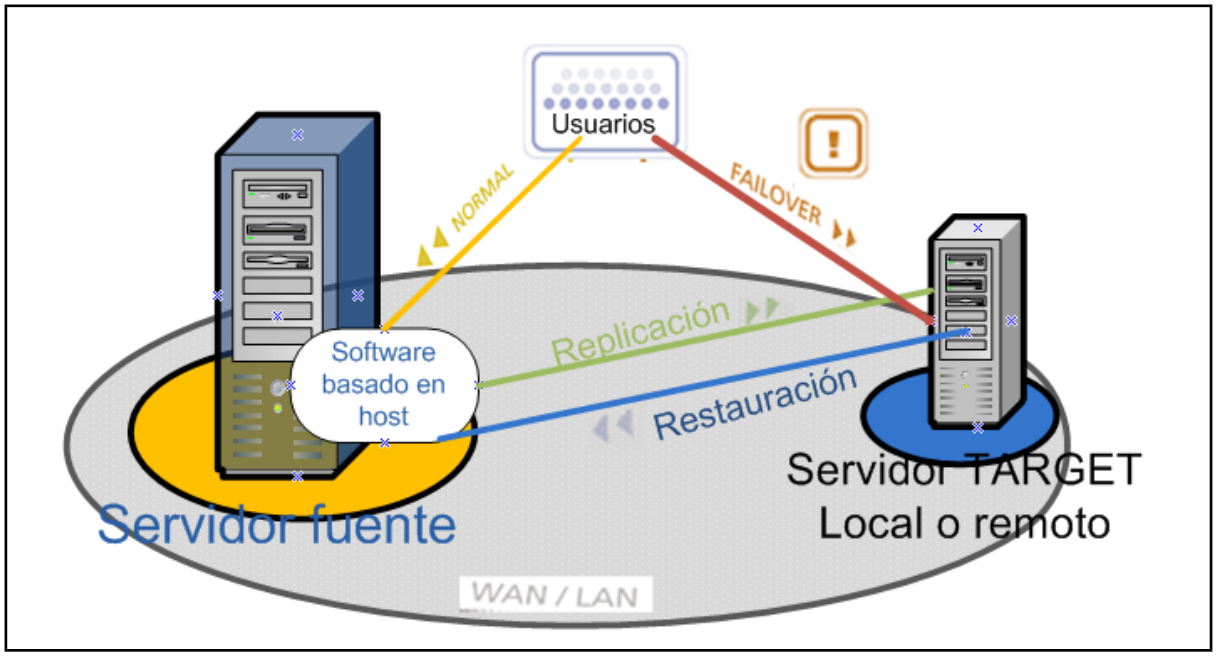

Figura 26. Visión general y funcionamiento para *double-take avalaibility*.

En la figura se muestra el funcionamiento de ésta estrategia de replicación entre los dos centro de datos, que se encuentran representados por los dos servidores (fuente y target). Se puede apreciar que si un usuario está haciendo uso de los servicios del sitio uno y se produce una interrupción o desastre entonces entra en modo *failover*[4] *clustering,* entonces todos los servicios son levantados en el sitio dos sin que el usuario tenga detalles de los incidentes. En condiciones normales se realiza la replicación entre los sitios de almacenamiento, en caso de fallo entonces después de que se restablecen los servicios en el sitio uno se recuperan todos los datos desde el sitio dos. Es decir, el software captura los cambios regularmente, manteniendo el disco virtual *target* actualizado y listo para la recuperación en

[4] Capacidad de automáticamente conmutar hacia un sistema de almacenamiento redundante si el sistema primario falla, especialmente para proveer servicio muy confiable en una red.

cualquier momento. Así, la máquina virtual replicada puede ser iniciada en un segundo servidor con los datos más recientes.

Este software de replicación se encarga de proteger tanto datos como aplicaciones con su dotación *full-server failover*, no como sucede con las estrategias de protección de datos tradicionales que se enfocan sólo en los datos y no en las aplicaciones. Además, se caracteriza por realizar replicación en tiempo real.

El uso de virtualización (que simplifica operaciones de recuperación) en conjunto con soluciones de almacenamiento de alta disponibilidad y software como *double-take avalaibility* ayuda en gran manera a economizar en equipos, ancho de banda, mientras permite diseñar un RTO de minutos con bajo riesgo de pérdida de datos (RPO).

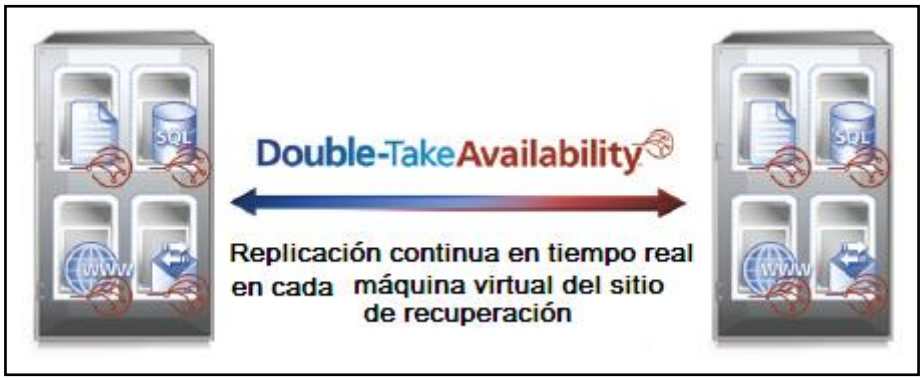

Figura 27. Protección de máquina virtual a máquina virtual con *double-take avalaibility.*

Vemos como el software está regularmente haciendo la replicación entre sitio y sitio posterior a que ha detectado cambios en la escritura de los discos de los servidores locales para enviar las solicitudes de replicación a los servidores remotos (llamada a procedimiento remoto, RPC), una vez que éstos las acepten el software se encarga de enviar los datos modificados.

2.3.4.1. Características y beneficios

Como se mencionó antes *Double-take software* va más allá de respaldo periódico para proveer replicación de datos continua, asegurar pérdida de datos mínima y permitir recuperación rápida por desastre o suspensión temporal del sistema; proporciona muchos características/beneficios más:

a. Distancia ilimitada de replicación. Permite la replicación de un sitio remoto tan largo del servidor fuente como se requiera y sobre todo con redes IP estándares para una máxima protección contra pérdida de datos.
b. Independencia de Hardware. Con esto se consigue flexibilidad de elegir cambios en hardware o reemplazos según el centro de datos crezca.

c. Independencia en la aplicación. La tecnología patentada STAR (*sequential transfer asynchronous replication*) permite la integridad completa de replicación de datos para cualquier aplicación.
d. Recurso exclusivo de herramienta de planeación. Simula la solución de replicación para estimar el ancho de banda necesario para estar activo.
e. Programación flexible del ancho de banda. Limita el uso de la red por parte del software durante las horas de mucho tráfico e incrementa estos límites durante las horas no pico para lograr una replicación muy eficiente con el menor impacto en la producción del servidor.
f. Compresión de datos inteligente. Mejora el desempeño y el uso de la red con el hecho de comprimir solo los datos que beneficiarán.

Los servidores existentes en el data center institucional utilizan tecnología de virtualización Hyper-V, la cual está integrada en Windows Server 2008 R2. *Double-take* fue diseñado para integrarse a este sistema y brindar protección a las máquinas virtuales en tiempo real.

Double-take se integra con Hyper-V para proveer descubrimiento de cada máquina virtual y sus recursos asociados. Una vez que las máquinas virtuales son descubiertas y catalogadas, se selecciona cada máquina virtual individual que se quiere proteger y la ubicación del objetivo (*target*) al que se quiere replicar.

El escenario para pruebas de *Double-Take* fue similar al de Hyperoo porque solo requería la instalación del software al igual que se hizo con Hyperoo con la excepción de que *Double-Take* solo se compone de la consola de administración que realiza todos los procesos necesarios para la replicación.

2.3.5. Resultados de los casos de estudio

Las evaluaciones anteriores se realizaron con tecnologías *host-based-software* como se mencionó con anterioridad. Se exponen los resultados en el orden en que se evaluaron y proponiéndose al final la estrategia elegida para la replicación entre el centro de datos institucional y el de la facultad de ciencias Médicas y las razones por las que se eligió incluyendo, por supuesto, la métrica de elección.

2.3.5.1. Hyperoo

Hyperoo proporcionó sencillez y rapidez en su configuración. Es fácil de integrar por su característica de cliente/servidor y su interfaz de usuario es amigable y comprehensiva al usuario. Se hizo un test de replicación de una máquina virtual obteniendo buenos resultados por sus características relevantes. También se pusieron a prueba sus capacidades de recuperación (restore) haciéndolo de manera

íntegra en cuanto a los datos se refiere. Además se comprobó su seguridad al utilizar al algoritmo de encriptación de datos muy conocido AES (Advanced Encryption Standard).

2.3.5.2. Starwind iSCSI SAN

Se realizaron las pruebas de replicación respectivas como objetivo principal del software Starwind. Así, cuando se creaban, escribían y modificaban archivos en uno de los nodos dichos cambios se registraban en el otro nodo por medio del *external storage* a los que se encuentran conectados dichos nodos. Es decir, había replicación sincrónica de datos a través de un clúster de dos nodos de almacenamiento.

También encontramos que Software de SAN iSCSI tiene varias características claves de las SAN físicas. Es totalmente compatible con protocolo de autenticación por desafío mutuo (CHAP) para la autenticación segura. Entrada/Salida múltiples rutas (MPIO) para aumentar la capacidad. Microsoft Volume Shadow Copy Service (VSS) para tomar instantáneas de los datos.

Sin embargo, se descubrió que en la forma más pura de clustering (dos nodos y un disco compartido) ésta configuración resulta en un solo punto de fallo. Agregando almacenamiento redundante es una manera de resolver este problema. Sin embargo, la dificultad aún estará allí puesto que el clustering proporciona disponibilidad de servicio, pero no protección para los datos usados por el servicio.

2.3.5.3. Double-Take

Las pruebas realizadas con este software demostraron que es una herramienta poderosa en cuanto replicación obteniendo un buen performance sin afectar notoriamente el rendimiento de la red ya que hace replicación continua solo de los cambios que se hacen en los archivos y no de los archivos completos, mejor dicho, solo envía las actualizaciones de los archivos de forma periódica. Posee un poco más de complejidad pero sus beneficios son indudables.

Asegura la integridad de los datos porque entiende muy bien la metodología de escritura de los datos en los discos locales de los servidores local y remoto.

2.3.6. Elección de la solución de replicación

Habiendo evaluado las anteriores estrategias de replicación se propone la elección del producto Hyperoo para replicar y respaldar datos entre el centro de datos institucional y el de la facultad de Ciencias Médicas por las siguientes razones:

1. Hyperoo soluciona la mayoría de las dificultades para realizar respaldo de máquinas virtuales en Hyper-V haciendo respaldos en vivo hacia el Hyperoo server sobre la red IP, respaldando también bases de datos SQL, ESx (Exchange mail stores), entre otros.
2. Su rapidez es eficiente al solo transferir los datos cambiantes (delta speed) aproximadamente cada 10 segundos mientras que otros productos lo hacen cada 10 minutos. Así, hace respaldos de manera rápida sobre enlaces de baja velocidad como son los de red pública.
3. Soporta replicación de cualquier tipo de archivo.
4. Es mucho más configurable dando mayor control a los clientes, servidores, compresión y encriptación.
5. Restauración a cualquier host. La restauración de los respaldos desde cualquier punto en el tiempo a cualquier cliente.
6. Su precio es accesible comparado con otras soluciones caras para pequeñas y medianas empresas (SMB´s) como el centro de datos institucional.
7. El sistema de alerta de Hyperoo es mucho mejor cuando se producen eventos de fallo.

Los factores determinantes para elegir Hyperoo como **métrica** fueron los siguientes:

Relación coste/beneficio

Una de las ventajas de Hyperoo, como se hizo mención anteriormente, es el factor económico comparado con los beneficios que representa. La licencia individual de este software se encuentra en el rango entre U$D 65 y U$D 79 por servidor físico. Esto quiere decir, que no importa cuántos servidores o máquinas virtuales tengamos en un servidor físico solo se debe comprar una *licencia hyperoo live server.* Sin embargo, se deben comprar licencias adicionales para cada máquina en la se quiere hacer la instalación de *hyperoo live client*, sea esta virtual o física.

Escenario

Óptimo para escenarios con enlaces de baja velocidad como lo son los enlaces WAN de la universidad, ya que no demanda mucho ancho de banda.

Confiabilidad

Integridad de los datos al ser replicados sobre toso en un escenario fiable como el que se mencionó anteriormente.

Funcionalidad

Realiza todas sus funciones de manera sencilla y con eficacia.

Como una desventaja, la transferencia en vivo en CSV (*cluster shared volume*, del inglés volumen en clúster compartido) actualmente no está soportada por Hyperoo.

2.4. Propuesta de implementación de nube privada

Empezamos por introducir esta propuesta con el término de nube privada. Nube privada es la implementación de servicios en la nube sobre los recursos que se dedican a la organización o institución (al data center en este caso) y que puede ser una implementación dentro (on-premises) o fuera de ellas (off-premises). Así con una nube privada, se pueden obtener beneficios de nube pública (autoservicio, escalabilidad y elasticidad) con el control adicional y personalización de disponer de recursos dedicados.

Si algo está claro es que la nube privada es una nueva y mejor manera de administrar y mejorar los recursos y los servicios de los sectores de tecnologías de información y comunicación. Así, en lugar de que los recursos del data center del TIC cumpla funciones predefinidas y limitadas, se forma un pool flexible que los administradores pueden aprovechar en los procesos de manera precisa cuando sea necesario.

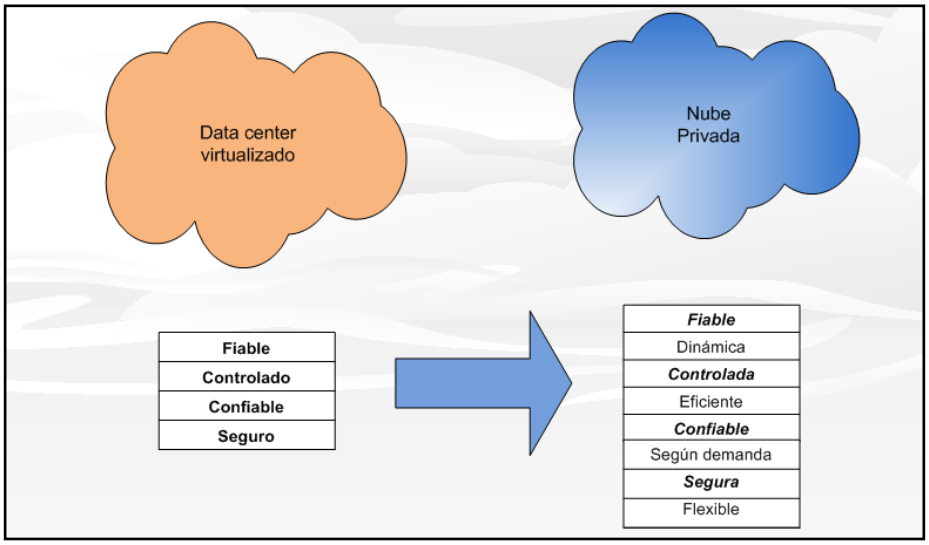

Figura 28. Características de la nube privada.

Podemos apreciar que la nube privada incorpora los beneficios de un data center virtualizado. Es por ello que se dice que la tecnología de virtualización está directamente relacionada con la computación en la nube o *cloud computing.*

Existen dos modelos de servicios de nube que se pueden brindar en una nube privada: infraestructura como un servicio (IaaS) y la plataforma como un servicio (PaaS). Para nuestra propuesta el enfoque fue IaaS. Con IaaS se puede utilizar los recursos de la infraestructura (servidores, sistemas operativos, bases de datos, de red y de almacenamiento de información) como un servicio.

La implementación de IaaS como un modelo de servicio es una parte fundamental del enfoque de cloud computing para esta propuesta, lo que permitiría construir un entorno de nube dedicado a transformar la manera en la que se brindan los servicios de TI para el data center de UNAN-MANAGUA, además de facilidad, rapidez, capacidad de adaptación y recuperación de desastres. Este último es uno de los objetivos primordiales que se han expuesto a lo largo del trabajo.

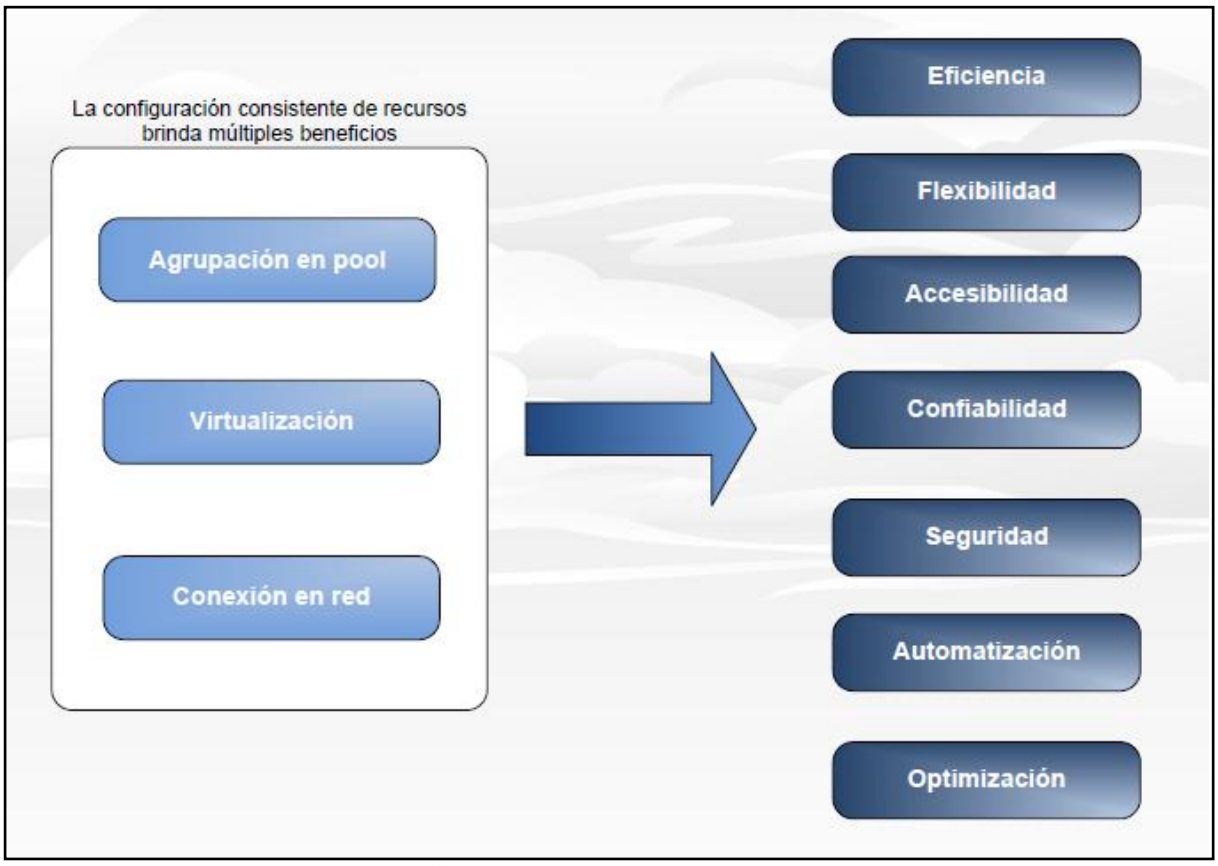

Figura 29. Características y ventajas de la infraestructura de nube.

Esta configuración consistente de recursos mostrada en la figura cambiaría plenamente la manera en que se administran y aprovisionan los recursos de información y tecnología del centro de datos. Vamos a explicar brevemente las características de los recursos de la infraestructura de nube privada:

La agrupación en pool permite que todos los recursos de infraestructura de nube se organicen y administren como un pool compartido en común, este pool se inicia con servidores y almacenamiento que establecen el escenario para los datos y aplicaciones.

Con la virtualización todos los recursos del pool están empaquetados en “contenedores de envío” electrónicos.

Por último la conexión en red, con esto se puede acceder a todos los recursos por medio de una red con interfaces estándares que se combinan como bloques.

Para formar nuestra propuesta de nube privada se necesitan dos elementos fundamentales:

- Un sistema operativo (hypervisor de primer nivel).
- Software o herramienta para administrar el pool de servicios.

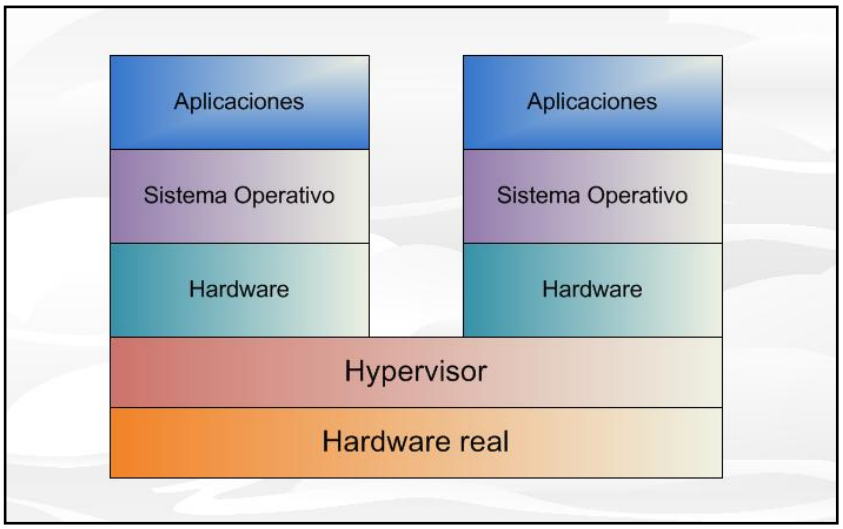

Figura 30. Modelo de hypervisor de primer nivel.

Se necesita el software de administración para ayudar a crear un pool virtualizado de recursos de computación, proporcionar acceso a los usuarios finales, y manejar la seguridad y la asignación de recursos.

En este caso el hypervisor es hyper-V del sistema operativo Windows Server, uno de los mejores sistemas operativos de servidor para la nube y la herramienta es *system center virtual machine manager* (SCVMM).

SCVMM ayuda a mantener una administración centralizada de la infraestructura física y virtual de TI, incrementa la utilización de un servidor, optimiza de manera dinámica los recursos a través de múltiples plataformas de virtualización incluyendo capacidades tales como planeamiento, despliegue, administración y optimización de infraestructuras virtuales. Las características más importantes de SCVMM son las siguientes:

- Crear y administrar máquinas virtuales de manera centralizada.
- Consolidar fácilmente múltiples servidores físicos dentro de un solo servidor host.
- Aprovisionamiento y optimizado rápido de máquinas virtuales.
- Administración dinámica de los recursos virtuales a través de los *management packs.*

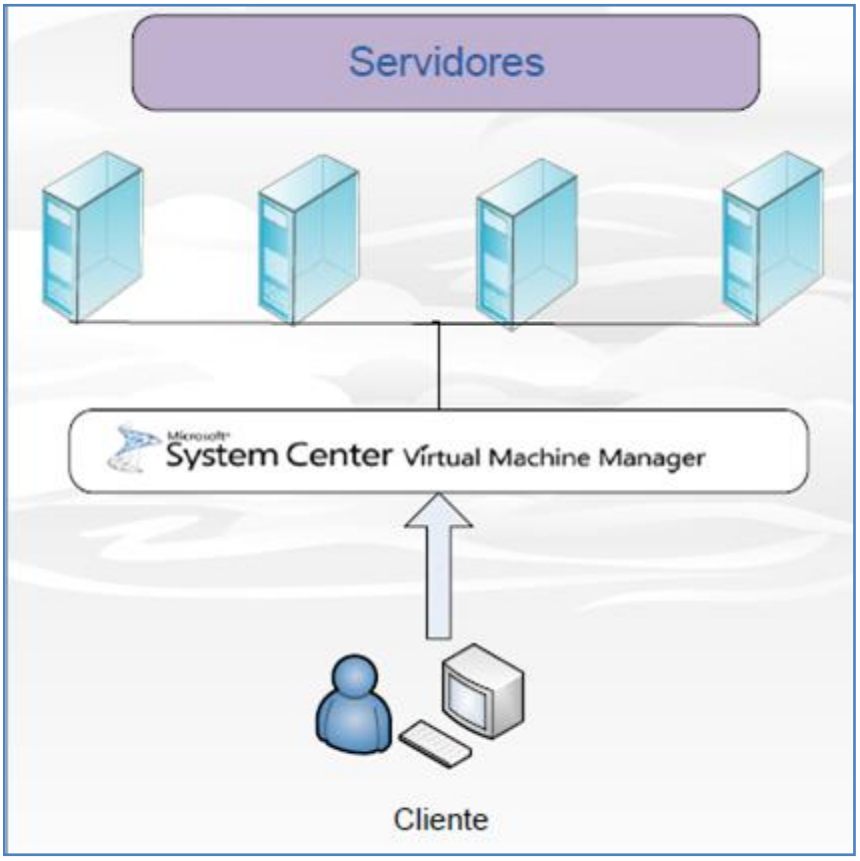

Figura 31. Administración de máquinas virtuales de manera centralizada por medio de system center virtual machine manager.

La figura anterior demuestra la forma centralizada en que SCVMM administra todas las máquinas virtuales, siendo más efectiva porque en lugar de que el cliente administre máquinas individuales la herramienta permite administrarlas como un conjunto.

A estos elementos se agregan los roles de administración y roles de acceso solo lectura integrado con los sistemas de autenticación. Con la nube privada para el data center institucional se pretende lograr alta disponibilidad, simplicidad en la prueba de aplicaciones y brindar servicios de manera transparente, es decir, tener el control total de dichos servicios.

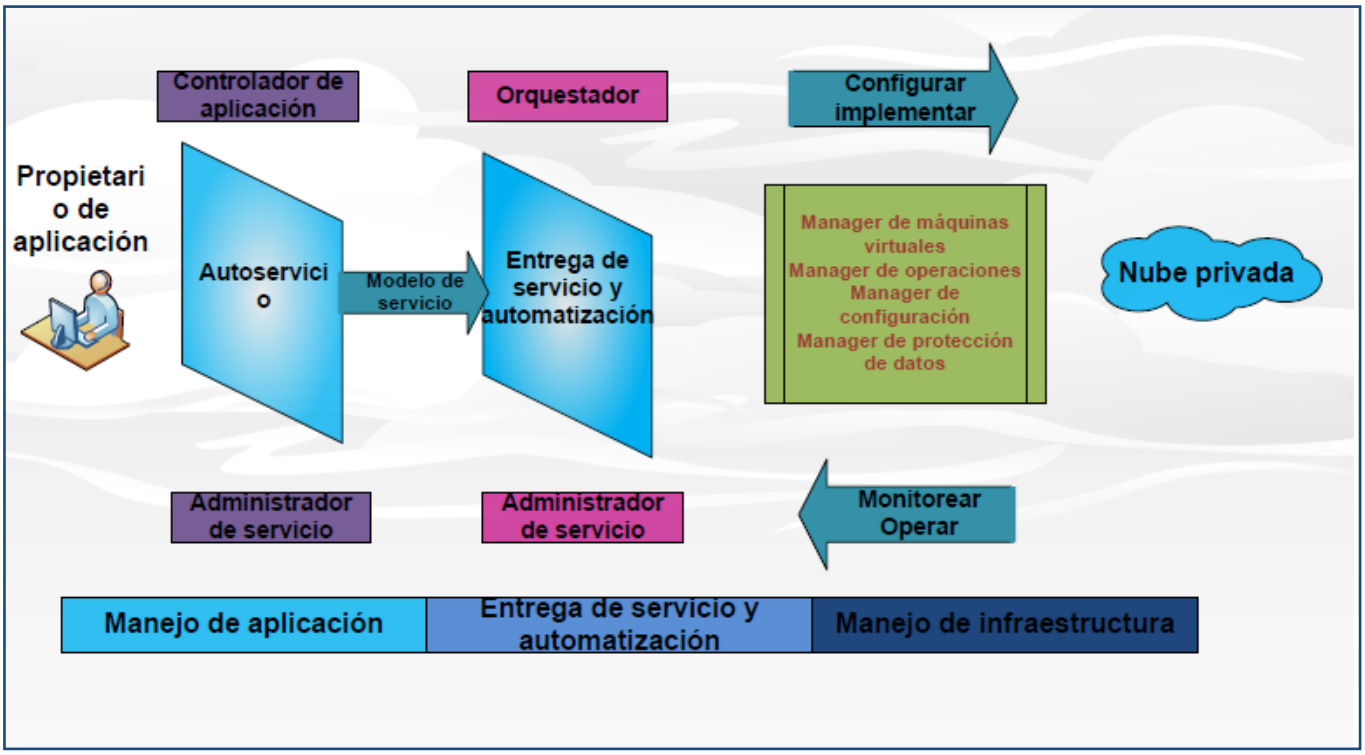

Figura 32. Modelo de infraestructura como servicio de nube privada.

Los recursos aprovisionados y administrados por la nube privada pueden extenderse más allá, brindando a administradores una experiencia nueva y fresca. Así, ya sea cualquier equipo que el administrador esté usando (por ejemplo PC, portátil o PDA) y donde sea que esté trabajando (casa, oficina).

Todo lo anterior es posible porque una de las cosas que se pueden empaquetar en un contenedor virtual es la interfaz personalizada de un usuario o administrador incluida la experiencia de una apariencia informática preferida e información sobre la identidad específica y los permisos para visualizar y usar los recursos específicos de una infraestructura de nube. Es decir, cuando la infraestructura de nube se extiende de esta manera:

- El administrador o usuario disfruta de la misma experiencia, no importa donde sea la ubicación o el dispositivo que utilice logrando una flexibilidad y productividad sin precedentes.
- Los dispositivos se pueden segmentar de manera segura con el ambiente de trabajo y el ambiente informático personal en ubicaciones distintas.
- Los dispositivos locales pueden ser "*thin clients*" simples y de bajo coste porque la funcionalidad y la mayoría de los procesos no se llevan a cabo en dichos dispositivos sino en la infraestructura de nube.

Con ésta triple ventaja (experiencia del empleado/administrador, acceso seguro y eficiencia de administración y costos) representa mucho de lo que implica la nube privada.

El modelo infraestructura como servicio (IaaS) de nube que se propone integra dos características principales, escalabilidad y alta disponibilidad.

La **escalabilidad** posibilita el crecimiento horizontal. Sin la necesidad de desplegar, probar y arreglar servidores físicos el centro de datos puede hacer fluctuar su capacidad informática según las necesidades y el crecimiento tanto como se requiera.

La **alta disponibilidad** (HA) es inherente porque los servicios de nube corren bajo servicios virtualizados, es decir, en un orden jerárquico bajo la nube siempre debe encontrarse una infraestructura virtual y bajo ésta, una infraestructura física formada por clústeres de alta disponibilidad. Además con el cloud computing, cuando las herramientas de gestión de los sistemas determinan que la infraestructura que soporta una aplicación está a punto de caerse, pueden lanzar una nueva máquina virtual y desviar el tráfico.

2.4.1. Direccionamiento hacia la nube privada

Lo primero para direccionar a la nube es que todas las subredes deben estar definidas en el *virtual network manager* de cada servidor que se desea direccionar a la nube. Así, el direccionamiento hacia la nube privada se hace por medio de una de las características de System center VMM, agregar infraestructura adicional para adaptar las necesidades de recursos. Esto se hace en la pestaña *networking* en el panel principal de virtual machine manager.

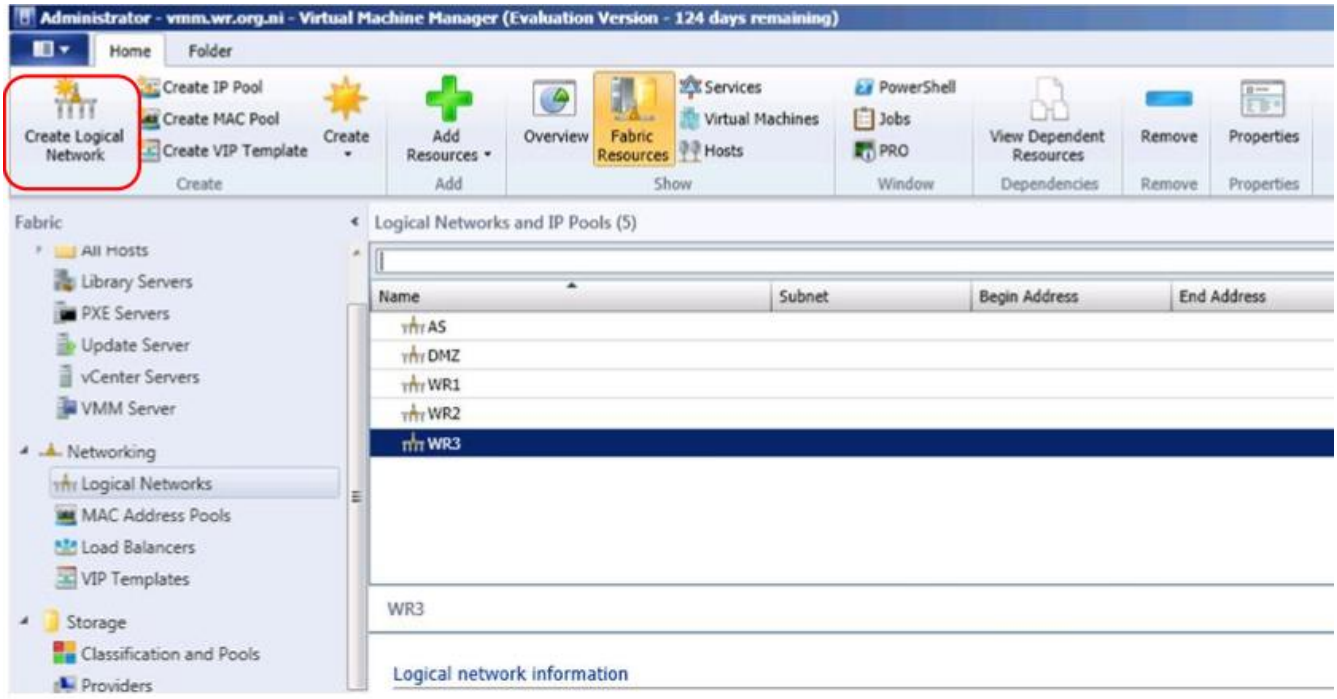

Figura 33. Creación de una red lógica en system center virtual machine manager.

Se crean las redes lógicas y el pool IP de manera que se simplifique el autoservicio. Así entonces se agregan las redes lógicas (*logical networks*). Las redes lógicas permiten a los usuarios de autoservicio implementar aplicaciones sin necesidad de entender la red fundamental. Al dar clic sobre *logical networks* nos aparecerá el asistente de creación.

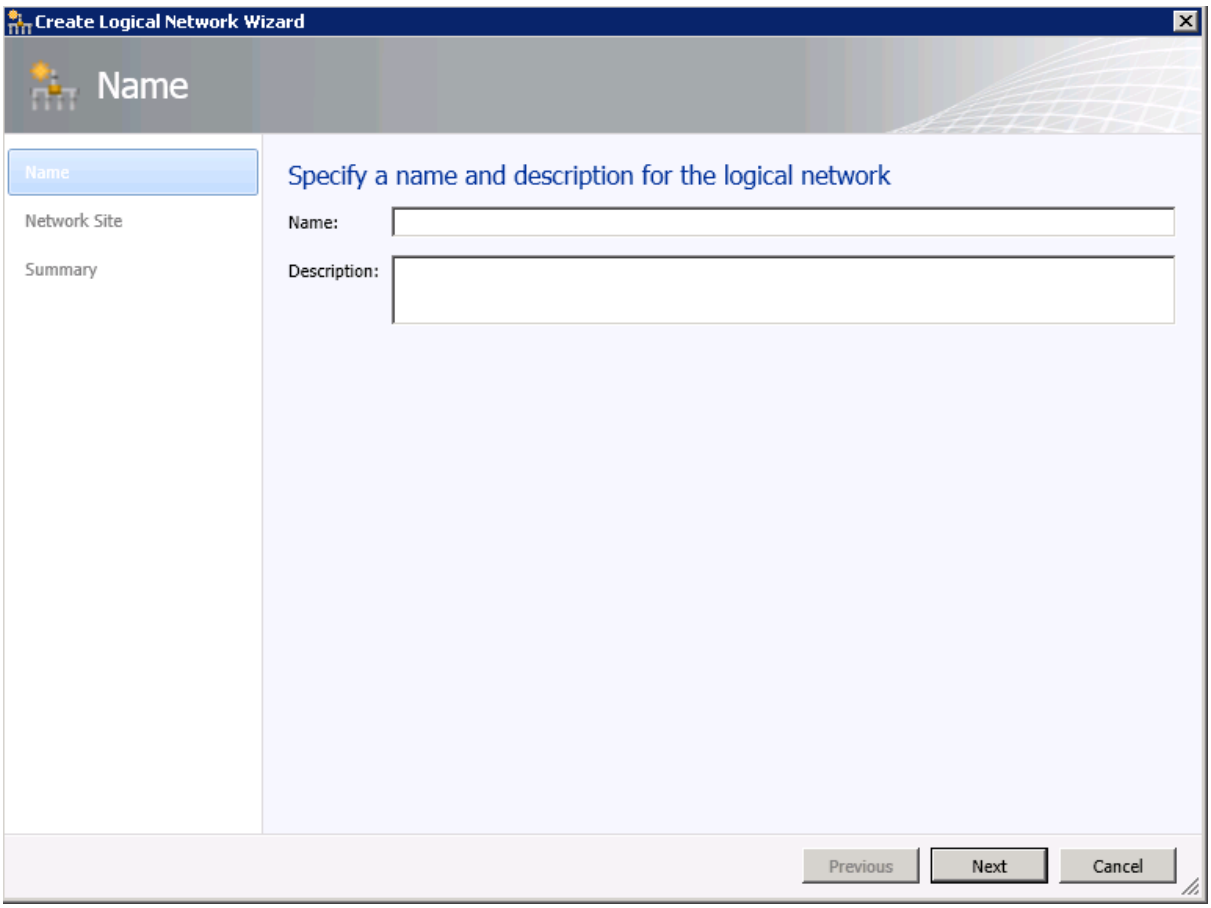

Figura 34. Asistente de creación para una red lógica.

En la ventana anterior se especifica el nombre y una breve descripción de la red lógica creada.
Lo último es designar la red LAN virtual (VLAN) asociada a la subred y su respectiva dirección IP de red con máscara.

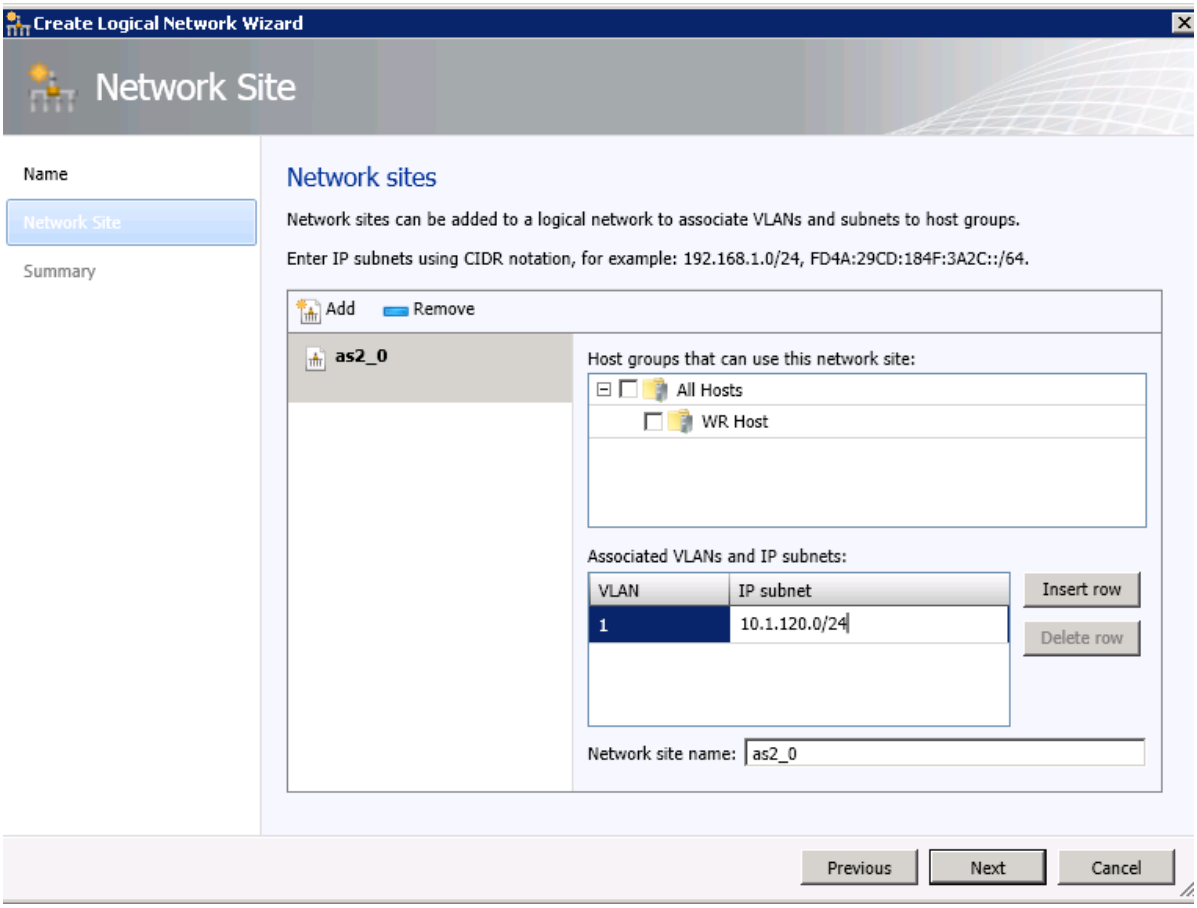

Figura 35. Número de VLAN y dirección IP de subred para finalizar el asistente.

2.4.2. Seguridad en la nube

Las principales preocupaciones por parte de directores y administradores de TI en cuanto a la migración a la nube privada están orientadas a la seguridad e integridad de la información y de los datos y de hecho son preocupaciones válidas (que a muchos administradores estas preocupaciones los llevan a descartarla). Sin embargo, la implementación de la nube privada ofrece la oportunidad de fortalecer la seguridad y el cumplimiento de normas específicas al incorporar estos elementos en las definiciones y la administración de datos y recursos.

Como parte de la seguridad actual de toda la infraestructura de nube privada funcionan los *firewalls*, la encriptación y las contraseñas. Con la encriptación se logra alcanzar flexibilidad, conformidad y privacidad en los datos, lo cual es requerido en ambientes de prestaciones de servicios.

El uso de *Bitlocker Drive Encryption* y *Microsoft bitlocker administration and monitoring* (MBAM) es un ejemplo sencillo de nuestra propuesta, este feature que viene integrado en Windows server 2008 R2 provee encriptación de datos a nivel de volumen para datos almacenados en dicha plataforma. Protege los datos cuando el sistema Windows está fuera de línea (cuando el S.O está apagado) y evita violación de datos tal como robo de información confidencial. Sin embargo, esto puede no ser suficiente para un entorno de nube privada que brinde un ambiente de seguridad para administradores del data center de la UNAN-Managua, así como los servicios, datos y aplicaciones propias de dicho centro. A continuación se presenta una herramienta que brinde esa seguridad que se requiere.

HighCloud Security

Es una herramienta que provee encriptación y manejo de llaves y permite cerrar máquinas virtuales y sus datos de forma que permanezcan seguras a través de su ciclo de vida en la nube privada. Es una solución de seguridad para virtualización y nube. Es decir, encripta todas las máquinas virtuales en el centro de datos virtualizado y por ende en cualquier ambiente de nube privada.

Su funcionamiento es sencilo. Se instala el *Key & Policy server* (KPS) y el *virtual machine vault* y se selecciona una política de encriptación. Posterior se realiza un *storage VMotion/live migration* de las máquinas virtuales dentro del *virtual machine vault* (VMV) sin ningún tiempo fuera.

EL KPS es el sistema de manejo de llave por el cual los administradores especifican la longitud de la llave y las políticas acerca de la rotación. El VMV encripta las VMs para asegurar los datos en los dispositivos de almacenamiento.

Es tan completo que provee características tanto para data center como para la nube privada.

HighCloud para el data center

1. Administración/manejo total de llaves.
2. Habilidad de encriptar todas las partes de la máquina virtual (discos de la VM, snapshots).
3. No aplica cambios a las VMs.
4. Respaldos encriptados.
5. Rotación dinámica de llave.

HighCloud para nube

1. Permite la migración a la nube de forma segura y con confianza.
2. Cumplir disposiciones con ambas regulaciones, existentes como nuevas, tales como HYPAA, PCI y SOX.

3. Protección a los datos sensibles con una solución de encriptación administrable y fácil de implementar.

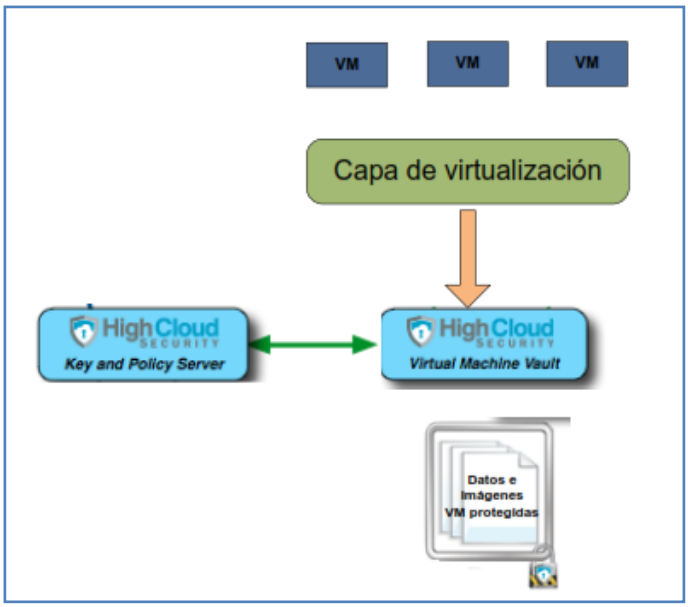

Figura 36. Arquitectura de HihgCloud security.

Esta herramienta tiene una gran ventaja, economía. Y es que permite implementar seguridad de nivel empresarial de forma gratuita la primera vez. El primer servidor de *key & policy* es totalmente gratis.

Depuración y calidad de la información

Con la infraestructura del centro de datos y su puesta sobre una nube privada se hace necesario un medio el cual permita estar evaluando y obteniendo resultados sobre la calidad de la información importante que se maneja de tal manera que se haya llegado a un nivel donde se encuentre depurada y filtrada toda esa información.

Specops para Active Directory

En el data center institucional como toda organización posee una gran cantidad de componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso. Un servidor virtual del CPD (ads1.unan.edu.ni) implementa el rol de *Active Directory* o servicio de directorio que utiliza distintos protocolos y así permite mantener una serie de objetos relacionados a las componentes de la red.

Specops deploy^{TM} convierte la infraestructura existente de Acitve Directory en una plataforma poderosa con un completo nivel de funcionalidad para: implementación de S.O, implementación de software e implementación de aplicaciones virtuales. Entre sus beneficios más importantes se destacan:

- Obtiene reportes detallados en tiempo real de todas las implementaciones.
- Implementación sobre enlaces de red de baja velocidad.
- Utiliza la infraestructura existente aprovechando los recursos.
- Automatización total del proceso de administración de escritorio.

Además utiliza las bases de datos, por ejemplo, SQL server, para almacenar los reportes que continuamente se están enviando durante todas las operaciones e implementaciones.

Como toda herramienta, es necesario hacer instalaciones tanto en el servidor como cliente.

Posee características de filtrado (filter *by deployment server y filter by state*) que permite calificar la información directamente de lo que se necesita encontrar.

Figura 37. Panel principal de Specops Deploy con los ítems más comunes.

También encontramos otra herramienta, un poco más sencilla y con otras características. Microsoft *assessment & planning toolkit* (MAP), es una excelente herramienta de de inventario, evaluación y reporte que ayuda a evaluar la infraestructura actual de TI y determina las tecnologías para las necesidades del data center.

Utiliza las tecnologías existentes para recolectar los datos en el ambiente y realiza inventario del hardware (reuniendo métricas de desempeño), software y sistemas

operativos y algo importante es que no se necesita instalar ningún agente de software en los equipos que se quieren evaluar.

Los datos y el análisis proveído por MAP permite hacer recomendaciones para promover cambios en el hardware.

Así entonces, MAP es ideal para:

i. Descubrimiento de servidores y sus aplicaciones.
ii. Preparación para migración de hardware y software.
iii. Capacidad de planeamiento para consolidación de servidores y bases de datos.

Procedimientos para respaldar los servicios

Como se ha descrito hasta ahora, uno de los objetivos primordiales del presente trabajo es tener un respaldo de los servicios que están bajo la responsabilidad del centro de datos garantizando la alta disponibilidad en el momento que se requieran. Se realizarían para las bases de datos y servidores, pilares del almacenamiento del data center.

Teniendo a Virtual Machine Manager como herramienta de administración que hace posible la conversión de máquinas físicas en virtuales y viceversa, facilita en gran manera el respaldo de dichas máquinas.

1. Determinar las bases de datos y servidores que se desean respaldar.
2. Si se trata de un servidor, se identifican los archivos o particiones que se van a respaldar. Además se establece la política y el esquema de respaldo tal como se muestra la tabla a continuación.

Nombre del Host	Edición S.O	Aplicaciones	Respaldo total del servidor	Esquema de respaldo		Regla de retención
				Full	Increm.	
Hyper-V1	WS2008R2	Hypervisor de virtualización	Sí/VMs	Sólo la primera vez	Día por medio	Eliminar los respaldos anteriores a 30 días.
Hyper-V2	WS2008R2	Hypervisor de virtualización	Sí/VMs			
Hyper-V3	WS2008R2	Hypervisor de virtualización	Sí/VMs			
Hyper-V4	WS2008R2	Hypervisor de virtualización	Sí/VMs			
Actasonline	OpenSuse	Actas en línea	Sí			

3. En caso de que sea una aplicación se evalúa si es la aplicación o los datos de la aplicación.
4. Para las bases de datos, se definen tres tipos de respaldos: completo, incremental y diferencial.

Base de datos	Tipo de respaldo	Parámetros de depuración
DB	Completo	• Mantener todos los respaldos de la última semana. • Mantener los respaldos de la penúltima semana a 1 mes hacia atrás. • Mantener el último respaldo completo de cada mes.
DB	Diferencial	• Mantener todos los respaldos de las últimas 2 semanas.
DB	Incremental	• Mantener todos los respaldos de la última semana.

5. Verificar que los servidores se encuentran administrados por System Center VMM.
6. Si se encuentran administrados por VMM, solo resta subir los respaldos a la nube creada por dicha herramienta de administración.
7. Finalmente, se comprueba que los servicios estén respaldados.

La red de la propuesta

La red de la propuesta de nube privada debe incluir los servidores de virtualización que contienen todas las máquinas virtuales que a su vez fungen como servidores de los servicios que son brindados por la universidad. Además de los servidores DNS y el que proporciona las actas en línea (actasonline).

Adicionalmente, se incluye un servidor dedicado para autoservicio (SCVMM) y otro para análisis y depuración de la información y a la vez para seguridad. Todos estos aspectos detallados anteriormente.

Otro detalle que agrega la propuesta es la implementación de almacenamiento NAS. Este tipo de almacenamiento es una tecnología para compartir los servidores de una manera diferente, es decir, las aplicaciones hacen las peticiones de datos a los sistemas de archivos de manera remota mediante protocolos CIFS y NFS[5], y el almacenamiento es local al sistema de archivos. La ventaja de implementar NAS es que hace utilización de la misma infraestructura de red y requiere de una gestión sencilla.

[5] CIFS, sistema de archivo en internet común y NFS, sistemas de archivos en red.

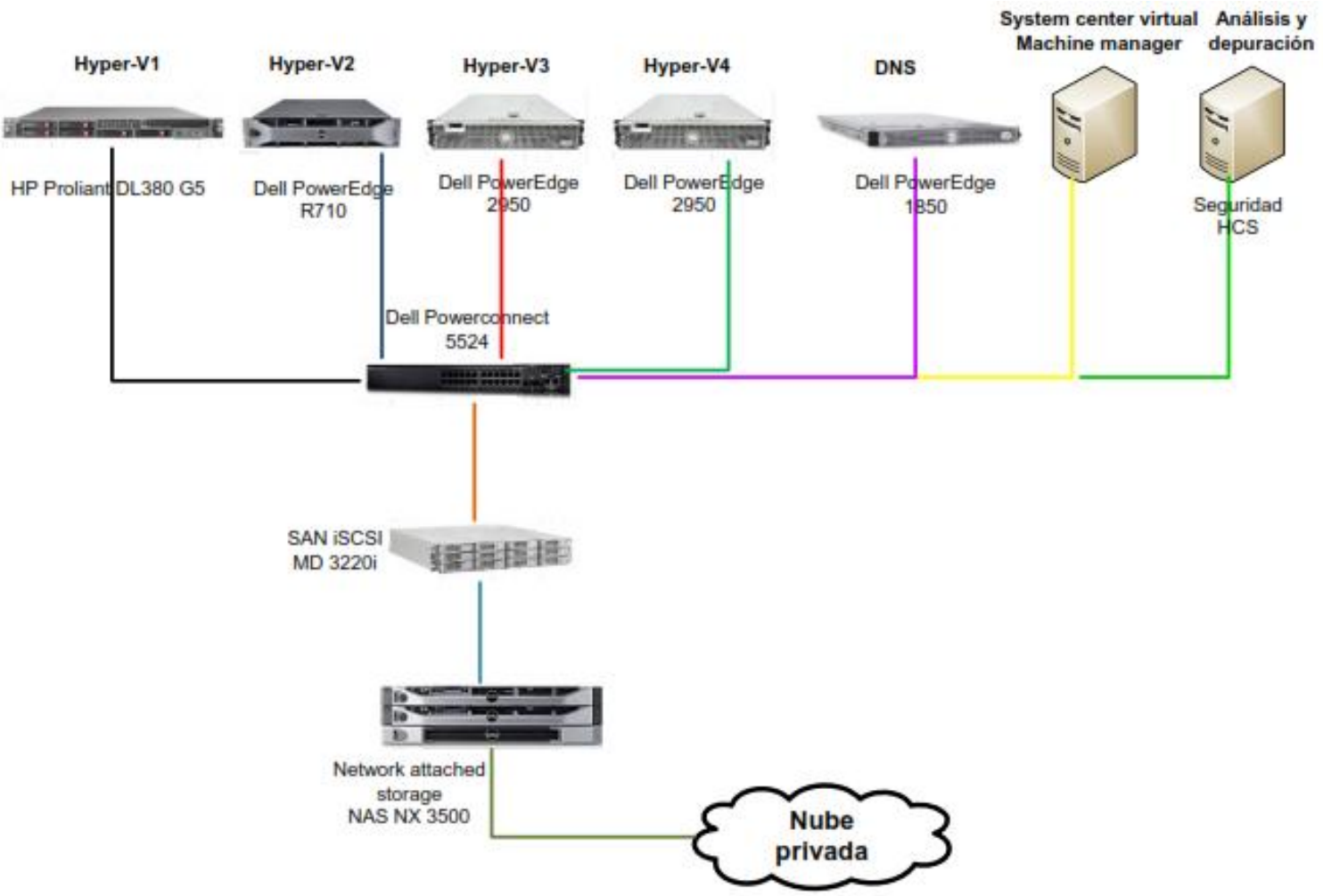

Figura 38. Esquema de red con los dispositivos que componen la propuesta de nube privada.

3. CONCLUSIONES

Construir una nube privada con las herramientas necesarias implica mucho trabajo de configuración, unir la configuración con la familia del hypervisor y encontrar las formas de agregar pools de recursos para que sean fácilmente disponibles mediante las instancias necesarias. Es necesario que el data center institucional se adapte a las nuevas exigencias de la universidad, atendiendo al creciente volumen de información que se maneja, la necesidad de contar con una rapidez y agilidad de respuesta cada vez mayor, sin que ello repercuta en una mayor complejidad en el entorno de TI de dicho centro de datos.

Con todo esto, la implementación de nube privada en el centro de datos de la UNAN-Managua aportaría beneficios claros: flexibilidad, al aprovisionar servicios según demanda y dimensionar la infraestructura dependiendo de las necesidades; un agrupamiento de los recursos, permitiendo obtener mayores niveles de automatización, aprovisionamiento y orquestación; una infraestructura escalable, que garantice el control sobre los datos; una reducción de las cargas de trabajo (*workloads*) y tareas de administración del sector de TI y todos estos beneficios reaprovechando la infraestructura existente. Lo más importante para tener en consideración es que la infraestructura de nube privada no es conjunto de tecnologías si no que es un modelo para implementar, administrar y utilizar recursos y servicios de tecnología de información.

Se propuso una técnica de replicación que sea accesible para el centro de datos, económicamente viable y que cumpla con los objetivos necesarios además de que posea tanto RTO como RPO bajos evitando grandes pérdidas de datos.

Tener establecida una estrategia de replicación es una práctica recomendable cuando se quiere tener protegidos los datos, prestar alta disponibilidad de servicios y evitar interrupciones de trabajo por fallos al tener un sitio remoto donde se mantengan activos todos los servicios en caso que fallen los equipos del centro de datos institucional por causas humanas, accidentales o naturales.

La ejecución de una estrategia de replicación de datos es obligatoria brindando beneficios directos como continuidad del negocio (de todos los servicios telemáticos de la UNAN-MANAGUA), siendo posible por la consolidación de servidores.

La tecnología de virtualización reduce los costos de un plan de continuidad de negocio (BC) y minimiza los tiempos fuera de operación. Así, teniendo un data center virtualizado, una estrategia de replicación establecida y una nube privada se logra un ambiente seguro.

4. BIBLIOGRAFÍA

- Consulting-cloud-ep. 2010. Extraído el 13 de Noviembre de 2012 de http://puertorico.emc.com/collateral/emc-perspective/h6870-consulting-cloud-ep.pdf
- OMEL. 2010. FAQ-Cloudcomputing. Extraído el 17 de Noviembre del 2012 de http://upcommons.upc.edu/eprints/bitstream/2117/10793/1/nubes%20privadas%20en%20plataformas%20virtualizadas.pdf
- Infraestructura como servicio (Iaas) en el cloud computing. 2011. Extraído el 08 de Octubre del 2012 de http://www.error500.net/software/infraestructura-como-servicio-iaas-cloud-computing
- Pressman, Roger S. Ingeniería del Software: Un enfoque práctico. Sexta Edición. McGraw Hill. México. 2007.
- Karen.Morales. 2008. Estandares data center. Extraído el 18 de Agosto de 2012 de http://www.google.com.ni/#hl=es-419&sclient=psy-ab&q=tesis+de+virtualizacion+para+data+center+pdf&oq=tesis+de+virtualizacion+para+data+center+pdf
- Rob. 2008. Data_Protection_Strategies_Using_Replication_Whitepaper. Extraído el 15 de octubre de 2012 de http://www.bcap.com.au/en/Products/DoubleTakeApplicationAvailabilityDTAM.aspx
- Starwind Software. 2012. Providing HA shared storage for Hyper-V. Extraído el 17 de Octubre de 2012 de http://www.starwindsoftware.com
- Rob. 2009. DBTK_Virtual_Systems_DR_Whitepaper. Extraído el 15 de octubre de 2012 de http://www.bcap.com.au/DocExt1/products/Software/Double-take_Software/Double-Take/Whitepapers/20091511-DBTK-EN-DBTK_Virtual_Systems_DR_Whitepaper.pdf
- Hyperoo. 2012. Hyperoo2_Gettingsatarted. Extraído el 20 de septiembre de 2012 de http://www.hyperoo.net
- Wiley. 2008. Mastering Hyper-V deployment. Extraído el 02 de Octubre de 2012 de http://www.hdspex.com/free-pdf-mastering-hyperv-deployment/
- Swhite. 2005. TIA-942. Extraído el 05 de Octubre de 2012 de http://www.tia.org
- IDG communications. 2012. Hablando Cloud: El punto de referencia sobre el cloud computing y la nube privada. Extraído el 26 de Noviembre de 2012 de http://www.idg.es/whitepapers/Cap1_Wp_microsoft_2012.pdf

5. ANEXOS

ANEXO A

Universidad Nacional Autónoma de Nicaragua

Entrevista sobre nube privada y respaldo (backup).

Fecha: 10/12/12 Hora: 2 P.M

Lugar: Oficinas proyecto TIC

Entrevistado (a): Ing. Ángela López Torrez

Introducción

La presente entrevista se realiza con el propósito buscar información sobre la implementación de sistemas de respaldo y nube privada. Está dirigida a personal de TIC y se seleccionó por su alta relación con el centro de datos donde se realiza el estudio. Los datos recolectados se utilizarán para validar la investigación y analizar dichos datos.

1. ¿Está preparado el data center para un desastre natural o accidental?

   No creo que esté preparado para un desastre.

2. ¿Sabe usted de si existe algún plan de contingencia ante un desastre descrito anteriormente?
   No se posee un plan de contingencia, lo cual hace vulnerable al data center.

3. ¿Considera -a su juicio- que la Universidad (UNAN) invierte lo suficiente para enfrentar este tipo de situaciones?

   Para los desastres, no se ha invertido en equipos de respaldo de información.

4. ¿Conoce usted de alguna institución, empresa o escuela de educación superior que haya enfrentado la situación de recuperar datos y disponibilidad de servicios después de un desastre para garantizar la continuidad del negocio?
   De manera personal, no conozco.

5. ¿Suponiendo que la universidad no posea un plan de contingencia, considera que el personal de tecnologías de información (TI) está:
   a. Capacitado
   b. No capacitado
   c. En proceso

R. Capacitado.

6. Desde su punto de vista, ¿qué es un sistema de respaldo?
   Lo interpreto como un sistema basado en realizar copias de seguridad de acuerdo a un tiempo establecido.
7. ¿Cree usted que es esencial ejecutar un plan de respaldo? Por qué?
   Por supuesto. En mi opinión debería ser obligatorio porque asegura la recuperación en caso de pérdidas.
8. ¿Qué significa para usted la nube privada?

   Es un modelo basado en recursos computacionales que últimamente se está implementando con mucha frecuencia por sus características y que mejora la agilidad del TI.

Matriz de datos #1

Unidad de análisis	Variables		
	Sí	**No**	**Desconoce**
UA1		X	
UA2		X	
UA3		X	
UA4			X
UA5	X		
UA6	X		

Referencia de la matriz de datos #1
UA=unidad de análisis
UA1: Data center preparado. **UA2:** Existe plan contra desastres. **UA3:** Hay inversión para plan de desastres. **UA4:** Antecedentes contra desastres. **UA5**: Personal de TI capacitado. **UA6**: Esencial plan de respaldo.

Universidad Nacional Autónoma de Nicaragua

Entrevista sobre respaldo (backup) y replicación de datos.

Fecha: 13/12/12 Hora: 8:40 A.M

Lugar: Oficinas Laboratorio informática Medicina

Entrevistado (a): Ing. Patricia Delgado.

Introducción

La presente entrevista se realiza con el propósito buscar información sobre la implementación de estrategias de replicación y respaldo de datos. Está dirigida a la responsable de informática de la Facultad de Ciencias Médicas y se seleccionó por su alta relación con el centro de datos de dicha facultad. Los datos recolectados se utilizarán para validar la investigación y evaluar las variables resultantes.

1. Desde su punto de vista, ¿qué significa un sistema de respaldo?
   En mi opinión un sistema de respaldo significa alta disponibilidad. Es decir, mantener los servicios y aplicaciones al día de forma que si se da algún fallo pueda utilizarse dicho sistema de respaldo.

2. ¿Cree usted que es esencial ejecutar un plan de respaldo?
   En lo absoluto. Pero el respaldo no debe ser solo de la información sino también garantizar los servicios y mantenerlos al día.

3. ¿Qué sabe usted de la replicación de datos?
   Entiendo que replicación es realizar una copia de datos de un sitio a otro, una manera de proteger la información.
4. ¿Conoce usted técnicas o tipos de replicación de datos? Si es así, mencione cuáles.
   Entiendo en nuestro caso específico que necesitamos una herramienta (software) para lograr replicación.
5. ¿Podría establecerse una técnica de replicación entre los centros de datos institucional y el de la facultad de ciencias médicas?
   Sí claro. Ese es uno de los objetivos primordiales de nuestro centro de datos.

Matriz de datos #2

Unidad de análisis	Variables			
	Sí	**No**	**Mucho**	**Poco**
UA1	X			
UA2	X			
UA3				X
UA4	X			

Referencia de la matriz de datos #2
UA=unidad de análisis
UA1: Esencial plan de respaldo. **UA2:** Conocimiento sobre replicación de datos. **UA3:** Conocimiento de técnicas de replicación. **UA4:** Establecimiento replicación entre los centros de datos.

ANEXO B

GLOSARIO

Data center: Un local o porción de local cuya función primaria es albergar un cuarto de cómputo y sus áreas de apoyo.

Nube: Forma metafórica de nombrar a Internet en los diagramas de red.

Nubes públicas: Los usuarios finales no conocen qué trabajos de otros clientes pueden estar corriendo en el mismo servidor.

Nubes privadas: Manejada por un solo cliente que controla qué aplicaciones debe correr y dónde. Son propietarios del servidor.

Nubes híbridas: Combinan los modelos de nubes públicas y privadas. El usuario es propietario de unas partes y comparte otras, aunque de una manera controlada.

Cloud computing: Consiste en los servicios ofrecidos a través de la red tales como correo electrónico, almacenamiento, uso de aplicaciones, etc., los cuales son normalmente accesibles mediante un navegador web.

SAAS (*Software as a service*): Es un modelo de distribución de software donde el software y los datos que maneja se alojan en servidores de la compañía de tecnologías de información y comunicación(TIC) y se accede con un navegador web o un cliente ligero especializado, a través de internet.

IAAS (*Infraestructure as a service*): La capa de "Infraestructura como servicio". Parte física de la nube. En vez de tener el equipamiento en su propio lugar de trabajo, los clientes pagan a un proveedor para que éste sea quien tenga todo ese equipamiento (llámese discos duros o equipamiento de redes) y se encargue de toda la mantención y optimización de dicho equipamiento.

PAAS (*Plattform as a service*): La capa de "Plataforma como servicio". Está muy ligada a la capa SaaS, ya que es la plataforma donde se envuelve el software que pone a disposición el proveedor y es el medio de virtualización para el hardware que el cliente arrienda. Un detalle a destacar es que, como todos los servicios se ejecutan desde esta plataforma externa, no es necesario descargar nada.

RTO *(Recovery Time Objective):* el intervalo de tiempo entre la invocación del DRP y el momento en que se considera operativo.

RTP *(Recovery Time Point):* marca la fecha y hora antes de la contingencia hasta la que podremos recuperar la información (cuántas transacciones se han perdido, frecuencia de copias de seguridad, demora de replicación).

iSCSI: El protocolo iSCSI es un estándar de internet que está definido para permitir que los comandos SCSI sean transportados sobre los protocolos TCP/IP.

RAID: Conjunto redundante de discos independientes, hace referencia a un sistema de almacenamiento que usan múltiples discos duros entre los que se distribuyen los datos.
Hot side: Servidores locales como los operacionales en el sitio remoto están activos en todo tiempo.
Warm site: Los servidores de respaldo se encuentran en el sitio remoto. Las tareas se completan cuando ocurra el modo failover.
Cold site: Sitio vacío con servidores esperando por el evento de recuperación de desastres.
Orquestador: Es una pieza de software (middleware) que permite integrar servicios provenientes de diferentes fuentes y proveer información de forma síncrona o asíncrona a través del uso de servicios web, HTML, bases de datos, archivos, entre otras fuentes.
Directorio: Es como una base de datos pero en general contiene una información más descriptiva y más basada en atributos.