Universidad Central de Venezuela
Facultad de Ciencias
Escuela de Computación
Laboratorio de Redes Móviles, Inalámbricas y Distribuidas (ICARO)

Diseño e Implementación de una Estrategia Basada en las Mejores Prácticas para la Virtualización de Servidores de una Organización

Trabajo Especial de Grado
Presentado ante la ilustre
Universidad Central de Venezuela
Por el Bachiller
Freddy Medina Majetic
para optar al título de
Licenciado en Computación

Tutor: Profa. María E. Villapol

Caracas, 14 de mayo de 2013

Universidad Central de Venezuela
Facultad de Ciencias
Escuela de Computación
Laboratorio de Redes Móviles, Inalámbricas y Distribuidas (ICARO)

ACTA DEL VEREDICTO

Quienes suscriben, Miembros del Jurado designado por el Consejo de la Escuela de Computación para examinar el Trabajo Especial de Grado, presentado por el Bachiller Freddy Medina Majetic C.I.: 18.936.315, con el título *Diseño e Implementación de una Estrategia Basada en las Mejores Prácticas para la Virtualización de Servidores de una Organización*, a los fines de cumplir con el requisito legal para optar al título de Licenciado en Computación, dejan constancia de lo siguiente:

Leído el trabajo por cada uno de los Miembros del Jurado, se fijó el día 28 de Mayo de 2013, a las 09:00 am, para que su autor lo defendiera en forma pública, en la Sala Internet II del Galpón 10, lo cual se realizó mediante una exposición oral de su contenido, y luego respondió satisfactoriamente a las preguntas que les fueron formuladas por el Jurado, todo ello conforme a lo dispuesto en la Ley de Universidades y demás normativas vigentes de la Universidad Central de Venezuela. Finalizada la defensa pública del Trabajo Especial de Grado, el jurado decidió aprobarlo.

En fe de lo cual se levanta la presente acta, en Caracas a los 28 días del mes de Mayo del año dos mil trece, dejándose también constancia de que actuó como Coordinador del Jurado la Profesora María Elena Villapol.

_____
Profa. María E. Villapol

_____ _____
Prof. Pedro Guzmán Prof. Rafael Angulo

A Freddy, Franjo, Kay, Lis y Rubén:
Lo hago por ustedes. Siempre.

Agradecimientos

Gracias de todo corazón a mi tutora, la Profesora María Elena Villapol, cuya atención y dedicación estuvieron siempre a la orden del día. Su criterio y guía fueron de utilidad en la consolidación de los objetivos metodológicos y académicos de este trabajo.

Gracias a todo el personal docente y administrativo de la Facultad de Ciencias de la Universidad Central de Venezuela, en especial de la Escuela de Computación, por su preparación y atención en todo lo referente a mi vida como alumno de pregrado.

Gracias a PricewaterhouseCoopers por su apoyo en este trabajo, tanto a su personal a nivel nacional como internacional. De manera muy especial a Ítalo Ayesterán y a Rafael Padrino, de quien he aprendido mucho bajo su tutela. Gracias por la confianza y las atenciones. Y gracias a todos mis compañeros de trabajo, excelentes profesionales de los que aprendo cada día. Gracias por la disposición y colaboración que mostraron durante el desarrollo de este proyecto.

Gracias a Carlos Zambrano, tutor de vida quien confió en mí desde el primer día. Gracias por todas las oportunidades brindadas, por el apoyo, por el criterio y confianza ofrecida en la consolidación de mis metas académicas, personales y profesionales.

Gracias a las personas que, de alguna manera u otra, han sido claves en mi vida académica: mis compañeros y amigos, Audel Dugarte y Víctor Felipe. Gracias a todos mis compañeros de clase, a mis alumnos, a mis profesores, a mis amigos. Y con especial cariño, gracias a Irena Cabanach, sin tu apoyo incondicional no hubiese podido. Mil gracias por todo.

Y por encima de todo, y con todo mi amor, gracias a los míos por estar ahí siempre junto a mí durante estos años. Gracias Isbel, Mamá, Papá, Kay, Memé, Rosa, Ben, Aylem, Julio, Franjo y Rubén. Y gracias a los que vienen, a las recién llegadas y a los que ya no están. Gracias por todo. Los quiero.

Resumen

La virtualización es una técnica que puede usarse para la consolidación de servidores y aplicaciones de propósito general que requiere de una estandarización en términos de las prácticas de instalación, configuración, gestión y mantenimiento de cada uno de los elementos que la componen. Actualmente existen un gran número de soluciones empresariales en el mundo de las tecnologías de información orientadas al desarrollo e implementación de infraestructuras virtualizadas que ofrecen diversas maneras, pasos y procedimientos para el cumplimiento de un objetivo en común: la consolidación de una plataforma virtual segura y estable que cumpla con las demandas diarias de una organización a corto, mediano y largo plazo. No obstante, debido a la gran variedad de productos y servicios dispuestos en el mercado actual es difícil determinar cuáles son los parámetros y lineamientos a seguir a la hora de decidir incursionar en la virtualización de servidores. En este trabajo se presentan una serie de planteamientos dedicados a la orientación en el proceso de migración a una infraestructura virtualizada, desarrollando una estrategia inspirada en las mejores prácticas destinada a cualquier organización que desee implantar este modelo tecnológico, tomando como referencia dos de las soluciones empresariales más notables en el mercado de tecnologías de la última década.

Tabla de contenido

Lista de figuras

Lista de tablas

Lista de códigos

1. Introducción

Uno de los principales objetivos de las organizaciones de pequeño y gran tamaño de los últimos años es la consolidación de un centro de datos que incluya un conjunto amplio de servidores y aplicaciones, dispuestos en una plataforma de red de comunicaciones y almacenamiento lo bastante segura y estable, de manera de poder satisfacer con las demandas de sus actividades de negocio diarias. La virtualización es una de las tecnologías con mayor auge de la última década en términos de ofrecer soluciones para la implementación de una infraestructura tecnológica que permita incrementar los niveles de eficiencia y rendimiento de los sistemas bajo una estructura de procesamiento, almacenamiento, comunicación y compartición de recursos fácil de gestionar y lo suficientemente escalable para pensar en desarrollos, mejoras e implementaciones a futuro.

1.1. Definición del problema

A pesar de que la virtualización no es un concepto nuevo, hoy en día ha tomado un nuevo auge por la necesidad de aprovechar mejor los recursos con que cuenta las computadoras hoy en día. Sin embargo, no existe una manera clara y bien definida para llevar un proyecto de virtualización sobre todo cuando el mismo involucra la migración de varios servicios y servidores a un ambiente virtualizado. Por lo cual con este trabajo se busca resolver el problema de la sistematización del proceso de migración de servidores y servicios a ambientes virtualizados a través de un conjunto de lineamientos específicos.

Para llevar a cabo un proyecto de virtualización en una organización, es primordial el desarrollo de una estrategia que considere diversos tópicos dentro de la infraestructura tecnológica. El solo hecho de plantear la posibilidad de implementar la virtualización implica el estudio de una serie de condiciones que requieren de una planificación eficaz y una metodología que soporte los grandes cambios implícitos en este proceso.

Particularmente, la entidad organizacional que fue sometida a los planteamientos expuestos en este documento cuenta con una plataforma física que aloja varias de las aplicaciones que soportan las actividades de negocio diarias. Con un contrato de mantenimiento próximo a vencer y una serie de proyectos a consolidar, se optó por incursionar en la virtualización de servidores en la nueva generación de plataformas adquiridas, permitiendo la adopción de más aplicaciones y servicios alojados en un único sistema más robusto, de administración centralizada y diseñado para el crecimiento a futuro.

Sin embargo, la poca experticia en el tema, diversos entornos operativos por consolidar y la necesidad de migrar los ambientes críticos a un ambiente más seguro supuso requerir una planificación del proyecto diseñada para satisfacer las necesidades de la organización en términos de tiempo de implementación y ahorro de costos, justificando así el retorno de la inversión realizada.

Por otra parte, dado que la virtualización es una tecnología que invoca nuevas terminologías y procedimientos, así como hace uso de diversos recursos tecnológicos críticos como procesamiento, almacenamiento y comunicaciones, la organización tuvo la necesidad de contar con una documentación que planteará un conjunto de mejores prácticas que sostuviesen los mecanismos de instalación, configuración y mantenimiento adaptadas a su infraestructura, así como el rendimiento de los sistemas, la facilidad en su gestión, los mecanismos de seguridad de datos, respaldos de información, recuperación ante desastres y la posibilidad de incrementar a futuro, en orden con el cumplimiento de las políticas de seguridad y resguardo de la información de la misma.

1.2. Justificación

El proceso de adopción y migración a una infraestructura virtual no es una tarea fácil. Siendo la principal meta la consolidación de una plataforma acorde a las necesidades de la organización, es necesario seguir a cabalidad un conjunto de procedimientos claramente definidos. De acuerdo a esto, se requiere seguir un conjunto de mejores prácticas en términos de configuración de hardware, instalación de software, cuantificación de riesgos y categorización de servidores y aplicaciones, acordes a las características de la organización y que permita cumplir con los objetivos planteados.

Si bien es cierto que la adquisición de una tecnología para virtualizar trae consigo un material documentado que dispone de una serie de pasos dedicados a la orientación en el proceso de instalación y configuración, así como de las mejores prácticas para la gestión de la misma, es requerido que dicho material sea acondicionado a la infraestructura de la organización, de manera de definir cuales procesos de instalación, configuración y gestión son los adecuados.

Por otra parte, las mejores prácticas para la virtualización no sólo se limitan al desarrollo de procedimientos de instalación, configuración y gestión adecuados. También deben exponer las etapas en las que un proyecto de este tipo debe ser planificado, donde cada etapa requiere el cumplimiento de diversas tareas orientadas al cumplimiento de principios básicos de seguridad de información, asegurando así un desarrollo acorde a los planteamientos de una entidad organizacional.

En términos generales, con toda esta información debidamente documentada y al alcance, así como la debida tecnología y personal capacitado, una organización puede contar con los requisitos que permitirán orientar un proyecto de virtualización de servidores en la dirección correcta, facilitando la implementación de nuevos modelos de gestión, tareas de resguardo y mantenimiento, con el fin de adoptar una plataforma adecuada que aproveche de la mejor manera los recursos disponibles y pueda mantener un nivel de estabilidad acorde a nuevos planes y proyectos y asegurando un crecimiento que se adapte rápidamente a los requerimientos futuros.

1.3. Objetivo general

El objetivo general de este trabajo es:

Desarrollar una estrategia basada en las mejores prácticas de gestión, seguridad y resguardo de información que permita orientar a una entidad empresarial en la consolidación de un proyecto de virtualización de servidores de propósito general.

1.4. Objetivos específicos

Los objetivos específicos de este trabajo son:

- Familiarizarse con el conjunto de servidores de la organización y determinar los requerimientos de los mismos, a fin de determinar candidatos a ser virtualizados, basándose en una determinada categorización.

- Virtualizar los servidores elegidos, considerando las migraciones de sistemas físicos a virtuales, así como las nuevas implementaciones.

- Evaluar los resultados obtenidos en términos de procesamiento, memoria, red y almacenamiento.

- Consolidar una estrategia basada en las mejores prácticas basada en los diferentes componentes de la virtualización, considerando los procedimientos ejecutados durante el desarrollo del proyecto.

Con la finalidad de alcanzar estos objetivos, este documento se encuentra organizado de la siguiente manera:

Capítulo 2: Ofrece una reseña de los conceptos presentes en la virtualización de servidores, así como de las tecnologías de hardware y software adoptadas en términos de rendimiento, compatibilidad y funcionalidad.

Capítulo 3: Plantea el problema presente en el ambiente de ejecución del proyecto y el esquema propuesto, estableciendo los objetivos y las etapas de desarrollo e implementación a consolidar, de acuerdo a la metodología adoptada.

Capítulo 4: Expone los procesos de implementación ejecutados en términos de instalación, configuración y resultados obtenidos, de acuerdo a las etapas planteadas. Identificando los recursos de los componentes de la infraestructura sometida al cambio y categorizando de acuerdo a criticidad.

Capítulo 5: Presenta la estrategia de virtualización basada en mejores prácticas propuesta, basada en su alcance y desarrollo metodológico. Considerando aspectos técnicos de seguridad, hardware, software, sistemas e infraestructura.

Capítulo 6: Conjunto de conclusiones obtenidas durante el desarrollo del proyecto de virtualización de servidores en una organización en particular y de los planteamientos expuestos en la estrategia propuesta.

2. Virtualización de Servidores

La industria de las tecnologías de información ha tenido un incremento considerable en los últimos años, sobre todo en cuanto a sus niveles de complejidad. Esto ha producido una evolución incremental en los componentes de hardware y software orientados a la consolidación de nuevas redes de comunicaciones y de servicios.

Un ejemplo de las nuevas tecnologías que ha surgido y que, particularmente ha retomado el auge perdido en la década pasada, es la virtualización. Una técnica que combina las virtudes de la emulación de hardware en conjunto con la consolidación de diversos ambientes operativos en una única unidad de procesamiento dedicada a la compartición de recursos y ejecución simultanea de sistemas.

Una de las ramas de esta tecnología es la virtualización de servidores, una técnica que ofrece un amplio número de posibilidades sobre la gestión de un centro de datos ya que dispone de mecanismos automatizados que pueden explotarse a la hora de controlar y monitorear tareas que involucren ambientes virtuales en ejecución orientados al cumplimiento de demandas empresariales.

Son muchos los mecanismos y procedimientos que una organización ó entidad pueden aplicar para la consolidación de esta tecnología, desde elegir una plataforma que pueda sostener la ejecución de sistemas virtuales hasta las aplicaciones de procedimientos de gestión para el control de los mismos. Sin embargo, es necesario definir cada uno de los componentes principales que utiliza antes de implementarla a plenitud.

2.1. Componentes de la virtualización

Un concepto fundamental en la virtualización es el de máquina virtual. Este término ha sido usado por múltiples tecnologías de información a lo largo de los años. Consiste en la consolidación de un sistema autónomo dentro de un sistema físico. Es decir, una máquina virtual es una máquina cuya arquitectura, funcionamiento y recursos son dispuestos por una máquina real, encargada de alojarla y de asegurar su ejecución, usando un nivel de abstracción adecuado.

Es por ello que el concepto de “virtual” se refiere a la implementación de un sistema dentro de otro sistema, particularmente se trata de una implementación que, en principio se basa en software, ya que una máquina virtual es capaz de disponer una plataforma que aloje y ejecute un sistema operativo, por lo que también puede ejecutar aplicaciones y servicios, independientemente del funcionamiento de la máquina real que la soporte.

Son muchas las ventajas que la implementación de máquinas virtuales ofrece, desde que la posibilidad de ejecutar múltiples sistemas operativos en el mismo computador es posible. Una de las aplicadas frecuentemente es la consolidación de servidores virtuales, permitiendo cambiar el modo tradicional de establecer diferentes máquinas que ejecuten servicios particulares por separado, a definir diferentes máquinas virtuales que ejecuten dichos servicios en una única máquina real [1].

Dentro de la virtualización de servidores, las máquinas virtuales forman parte de un conjunto de elementos que conforman una plataforma virtual. Este conjunto incluye nuevos elementos como los sistemas anfitriones y programas de control. A continuación, se definen cada uno de ellos.

2.1.1. Sistema invitado

Por su parte, una máquina virtual se conoce como sistema invitado. Una ó varias máquinas virtuales pueden ejecutarse de manera ininterrumpida ya que son independientes entre sí y

desconocen su condición de ser “virtuales”. Todo esto es posible ya que debe existir un nivel de abstracción entre sistemas invitados, así como entre sistemas invitados y el sistema anfitrión. Este nivel de abstracción es dispuesto por un sistema adicional conocido como programa de control ó hypervisor

2.1.2. Sistema anfitrión

Para poder soportar una implementación de máquinas virtuales en función de una consolidación de servidores virtuales, es necesario determinar los componentes involucrados y cuáles son las soluciones en el mercado que permiten la gestión de los mismos. Por ejemplo, los sistemas que alojan las máquinas virtuales se conocen como sistemas anfitriones ó hosts. Un host es un sistema físico, capaz de soportar la ejecución simultánea de máquinas virtuales mediante la compartición de sus recursos de procesamiento, almacenamiento y demás.

2.1.3. Hypervisor

Un hypervisor, programa de control ó gestor de máquinas virtuales es un componente esencial en términos de virtualización de ambientes operativos. Puede ser un sistema operativo, parte de una aplicación ó un componente de hardware que permite la creación y ejecución de máquinas virtuales en sistemas físicos. Existen dos tipos de programas de control ó hypervisores, de acuerdo a los planteamientos de Gerald J. Popek y Robert P. Goldberg: hypervisor de tipo 1 e hypervisor de tipo 2 [2].

Un hypervisor de tipo 1 ó nativo (tipo bare-metal) se ejecuta directamente en el hardware del sistema anfitrión, lo que le permite controlar los recursos físicos del mismo y gestionar los sistemas invitados, los cuales se ejecutan a un segundo nivel del hardware. Este modelo es el más común a la hora de implementar una arquitectura basada en máquinas virtuales, donde productos como Oracle VM Server, XenServer, VMware ESX/ESXi y Microsoft Hyper-V lo han adoptado.

Por su parte, un hypervisor de tipo 2 ó alojado, se ejecuta en un sistema operativo convencional haciendo que las máquinas virtuales se ejecuten en un tercer nivel del hardware del sistema anfitrión. VMware Workstation y Oracle VirtualBox son ejemplos de hypervisores de tipo 2.

2.2. Planteamientos generales

Cuando se trata de elegir la tecnología adecuada para la consolidación de una plataforma de tecnologías de información basada en la virtualización, son muchos los planteamientos que deben ser tomados en cuenta en función de determinar los requisitos que se desean cumplir y el costo asociado a los mismos. Sin embargo, la virtualización es una tecnología conocida por los diversos beneficios que ofrece en el centro de datos que la implemente. La reducción de costos en hardware es un ejemplo de ello, ya que permite ofrecer diversos servicios en un único sistema de procesamiento, en lugar de tener varios de ellos [3].

Otro ejemplo es la optimización en el uso de los recursos. En una plataforma con sistemas tradicionales, los requerimientos de recursos varían en intervalos de tiempo. Mientras que un recurso está saturado por peticiones de usuario, otro similar puede estar subutilizado [10]. La virtualización permite gestionar estos inconvenientes mediante la asignación dinámica de recursos entre sistemas operativos, conforme a sus necesidades.

Entre los planteamientos generales a tomar en cuenta a la hora de elegir una tecnología de virtualización en específico se encuentran:

2.2.1. Respecto a sistemas operativos

El programa de control elegido debe soportar la ejecución de diversos sistemas operativos, el cual debe estar diseñado de acuerdo a que sistemas operativos pueden ejecutarse sobre él. Sin embargo, otros sistemas operativos pueden ejecutarse incluso si el programa de control no está específicamente diseñado para ello [4]. En caso de una falla de estos sistemas, el soporte asociado al programa de control no será capaz de determinar las causas ni proveer de una solución particular.

Adicionalmente, ciertos sistemas operativos pueden ser notificados de la presencia de un programa de control, los que les permite ejecutarse de una mejor manera a través de una interacción más eficiente.

2.2.2. Respecto a los controladores

Si el programa de control se elegido se ejecutará directamente en el hardware del sistema anfitrión y será el encargado de gestionar los sistemas invitados, debe tener a su disposición todo un conjunto de software destinado al control del hardware subyacente.

Muchos programas de control soportan un conjunto limitado de componentes de hardware que serán expuestos las máquinas virtuales, lo que puede significar un inconveniente si se requiere de la representación de un componente en particular. Sn embargo, existen soluciones para estos inconvenientes. Por ejemplo, los programas de control de tipo 2 toman ventaja de esta situación al utilizar los controladores del sistema operativo instalado en el sistema anfitrión [5].

2.2.3. Respecto a la facilidad de gestión y soporte

Aspectos como la seguridad, asignación de recursos y la instalación de sistemas operativos son algunos de los temas que juegan un papel importante a la hora de adoptar un programa de control que gestione los ambientes virtuales. La interfaz de usuario debe ser lo suficientemente amigable para que un administrador con conocimientos técnicos básicos pueda usarla.

En caso de que la indisponibilidad de los sistemas cause perdidas razonables en las actividades de negocio, definitivamente el objetivo es adquirir un producto que cuente con soporte de tipo profesional [6]. En caso de que la virtualización se implemente en escenarios pequeños orientados a pruebas, el soporte es un aspecto secundario que puede ser tomado en cuenta posteriormente.

2.3. Tecnologías de virtualización

Tomando en cuenta los lineamientos anteriores, se pueden considerar diversas tecnologías de virtualización presentes en el mercado actual para determinar si pueden satisfacer las necesidades del centro de datos que desee consolidar una plataforma virtual. A continuación se ofrece una breve reseña de tres de las soluciones con mayor impacto en la industria.

2.3.1. XenServer

XenServer es una tecnología de virtualización basada en software libre. Fue desarrollada inicialmente en el Laboratorio de Computación de la Universidad de Cambridge y actualmente está disponible bajo una licencia GPL.

Dada su condición de ser software de carácter libre, XenServer ha sido usado ampliamente y cuenta con una gran comunidad dedicada a su soporte. La mayoría de las industrias desarrolladoras de componentes de chips (como Intel y AMD, por ejemplo) han contribuido en el código fuente de XenServer con el fin de habilitar su ejecución en diversas arquitecturas.

XenServer requiere de un sistema operativo anfitrión para poder ser instalado. Esto significa que si se requiere la ejecución de ciertos sistemas operativos usando XenServer como plataforma de virtualización, estos deben ser notificados de que serán ejecutados sobre un programa de control y no sobre el hardware [7], lo que no representa un inconveniente desde que existen muchos sistemas operativos que disponen de paquetes adicionales para ser notificados (un ejemplo de ello son los sistemas operativos de software libre tales como Ubuntu).

Con respecto a los controladores, XenServer ofrece una ventaja interesante. Para permitir su ejecución, uno de los sistemas operativos invitados debe ser identificado como “dom0”, de manera de que toda la gestión de controladores de dispositivos recaerá en este sistema. Para lo cual, el sistema dom0 es usualmente Linux y es capaz de interactuar con todos los sistemas invitados. Como los demás sistemas conocen de la existencia del sistema dom0, los controladores están al tanto de que no se ejecutan sobre el hardware real, permitiendo la generación de instrucciones apropiadas.

Comparado con otras tecnologías de virtualización como VMware, XenServer es notablemente más rápido y puede alojar más sistemas invitados [7]. La velocidad con la que un sistema invitado se ejecuta sobre XenServer es generalmente igual que la de un sistema Linux, ejecutándose directamente en el hardware. Adicionalmente, XenServer cuenta con una variedad de herramientas de gestión y soporte. Sin embargo, cuenta con una versión Enterprise paga a través de la organización Citrix Systems, ideal para ambientes de producción.

2.3.2. Microsoft Hyper-V

Microsoft es relativamente nueva en el negocio de la virtualización, pero cuenta con una posición dominante sobre el mundo de la computación, los que les hace acreedora de cierta ventaja sobre la competencia. La tecnología de virtualización que propone es conocida como Microsoft Hyper-V.

El núcleo de Hyper-V está disponible como descarga libre desde Octubre del año 2008, dado de que su interfaz es basada en texto. De hecho, se pueden adquirir versiones de Windows Server 2008 con Hyper-V embebido [8]. Naturalmente, no es un producto gratis, pero cuenta con funciones importantes para la gestión de sistemas. La arquitectura de esta tecnología al igual que XenServer, requiere de un sistema invitado para ser designado como sistema operativo principal. De acuerdo a la terminología de Microsoft, este sistema es conocido como partición principal. Sin embargo, a diferencia de XenServer, esta partición principal debe ser un sistema Windows Server 2008.

Adicionalmente, Microsoft Hyper-V sólo se ejecuta en procesadores basados en 64 bits que tienen soporte para virtualización. Los sistemas invitados deben ser advertidos de su presencia, soportando sólo sistemas Windows y Linux SUSE [8].

Como la partición principal es una versión de Microsoft Windows Server 2008 y los demás sistemas son advertidos, estos pueden hacer uso del conjunto de controladores dispuestos por Windows Server, el cual soporta la mayoría de los componentes de hardware disponibles. Las comunicaciones entre invitados y la partición primaria se hacen a través de buses virtuales, lo que facilita las peticiones de entrada y salida al hardware.

En comparación con otras tecnologías como XenServer y VMware, Hyper-V es un poco lento. Esto es una consecuencia del complejo código en el que está basado Windows Server 2008 [44]. Sin embargo, cuenta con una interfaz de usuario con diversas herramientas para gestionar y controlar los sistemas operativos invitados.

2.3.3. VMware ESXi

Tanto ESXi como su versión anterior ESX son sistemas operativos que funcionan como programas de control de máquinas virtuales diseñados por VMware. Están diseñados para ser implementados en ambientes de producción, debido a la variedad de funcionalidades que ofrecen. Particularmente, ESXi es parte de la suite de productos VMware vSphere [39], contando con una arquitectura ligera ya que no depende de un sistema operativo de propósito general. Está diseñado para ser un sistema simple orientado a la gestión centralizada de ambientes virtuales.

VMware ESXi se instala directamente en el hardware del sistema anfitrión, creando una capa de abstracción entre hardware y sistemas operativos invitados. Un sistema físico que aloje ESXi permite la ejecución de múltiples máquinas virtuales portables que funcionan de manera independiente, cada una representando un sistema autónomo con procesadores, memoria, red, almacenamiento y BIOS que permite la instalación y ejecución de sistemas operativos completos y demás aplicaciones [9].

A pesar de ser un programa de control nativo, ESXi no es capaz de gestionar las máquinas virtuales por sí mismo. Requiere de un conjunto de herramientas de gestión provistas por la suite vSphere para la administración, control, monitoreo, respaldo y recuperación de los sistemas virtuales.

A diferencia de otros sistemas de tipo hypervisor, las funciones de gestión de ESXi, y de todo el entorno vSphere se realiza a través de herramientas de gestión remota sin la necesidad de un sistema operativo adicional. Entre sus capacidades y funciones mas destacas se encuentran [31]:

- Poco espacio en disco
- Independencia de sistemas operativos y controladores
- Gestión avanzada de memoria
- Gestión avanzada de almacenamiento
- Alta escalabilidad de E/S

En un principio, esta arquitectura se basaba en un núcleo de virtualización, conocido como VMkernel y un gestor de particiones conocido como sistema operativo de consola (*Console Operating System*). El objetivo principal de este sistema era proveer una interfaz de gestión dentro del host, donde varios agentes de gestión de VMware se implementan en conjunto con otros servicios.

- **VMkernel**

En la actualidad, la arquitectura de ESXi sólo se basa en el VMkernel, por lo que los agentes de VMware se ejecutan directamente en él y los servicios de infraestructura se proveen a través de módulos nativos [30]. Los módulos adicionales, tales como controladores de hardware y componentes para monitoreo del mismo, pueden ejecutarse en el VMkernel. Sin embargo, sólo los módulos aprobados y asignados por VMware son permitidos en el sistema, creando una arquitectura cerrada que previene de ejecuciones de código arbitrarias en un host vSphere.

En la figura 2.1, tomada [31] de se muestra la disposición de los componentes del sistema ESXi en función del VMkernel

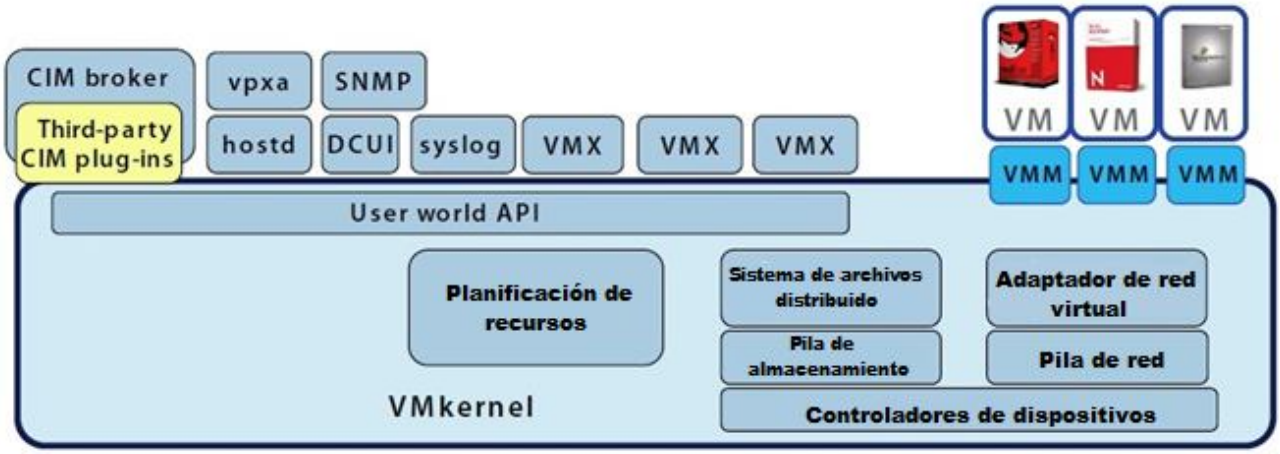

Figura 2.1: Componentes de la arquitectura ESXi

El VMkernel es el encargado de crear y controlar procesos, señales, sistemas de archivo e hilos de ejecución. Tiene el control de todo el hardware del servidor en donde es instalado y gestiona estos recursos para las aplicaciones del mismo [31]. Esta diseñado específicamente para soportar la ejecución de múltiples máquinas virtuales y proveerlas de funciones como:

- Gestión de recursos
- Pilas de ejecución de E/S
- Gestión de controladores de dispositivos

Los procesos principales que se ejecutan en el VMkernel son los siguientes:

- Una interfaz de usuario basada en consola para ejecutar tareas de configuración y gestión a bajo nivel. Es accesible a través de una consola del servidor (ò consola de servicio) y es usada, inicialmente, para configuraciones básicas.

- Un monitor de máquinas virtuales que provee un ambiente de ejecución para la ejecución de las mismas. Es conocido como VMM.

- Un proceso adicional de ayuda para complementar el monitor de máquinas virtuales. Es conocido como VMX.

- Varios agentes para la gestión de alto nivel de la infraestructura VMware vía aplicaciones de gestión remota.

- Un modelo de gestión que agrupa un conjunto de APIs estandarizadas que sirve como interfaz para la gestión del hardware vía aplicaciones de gestión remota.

- **Sistema de archivos**

El VMkernel usa un sistema de archivos simple alojado en memoria que alberga los archivos de configuración del sistema ESXi, archivos de registro y parches instalados. La estructura del sistema de archivo está diseñada para ser la misma usada en la consola de servicio [31].

El sistema de archivos es independiente al sistema de archivos usado para almacenar máquinas virtuales (conocido como VMFS) [32]. Un datastore VMFS puede ser creado en el disco local del host ó en una entidad de almacenamiento compartido.

Las interfaces de líneas de comando remotas permiten la gestión de archivos para ambos, tanto para el sistema de archivos en memoria y para el datastore VMFS. El acceso al sistema de archivo

es implementado vía instrucciones get y put del protocolo HTTPS, usando autenticación de usuarios y grupos locales del servidor y controlados con privilegios locales. Como el sistema de archivos en memoria no es persistente, ESXi tiene la capacidad de configurar un servidor syslog remoto, habilitando el almacenamiento de toda la información de registros en un sistema externo.

- **Interfaz de usuario basada en consola**

Es una interfaz de usuario local dispuesta sólo en la consola de un sistema ESXi. Muy similar a un BIOS, con un menú de usuario para la interacción con el sistema [30]. Su propósito principal es la configuración inicial y la resolución de problemas.

Entre sus tareas de configuración se incluyen:

- Configurar credenciales administrativas
- Configurar parámetros de red (En caso de que no se haga mediante el protocolo DHCP)

Entre sus tareas de resolución de problemas (troubleshooting) están:

- Llevara a cabo pruebas de conectividad a la red
- Ver los registros (logs)
- Reiniciar agentes y servicios
- Restauración de configuraciones

La intención es que sea usada para configuraciones pequeñas, dejando el resto a aplicaciones de gestión remota tales como el cliente de vSphere. A continuación se definen los componentes que están presentes en la imagen del sistema ESXi [31]:

- Una partición de 4 MB que se ejecuta cuando el sistema arranca por primera vez (*bootloade*r)
- Una partición de 48 MB que contiene 32 MB de código fuente, en conjunto con una segunda partición alternativa del mismo tamaño
- Una partición de almacenamiento de 540 MB que aloja varias aplicaciones como el cliente de infraestructura virtual y herramientas de gestión de imágenes propias de VMware
- Una partición de 110 MB para desechos, la cual normalmente está vacía pero puede alojar información de diagnostico en caso de problemas en el sistema.

La figura 2.2, tomada de [31] muestra la disposición de las particiones que conforman el diseño de ESXi.

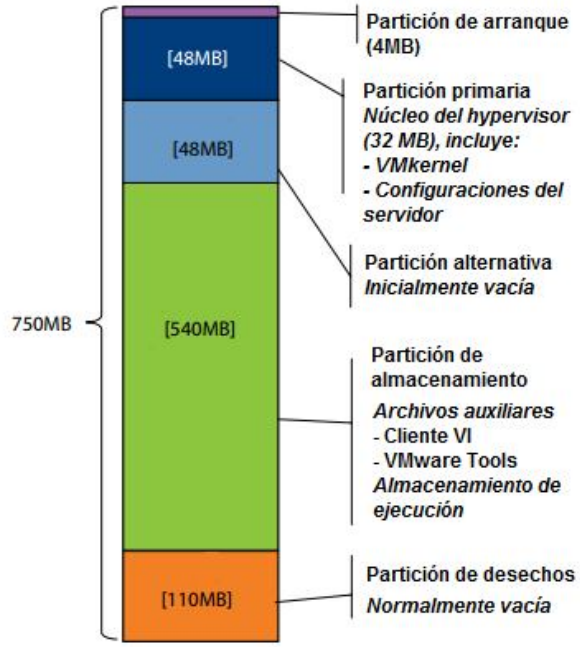

Figura 2.2: Diseño del sistema ESXi

Los sistemas ESXi tienen dos particiones independientes en memoria, cada una almacenando la imagen del sistema completa para la aplicación y pruebas de actualizaciones. Cuando se actualiza el sistema, la nueva versión es cargada en la partición inactiva y a su vez, es configurada para ser cargada y ejecutada cuando el sistema reinicie [31]. Si algún problema es detectado durante el proceso de arranque, el sistema automáticamente inicia en la partición original.

- **Funcionamiento**

Para describir el funcionamiento de los sistemas para virtualizar, deben exponerse los diferentes procesos involucrados en la gestión y mantenimiento de ambientes virtuales. VMware vSphere cuenta con una secuencia de arranque especifica [31].

Cuando el sistema inicia por primera vez, el VMkernel detecta los dispositivos y selecciona los controladores adecuados para ellos. Además descubre los discos locales presentes y, si el disco está vacío, lo formatea para que pueda almacenar máquinas virtuales.

Durante esta primera ejecución, el VMkernel crea automáticamente los archivos de configuración usando valores por defecto (por ejemplo, usa DHCP para obtener información de la red). Sin embargo, los usuarios pueden modificar estos valores a través de la interfaz de consola directa ó con herramientas de gestión de VMware.

Esta configuración es almacenada en una parte específica de los módulos de memoria usada para lectura y escritura. En los arranques subsecuentes, el sistema encuentra la configuración en dicha memoria persistente. En el resto del proceso de arranque, el sistema es inicializado y el sistema de archivos es creado en memoria. Los controladores de hardware son cargados, los agentes y servicios se inician y finalmente, el proceso de interfaz de usuario basada en consola es iniciado.

Una vez que el sistema está arriba y se está ejecutando, todas las operaciones de rutina se ejecutan con regularidad. Sólo las actividades de gestión y configuración se tienen que llevar a cabo usando aplicaciones diseñadas para ello, como el cliente de infraestructura virtual.

2.4. Estructura de hardware

Continuando con la línea exploratoria expuesta anteriormente, la estructura del hardware dispuesto para sostener una plataforma virtualizada es un caso de estudio notable en la adquisición de nuevas tecnologías, desde que el objetivo principal en el uso de máquinas virtuales ha sido maximizar el uso de los recursos físicos de un sistema [1]. Sin embargo, son muchas las ventajas que el uso de máquinas virtuales en términos de seguridad, disponibilidad y aislamiento puede ofrecer [18] y que no solo se restringen al cumplimiento del objetivo planteado anteriormente.

Mientras que uno de los propósitos de las aplicaciones de virtualización es de dividir y usar adecuadamente el hardware para ejecutar múltiples aplicaciones e incrementar el uso de los recursos de cómputo, el mismo está limitado por las capacidades del sistema ó de los sistemas en donde se ejecutarán dichas aplicaciones. A primera vista es fácil determinar que, mientras más control sobre los componentes físicos tenga una aplicación de virtualización, tales como procesadores, memoria, red y almacenamiento, más fácil es determinar la importancia de tener el balance adecuado de dichos recursos [1].

Actualmente, existe mucha demanda sobre sistemas diseñados para virtualización con altos niveles de procesamiento, más núcleos por procesador, incremento en la capacidad de memoria, baja latencia, accesibilidad a recursos de almacenamiento en la red, entre otros. Es por ello que la elección de una plataforma de hardware para la virtualización de servidores es tan importante como elegir el software para virtualizar [37].

Para tomar la decisión adecuada, más de una consideración debe ser tomada en cuenta. A continuación se exponen las más relevantes.

2.4.1. Rendimiento

El incremento en las cargas de trabajo requiere de mejores rendimientos en el sistema que permitan mantener los niveles de servicio y tiempos de respuesta adecuados. Un mejor rendimiento puede obtenerse al adquirir nuevas tecnologías de procesamiento con múltiples núcleos por procesador en conjunto con un sistema que pueda aprovecharlas [4]. También se requiere que la arquitectura facilite la ejecución del programa de control de virtualizaciones, minimizando la sobrecarga, sobre todo en términos de entrada y salida.

2.4.2. Energía, espacio y costo

La energía y ventilación son factores importantes ya que se requiere costear contratos de mantenimiento para garantizar el funcionamiento de los sistemas. Es necesario considerar el límite del presupuesto ó los requerimientos de energía. El espacio físico puede ser un inconveniente importante a la hora de expandir la infraestructura tecnológica, sin embargo un sistema diseñado para la virtualización ayuda a reducir espacio y consumo de energía.

Desde que los servidores x86 fueron adoptados en masas, los costos de mantenimiento han crecido significativamente. El incremento en costos operativos ha provocado la desviación de los recursos y capital a iniciativas destinadas a impulsar la innovación en tecnologías de información [10]. La adquisición de entornos virtuales tiene el potencial de aumentar el uso de los sistemas con un bajo consumo de energía y ventilación, así como una reducción de los requerimientos de gestión y simplificación de operaciones.

2.4.3. Optimización y compatibilidad

Los vendedores de sistemas y componentes físicos incluyen funciones destinadas a la optimización. Por ejemplo, tanto Intel como AMD incorporan módulos de virtualización en sus procesadores [12]. Estás capacidades facilitan el diseño de aplicaciones de virtualización más robustas y reduce la sobrecarga con respecto al rendimiento ofrecido. También ofrecen funciones adicionales, como la calidad de servicio para garantizar prioridad entre máquinas virtuales.

Mientras que mantener la compatibilidad a través de diferentes generaciones en plataformas es un atributo clave en la disposición de futuros sistemas. Mover máquinas virtuales de un servidor a otro requiere de consideraciones en la arquitectura, para poder maximizar la flexibilidad dentro de la infraestructura [45]. Las nuevas plataformas permiten la migración de máquinas virtuales en ejecución, considerando un amplio soporte sobre el hardware.

2.5. Plataformas en el mercado

Luego de considerar las diferentes características que conforman la estructuración de una plataforma de hardware que aloje los sistemas virtualizados, se procede a la evaluación de las diferentes opciones en el mercado. Es de esperarse que en el proceso, se presenten muchas alternativas que una organización pueda tomar en cuenta. A continuación se presentan una breve reseña de tres soluciones diferentes, ofrecidas por las más importantes industrias del mercado actual.

2.5.1. Dell PowerEdge

La corporación en tecnologías Dell ofrece los servidores PowerEdge [13] como soluciones para virtualizar. Se trata de un servidor en rack de dos unidades que cuenta con procesadores Intel Xeon y una gran variedad de funciones orientadas al mejoramiento en la gestión de ambientes virtualizados.

Tiene 18 ranuras DIMM con posibilidad de expansión, además de 4 conexiones de red, con un procesador adaptable al software en tiempo real, lo que hace posible la ejecución de más tareas en simultáneo. Cuenta con una tecnología diseñada para aumentar el rendimiento en las horas pico de uso, conocida como Turbo Boost y adicionalmente, permite la reducción de costos operativos y de consumo de energía a través de una configuración proactiva de acuerdo a la demanda de uso [15].

Con una arquitectura basada en Intel Xeon, programas de control integrados, amplia capacidad de memoria y componentes de entrada y salida integrados, los servidores PowerEdge ofrecen un rendimiento general del sistema adecuado para cumplir con las capacidades requeridas por máquinas virtuales [14]. Posee funciones de virtualización integradas que son opcionales, orientadas a la optimización y simplificación de infraestructuras virtuales. Soporta virtualizaciones de VMware, Citrix, Microsoft y demás.

Adicionalmente, cuenta con herramientas de administración y gestión simplificadas que permiten ejecutar operaciones y comandos basados en estándares para facilitar la integración con los sistemas existentes, permitiendo un control eficaz. Una de sus principales herramientas es una consola de administración [15], la cual permite reducir el número de herramientas de gestión en una única consola con una fuente de datos común, permitiendo la administración de los recursos de hardware y seguridad de activos.

Finalmente, los servidores PowerEdge cuentan con una herramienta de configuración: Unified Server Configurator (USC) [16], una aplicación segura, eficiente y fácil de usar, que se encuentra integrada en el sistema diseñada para aumentar la flexibilidad y capacidades de los sistemas. Útil

en la implementación de sistemas operativos que requieren de controladores integrados, actualizaciones de firmware, configuraciones especificas de hardware y diagnostico de problemas

2.5.2. HP ProLiant

La industria HP ha tenido una gran experiencia en el desarrollo de plataformas de clase empresarial, pensadas en la gestión de capacidades. Un ejemplo de ello es la suite de servidores ProLiant [17], los cuales cuentan con dos procesadores Intel Xeon de alto rendimiento y densidad, el cual ha tenido una notable aceptación en comparaciones con sus competidores.

Puede tener hasta 64 GB de memoria, además de 4 ranuras para tarjetas PCI-Express para entrada y salida de alto rendimiento. Adicionalmente, cuenta con dos tarjetas de red Gigabit Ethernet multifuncionales y 8 bahías para dispositivos SAS ó SATA [18]. Esta plataforma soporta virtualizaciones de VMware y XenServer con herramientas diseñadas para la protección de datos. Una de sus funcionalidades más importantes es que cuenta con tecnologías avanzadas para protección de memoria, lo que protege al sistema de errores de la misma.

Cuenta con diversas herramientas de gestión de la infraestructura que aceleran la implementación del servidor, gestionando de forma activa su estado y optimizando la gestión de energía y permitiendo el control general de los sistemas, incluso desde un navegador web tradicional.

2.5.3. IBM BladeCenter

Una de las opciones recomendadas para el soporte de una infraestructura virtual es el sistema BladeCenter, provisto por la familia de sistemas IBM. El BladeCenter es un sistema de integración capaz de alojar múltiples aplicaciones a través de una serie de servidores, conocidos como servidores blades [26]. Es versátil y eficiente con respecto a otras tecnologías de servidores.

Un BladeCenter consiste en una estructura física conocida como chasis que aloja los distintos servidores blade y demás componentes físicos que facilitan la gestión y consolidación de los sistemas a virtualizar. Particularmente, el modelo BladeCenter S soporta una cantidad máxima de seis servidores blade que pueden compartir recursos en común, tal y como fuente de energía y refrigeración, administración de dispositivos y recursos de entrada y salida en un único chasis [19].

Adicionalmente, soporta hasta doce unidades de discos duro SAS (unidades de disco de tasas de transferencias altas que permiten conexiones y desconexiones de forma rápida) ò SATA (unidades de disco estándar de la industria, caracterizada por su velocidad de transferencia y prestaciones) y puede implementarse en poco tiempo ya que está diseñado específicamente para oficinas y entornos empresariales distribuidos. Dichos discos pueden ser fácil y rápidamente asignados directamente a los blades usando configuraciones predeterminadas o a través de configuraciones particulares del usuario [26]

- **Chasis**

El término chasis también se refiere a las conexiones internas contenidas en un BladeCenter, como por ejemplo: fuentes de energía y ventiladores. Todos los componentes del chasis conforman la columna vertebral de esta plataforma, permitiendo la compartición de servidores, conmutadores y energía.

En la figura 2.3, tomada de [19] se muestra una vista frontal del sistema IBM BladeCenter

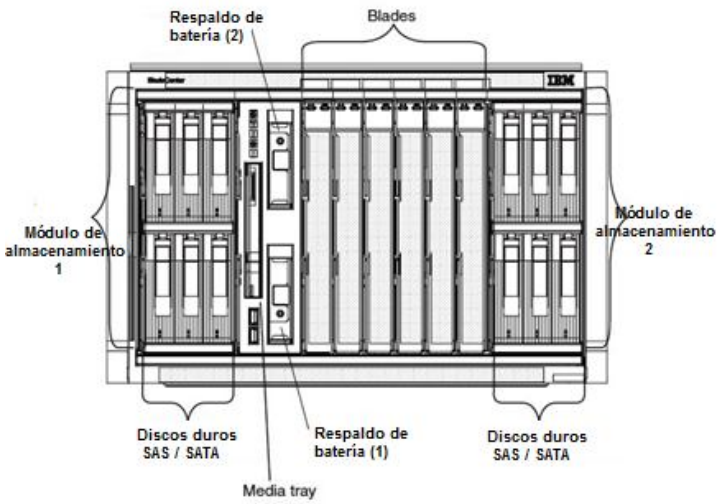

Figura 2.3: Vista frontal del sistema IBM BladeCenter

Mientras que la figura 2.4, tomada de [19] muestra la vista trasera del sistema IBM BladeCenter

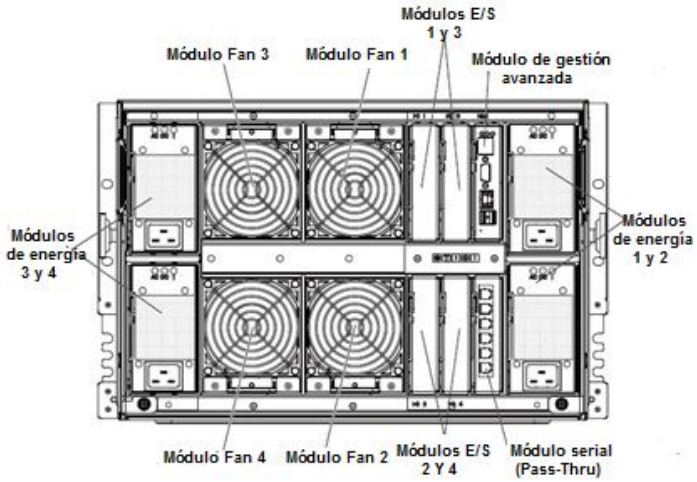

Figura 2.4: Vista trasera del sistema IBM BladeCenter

Adicionalmente, el BladeCenter incorpora doce ranuras para modulo de memoria, dos bahías para dispositivos de almacenamiento de tipo hot-swap (capacidad para realizar instalación ó sustitución, sin alterar el funcionamiento del sistema), un conector para tarjetas de expansión de canal de fibra, un conector Ethernet y un conector USB interno [19].

- **Blades**

Todo servidor que esté diseñando dentro de los estándares del BladeCenter, es considerado un servidor blade (o simplemente, blade). Un servidor blade está conformado por una tarjeta madre, procesadores, memoria, puertos de expansión y dos conexiones redundantes de tipo midplane. No contienen una fuente de energía, fuente de enfriamiento o conexiones E/S directas [25]. Para ello, cuentan con el chasis, quien es el encargado de suministrar la energía, enfriamiento y conectividad.

Un servidor blade simplemente se desliza dentro de una bahía del chasis y es conectado al tablero de circuitería, fuente de energía, ventiladores, conmutadores y puertos con otros servidores blade.

En la figura 2.5, tomada de [19] se muestra la disposición física de los componentes de un servidor blade.

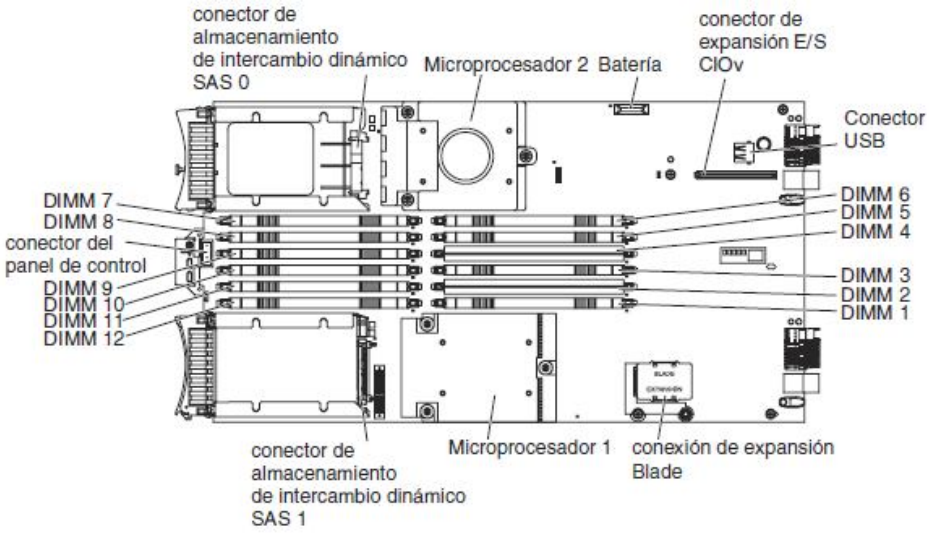

Figura 2.5: Componentes físicos de un servidor blade

- **Midplane**

Un midplane es un tablero de circuitos físicos, responsable de suministrar toda la energía y conectividad al chasis, y por tanto, a los servidores blade. Este tablero es configurado para que exista una serie de puntos de conexiones principales, además de un conjunto idéntico pero de menor cantidad de puntos, los cuales proporcionan energía y redundancia. Del lado posterior, existen una serie de puntos de conexión que permiten suministrar energía, ventilación y conectividad con las bahías de módulo de expansión [26].

- **Bahía**

Una bahía es un dispositivo dispuesto en el chasis que cumple con una función específica en la plataforma. Existen una serie de bahías: de módulo de expansión, de suministro de energía, de módulo de gestión y de conexiones seriales [26]. Estas bahías están directamente conectadas con el midplane.

- **Módulo de gestión avanzada**

El módulo de gestión avanzada [20] es usado por el BladeCenter para comunicarse con el procesador de servicios en cada servidor blade, permitiendo el monitoreo de sistemas, registro de eventos y alertas, lo que hace posible la administración del chasis, así como sus dispositivos y los servidores blade de manera remota. Despliega un firmware y una interfaz web de usuario para llevar a cabo todo tipo de tareas basadas en la gestión de hardware de los servidores blades y módulos de expansión. Además de la configuración de los módulos de almacenamiento [19].

- **Módulo de conexiones seriales**

El módulo de conexiones seriales provee de acceso directo a cada ranura blade del chasis. Este modulo tiene seis puertos seriales RJ45 externos (interfaces físicas usadas para conectar redes de cableado estructurado), cada uno físicamente asignado en cada una de las ranuras donde los servidores blade son dispuestos [19].

- **Configuración**

Particularmente, por cada uno servidor blade de un BladeCenter se suministran una serie de programas de configuración, usados para cambiar valores del sistema tales como las peticiones de interrupción (IRQ), la fecha, hora y contraseña, así como un programa almacenado en el firmware del servidor que se utiliza para establecer el orden de exploración de dispositivos y para establecer los identificadores de controlador de unidad de almacenamiento [26]. Por otra parte, también se suministran herramientas para la localización de dispositivos.

Son muchas las características de un servidor blade que pueden ser consultadas y modificadas a través de un programa de utilidad de configuración. Entre ellas se encuentran:

- Información del sistema, tal y como el identificador del servidor, número de serie, la velocidad, el tamaño de la memoria instalada y el tamaño de la memoria caché de los microprocesadores.

- Datos del producto, tal y como el identificador de la placa del sistema, el nivel de revisión y la fecha de emisión del firmware. Incluye el Módulo de Gestión Integrado (IMM) y los códigos de diagnostico, versión y fecha.

- Valores del sistema y sus componentes como procesadores, memoria, dispositivos y puertos E/S. Incluye alimentación y Módulo de Gestión Integrado (IMM). La configuración de red también es accesible, en donde se pueden visualizar el puerto de la interfaz de red de gestión del sistema, la dirección MAC del IMM, la dirección IP actual del IMM y el nombre del host. Incluye definición de direcciones IP estáticas, mascara de subred y dirección de Gateway.

- Seguridad del sistema, adaptadores y controladores UEFI, red, módulo TPM (*Trusted Platform Module*), fecha y hora, gestión y opciones de arranque, registro cronológico de sucesos de sistemas (*System Events Logs*) y seguridad de usuario.

- **Módulos de almacenamiento**

Particularmente, el módulo de almacenamiento de un IBM BladeCenter es fundamental en una colección de discos, ya que hace que estos sean accedidos por los servidores blade a través del módulo de conmutación SAS del chasis y la tarjeta de expansión SAS de cada blade [27]. Se pueden instalar un máximo de dos módulos de almacenamiento donde cada módulo puede contener hasta seis discos hot-swap. La convivencia de discos de tipo SAS y de tipo SATA en un mismo módulo está permitida.

En las figura 2.6, tomada de [19] se muestran los módulos y componentes que conforman toda la estructura física del sistema IBM BladeCenter.

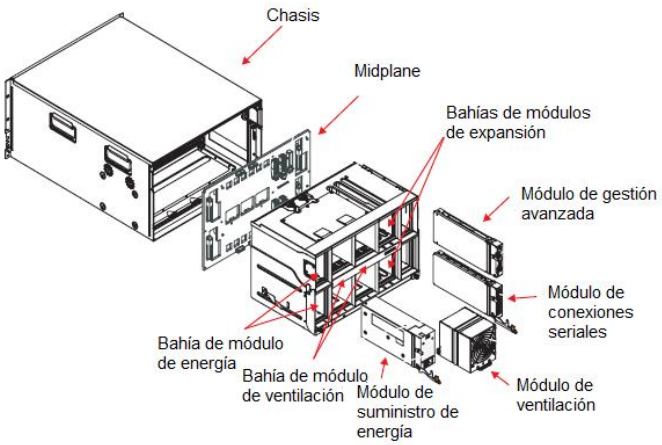

Figura 2.6: Componentes del IBM BladeCenter

Así como en la figura 2.7, tomada de [19] se muestran la disposición de un módulo de almacenamiento en el chasis de un sistema IBM BladeCenter.

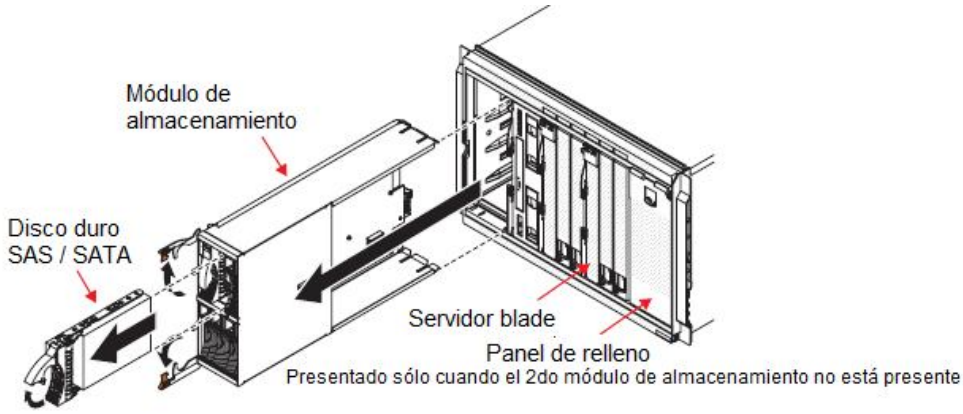

Figura 2.7: Módulo de almacenamiento

Un módulo SAS es el responsable de proveer discos físicos a través de la locación de recursos. El módulo de almacenamiento funciona con una tarjeta de expansión SAS, la cual actúa también como un controlador RAID de servidores blade [19] (un controlador RAID es un sistema de almacenamiento que usan múltiples discos duros entre los que se distribuyen ó replican los datos).

Por su parte, el sistema BladeCenter S soporta varios tipos de discos duro, los cuales son:

- Discos SAS, discos de tipo *Serial Attached SCSI* diseñados y usados para requerimientos de alto rendimiento donde es el máximo *throughput* y prestaciones en transacciones son requeridas.

- Discos SATA, discos de tipo *Serial Advanced Technology Attachment* diseñados para proporcionar más capacidad de almacenamiento a menor costo, en comparación con discos SAS, donde el rendimiento no es un requerimiento prioritario.

El módulo de conectividad SAS es el encargado de proveer conectividad y acceso entre los blades y los discos en los módulos de almacenamiento [26]. También ofrece cuatro puertos SAS externos para conexiones adicionales. El acceso a los datos es controlado mediante una configuración definida por el usuario, la cual puede ser:

- Conexiones internas en el chasis desde los blades hasta los discos.
- Conexiones internas en el chasis desde los blades hasta los puertos externos del módulo de conectividad SAS.

Para ello, cada blade debe tener una tarjeta de expansión SAS ó una tarjeta de conectividad SAS instalada para poder establecer conexión con el almacenamiento a través del módulo de conectividad SAS. El módulo de conectividad SAS sólo provee conectividad entre los dispositivos SAS instalados en el BladeCenter.

En la figura 2.8, tomada de [19] se muestra la vista frontal de un módulo de conectividad SAS del IBM BladeCenter.

Figura 2.8: Módulo de conectividad SAS

- **Herramientas de administración**

Conocer las herramientas de gestión de una plataforma permite llevar a cabo tares necesarias para su administración y mantenimiento. Se requiere definir las funcionalidades de cada uno y como pueden ser usadas para ejecutar tareas especificas. Es posible administrar el módulo de conectividad SAS usando una serie de herramientas de gestión:

- Interfaz de usuario del módulo de gestión avanzada
- Interfaz de usuario del módulo de conectividad SAS
- Storage Configuration Manager
- Telnet y la interfaz de línea de comando (CLI)

Dependiendo de la tarea que se quiera llevar a cabo, es posible elegir entre:

- La interfaz CLI provee de muchas más funcionalidades, aunque no debe ser requerida para uso diario.
- Storage Configuration Manager es la aplicación más versátil y simple de las herramientas web listadas.

Por su parte, el IBM Storage Configuration Manager es una aplicación de gestión de sistemas que permite utilizar un navegador web para configurar y administrar los dispositivos de una unidad IBM BladeCenter.

Esta aplicación se ejecuta en un servidor web que se comunica con los dispositivos administrados, entre los que se incluye: módulos de conectividad SAS, módulo de almacenamiento en discos y el módulo de controladores RAID [27]. Cabe destacar que las aplicaciones IBM Storage

Configuration Manager e IBM Director no pueden ser instaladas en un mismo servidor, aunque pueden convivir en la misma red.

En la tabla 2.1, tomada de [27] se describen los requerimientos de la aplicación.

Aplicación	IBM Storage Configuration Manager
Velocidad de CPU	Pentium de 1.5 GHz
Memoria RAM	1 GB
Espacio en disco	120 MB
Pantalla	Colores 256 (Navegador web)
Sistema Operativo	Microsoft Windows XP Microsoft Windows Server 2003 / 2008 R2 Red Hat Enterprise Linux SUSE Linux
Navegador web	Microsoft Internet Explorer Mozilla Firefox

Tabla 2.1: Requerimientos de IBM Storage Configuration Manager

En cuanto a los aspectos de red, los procesos del IBM Storage Configuration Manager requieren de acceso a una serie de puertos TCP del ambiente en donde es instalado. Si estos puertos son bloqueados por un Firewall ó son usados por otros procesos, la aplicación no podrá funcionar.

- **Módulo controlador SAS RAID**

Un módulo controlador SAS RAID consiste en un conmutador integrado SAS, combinado con un controlador RAID que provee de una solución de almacenamiento RAID embebida con funciones avanzadas orientadas a la gestión SAN. Debe ser usado cuando se requiera un máximo de rendimiento, confiabilidad y flexibilidad con respecto a la localización de almacenamiento.

Los requerimientos de un módulo controlador SAS RAID de un sistema IBM BladeCenter son los siguientes [27]:

- Dos módulos controladores SAS RAID
- Dos unidades de batería para respaldo
- Al menos dos unidades de disco duro para configuración RAID 0 y 1, ó tres unidades de disco duro para RAID 5
- Un módulo de gestión avanzada
- Dos fuentes de energía para el módulo DSM
- Un conmutador Ethernet (Nortel 1/10 GB Uplink Ethernet Switch Module)

En la tabla 2.2, tomada de [27] se indican las interfaces usadas para la gestión y configuración, luego de una instalación.

Interfaz	Gestión y configuración
Interfaz web del Módulo de Gestión Avanzada	- Direcciones IP del módulo controlador SAS RAID - Direcciones IP del conmutador SAS - Monitoreo de estado del IBM BladeCenter
IBM Storage Configuration Manager	- Crear una configuración de almacenamiento - Permitir a los hosts acceder al almacenamiento - Asignar almacenamiento a los hosts - Monitorear el estado del controlador - Actualizar el código del controlador - Actualizar el firmware del conmutador SAS
Interfaz de línea de comando del controlador RAID	- Crear una configuración de almacenamiento - Permitir a los hosts acceder al almacenamiento - Asignar almacenamiento a los hosts - Monitorear el estado del controlador - Actualizar el código del controlador usando el paquete de actualización de firmware
Interfaz de línea de comando del conmutador SAS	- Monitorear el estado del conmutador SAS - Actualizar el firmware del conmutador SAS
Interfaz web del conmutador SAS	- Monitorear los componentes del conmutador SAS

Tabla 2.2: Interfaces usadas en la gestión del módulo controlador SAS RAID

Todas estas herramientas y utilitarios están orientadas a la gestión del módulo controlador SAS RAID y pueden ser usadas de diversas formas. Por ejemplo, si se usa el IBM SCM (Storage Configuration Manager) para configurar el almacenamiento, redundancia de datos y mantenimiento del firmware, se estaría llevando a cabo una gestión más automatizada en lugar de hacerlo a través de la interfaz de línea de comando ó el paquete de actualización de firmware.

Sin embargo, a pesar de la forma en que se elija llevar a cabo las configuraciones de sistemas de almacenamiento y mantenimiento, el módulo controlador SAS RAID permite configurar soluciones de almacenamiento integradas mediante:

- Creación de pools de almacenamiento
- Definición de volúmenes para esos pools
- Recibir números de unidad lógica (LUN, *Logical Unit Numbers*)
- Mapear esos números a hosts (servidores) contenidos en el IBM BladeCenter

- **Uso de pools y volúmenes de almacenamiento**

Una manera de particularizar la configuración de almacenamiento es la capacidad de dividir el almacenamiento disponible en unidades lógicas llamadas pools. Un pool de almacenamiento es una colección de discos convertidos en una unidad lógica. Cuando se crea un pool de almacenamiento, se asigna un nivel RAID para agregar un nivel de redundancia [28]. Además, se indica que pool se comunica con un servidor blade, como parte de la configuración de almacenamiento.

Cabe destacar que todos los discos que conformen un pool de almacenamiento deben ser del mismo tipo, donde cada disco debe pertenecer a un único pool de almacenamiento.

Luego de haber creado un pool de almacenamiento, se pueden crear volúmenes para la gestión de los datos. Los volúmenes son la unidad básica del almacenamiento expuesto en un servidor blade y son creados a partir del espacio disponible de un pool, por lo que un volumen está completamente contenido en un único pool de almacenamiento y así mismo, un pool de

almacenamiento puede contener múltiples volúmenes. Luego de crear los volúmenes, estos deben mapearse a cada servidor blade en particular.

Estos volúmenes pueden ser usados para almacenar datos de aplicaciones ó como volúmenes de arranque que almacenen imágenes de sistemas operativos. Por cada volumen, deben determinarse características como: tamaño, servidores que tendrán acceso y aplicaciones que requieran acceso.

- **Niveles RAID**

Tener arreglos de redundancia en discos independientes RAID (*Redundant Arrays of Independents Disks*) permite la una variedad de casos en la configuración del almacenamiento, permitiendo que la pérdida de un disco, por ejemplo, no interfiera con el disponibilidad de los datos [29]. Sin embargo, hay una serie de consideraciones a tomar cuenta para poder decidir qué nivel RAID usar en la configuración, tal y como la cantidad de almacenamiento que se tenga a disposición, el costo y los requerimientos de seguridad.

Los niveles RAID soportados son:

- Nivel 0: *Striping* de discos
- Nivel 1: Copia espejo (*mirroring*)
- Nivel 5: *Striping* con paridad distribuida
- Nivel 10: *Striping* a través de espejos

Es posible administrar el módulo controlador SAS RAID usando una serie de herramientas de gestión:

- Interfaz de usuario del módulo de gestión avanzada
- Interfaz de usuario del módulo de conectividad SAS
- Storage Configuration Manager
- Telnet y la interfaz de línea de comando (CLI)

- **Módulo de gestión avanzada**

El módulo gestión avanzada (MGA) es un componente que puede ser usado para configurar y gestionar cualquier elemento instalado en el BladeCenter. Provee funciones para la gestión de sistemas y un componente KVM compartido por todos los servidores blade. Se comunica con todos los elementos del BladeCenter, detectando su presencia ó ausencia, reportando sus estados y enviando alertas cuando las condiciones lo requieran.

Los componentes del BladeCenter se configuran usando la interfaz web de usuario del MGA. Esta interfaz se comunica con la aplicación de gestión y configuración, la cual forma parte del firmware instalado en el módulo. Se puede usar el MGA para llevar a cabo las siguientes tareas:

- Definir credenciales
- Configurar opciones de seguridad, tales como cifrado de los datos y seguridad en cuentas de usuario
- Seleccionar los recipientes para las notificaciones de alerta ante eventos específico
- Monitorear el estado de la unidad BladeCenter, servidores blade y demás componentes
- Descubrir otras unidades BladeCenter en la red, permitiéndoles el acceso a ellos a través de interfaces web
- Controlar la unidad BladeCenter, servidores blade y demás componentes
- Acceder a los módulos de E/S y configurarlos
- Cambiar la secuencia de arranque de los servidores blade

- Configurar la fecha y hora
- Usar la consola remota para los servidores blade
- Controlar el teclado, video y mouse
- Controlar los dispositivos y puertos USB

3. Metodología

En este capítulo se expone el modelo usado para planificar e implementar la tecnología de virtualización en una infraestructura organizacional, tomando como caso de estudio las soluciones para virtualizar de VMware bajo una plataforma de servidores blades, dispuestas por la tecnología IBM BladeCenter.

Cabe destacar que el modelo expuesto corresponde a una metodología de trabajo planteada ante la necesidad de consolidar un proyecto de virtualización de servidores en una organización, la cual define tres etapas, expuestas en la figura 3.1:

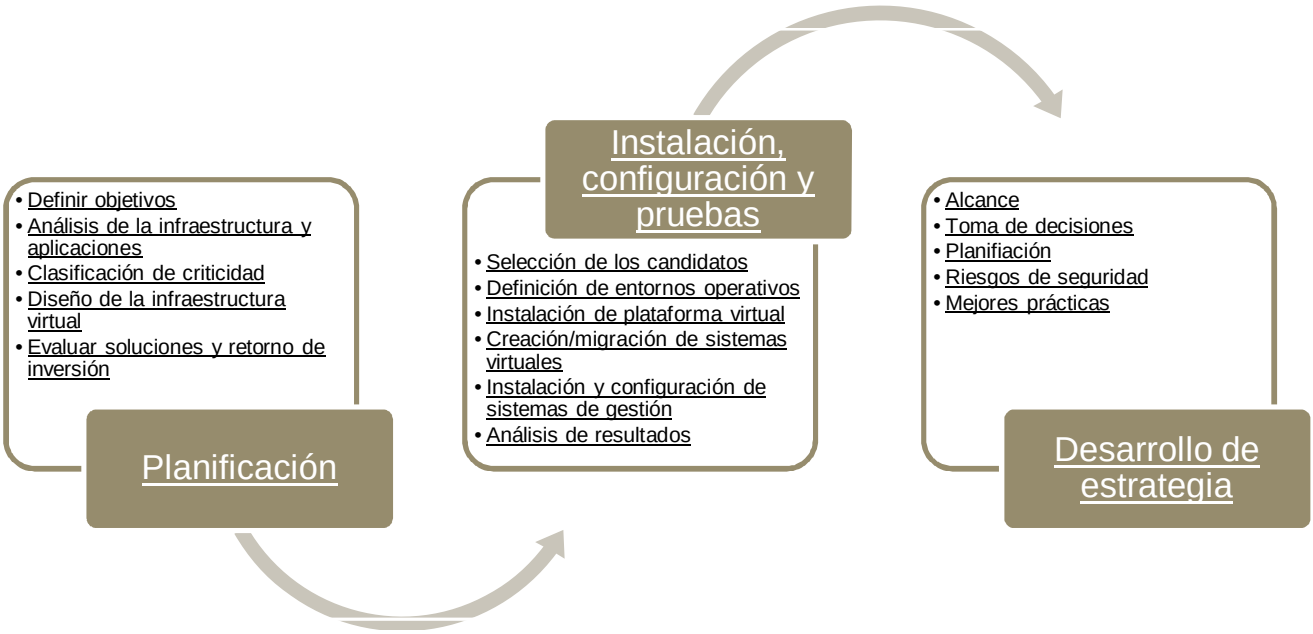

Figura 3.1: Etapas del proyecto de virtualización de servidores

La primera etapa corresponde a la planificación del proyecto en donde deben definirse los objetivos y realizar un análisis de la infraestructura física presente, contemplando tanto servidores como aplicaciones con el fin de categorizarlos de acuerdo a sus niveles de criticidad. Posteriormente, se procede a diseñar la infraestructura virtual, considerando todas las entidades que la componen y su disposición en la plataforma de comunicaciones. Una vez consolidados dichos planteamientos, es posible evaluar las diferentes soluciones dispuestas en el mercado a fin de adquirir la que más se acomode a los requerimientos de la organización.

La segunda etapa corresponde a la instalación, configuración y pruebas de los sistemas de virtualización, tanto físicos como de software. Esta etapa requiere de una selección de candidatos a virtualizar, soportada por la categorización realizada en la etapa anterior, de manera de poder instalar las tecnologías adquiridas y virtualizar dichos sistemas. Luego se procede a la disposición de todas las herramientas de gestión, ejecutando los planes de implementación propios del diseño de la infraestructura virtual. Una vez dispuestos tantos los sistemas virtuales como las herramientas de gestión, es posible realizar pruebas de rendimiento para evaluar el funcionamiento de los mismos.

Finalmente, la tercera etapa permite consolidar un plan metodológico diseñado desde la primera fase a través del diseño y aplicación de una estrategia de virtualización basada en las mejores prácticas. Esta estrategia pretende cumplir con los objetivos que se desean lograr con la virtualización, permitiendo alcanzarlos con la aplicación de ciertas consideraciones con respecto a cada uno de los componentes que conforman una infraestructura virtual. También incluye todos los

procedimientos y mecanismos de seguridad adecuados en la aplicación de la segunda fase del proyecto, permitiendo así la consolidación de una plataforma segura y eficiente que cumpla con los requisitos planteados.

Esta metodología de trabajo pretende desarrollar una estrategia de mejores prácticas para la virtualización empresarial a través de la ejecución de un proyecto de migración de un conjunto de servidores de propósito general de una organización, de una plataforma física a una plataforma virtual, de manera de consolidar una serie de lineamientos, tanto técnicos como de negocio, que oriente a organizaciones en este proceso.

A continuación se plantean cada una de las tareas asociadas a cada etapa de la metodología de trabajo expuesta.

3.1. Planificación del proyecto

La planificación de las tareas a ejecutar juega un papel importante en todo proyecto de tecnologías de información de una organización, ya que el éxito del mismo dependerá en gran parte de los modelos de gestión adoptados. Esta planificación debe ser lo bastante amplia para garantizar el mejor retorno de inversión posible.

Una de las tareas iniciales es la de comprender los conceptos ligados a la virtualización, de manera de determinar cuáles son los obstáculos que se presentan y la manera de sobrellevarlos ó de erradicarlos del mapa de ejecución por lo que una investigación exhaustiva de estos términos es necesaria para garantizar el éxito de la implementación del proyecto.

Dicha investigación debe asemejarse a la presentada en el capitulo anterior, la misma contempla los diferentes conceptos y terminologías, asociándolos a las diferentes soluciones dispuestas en el mercado. Para tomar la decisión adecuada, la organización debe plantearse una serie de objetivos que desee cumplir.

3.1.1. Definición de objetivos

La definición de un conjunto de objetivos es la segunda acción planificada con el fin de poder evaluar si las soluciones disponibles satisfacen plenamente los requerimientos de la organización y que proporcione el máximo retorno de inversión posible. La propuesta de estos objetivos debe definir y detallar de manera clara y concisa, los resultados esperados en la consolidación del proyecto y proporcionar respuestas a los siguientes planteamientos:

- Motivos por la cual la organización desea consolidar servidores en una plataforma de virtualización
- Cantidad de servidores físicos que podrían consolidarse
- Soluciones que podrían aprovecharse, determinando la solución preferida
- Impacto de la virtualización en los usuarios
- Implicaciones de seguridad de migrar a una infraestructura virtual
- Tiempo de desconexión necesario para ejecutar una migración
- Posibles riesgos y minimización de los mismos
- Costo estimado
- Retorno de inversión estimado

Naturalmente, el planteamiento inicial de los objetivos estará sujeto a modificación y serán refinados durante las últimas etapas del proceso de planificación, previo a la ejecución del plan. Cabe destacar que cada meta a cumplir debe estar sostenida por medidas específicas que se puedan reproducir, dejando claro la razón de dicha meta y los resultados esperados.

La definición de metas y objetivos impulsará el proyecto de virtualización de servidores en la dirección correcta, permitiendo consolidar una solución adecuada en términos de flexibilidad, seguridad, costos y demás, satisfaciendo las necesidades presentes y futuras de la infraestructura tecnológica de la organización.

3.1.2. Análisis de la infraestructura

El proceso de identificación de servidores de una infraestructura tecnológica a nivel es una tarea ardua, dependiendo del tamaño y orientación de la organización que la implemente. El objetivo principal de esta acción es la de categorizar los servidores de manera de determinar los candidatos a someterse a la virtualización.

Se requiere estudiar individualmente los riesgos y efectos de la consolidación de cada servidor en un entorno virtual. La consolidación no es una tarea unívoca, ya que puede existir la posibilidad de migrar un servidor virtual de nuevo a un entorno físico, en caso de modificaciones en los requerimientos de la máquina virtual, por ejemplo [21]. Una parte importante de la planificación es prepararse para el futuro y reconocer que los cambios de esta índole son posibles e incluso necesarios [52].

Dentro de los parámetros que se pueden recopilar en los servidores para determinar su candidatura a ser sometidos a una migración se encuentran:

- Estadísticas de uso
- Ubicación
- Cargas de trabajo
- Requisitos de alimentación y espacio
- Costo
- Análisis de situaciones

Antes de tomar la decisión de migrar una aplicación a un entorno virtual, la organización debe asegurarse de que el fabricante ó proveedor de la misma, ofrezca asistencia técnica. De lo contrario, la virtualización de la aplicación debe someterse a un análisis adicional para determinar si realmente es necesaria su incorporación en la plataforma virtual [22]. De hecho, el análisis de las aplicaciones debe considerar los siguientes aspectos:

- Implicaciones de una migración de físico a virtual, como de una migración de virtual a físico
- Cambios en la funcionalidad
- Uso
- Número de usuarios
- Estabilidad
- Tiempo restante de vida útil
- Tiempo restante de soporte técnico

Es importante cuestionar si realmente vale la pena ó no, dedicar recursos y tiempo en la migración de aplicaciones que se ajusten de manera adecuada a los criterios establecidos con anterioridad, a fin de determinar una mejor opción, como por ejemplo, descartar y sustituir la aplicación en cuestión [52].

3.1.3. Clasificación según niveles de criticidad

Los niveles de criticidad permiten cuantificar el grado de seguridad que poseen los servidores, tomando en consideración varios aspectos como lo son la exposición de información confidencial contenida o gestionada por una aplicación, la integridad de la misma y los casos en los que la información no estuviese disponible o no pudiese ser accedida [44].

Para determinar la clasificación del riesgo se puede hacer uso de un cuestionario que los responsables a nivel de tecnología de información de una organización deben contestar. Considerando la naturaleza y clasificación de la información procesada y/o almacenada en las aplicaciones, así como la disponibilidad de la misma.

La estructura del cuestionario de clasificación de riesgo debe basarse en los siguientes planteamientos:

- **Detalles de la aplicación:**
  - Nombre de la aplicación
  - Descripción de la aplicación y su información
  - Propietario de la aplicación
  - Unidad de negocio
  - Ubicación física
  - Custodio de información y tecnología
  - Contacto del personal de tecnología

- **Confidencialidad:**
  - Tipo de información procesada ó almacenada
  - Impacto de una fuga de información en la confidencialidad
  - Impacto de negocio
  - Impacto a la reputación de la organización

- **Integridad:**
  - Grado de impacto con respecto a la imprecisión de la información dentro de la aplicación
  - Impacto de negocio
  - Impacto a la reputación de la organización

- **Disponibilidad:**
  - Tiempo de indisponibilidad de la aplicación sin causar impacto en la organización
  - Impacto máximo potencial a la organización si el tiempo de indisponibilidad se excede
  - Impacto de negocio
  - Impacto a la reputación de la organización

De acuerdo a las respuestas proporcionadas frente a los planteamientos dispuestos anteriormente, se puede determinar una clasificación de riesgo o criticidad para una aplicación comprendida entre los niveles Bajo, Medio, Alto y Crítico.

Adicionalmente, se puede determinar una clasificación de la información cuyos niveles pueden estar comprendidos entre:

- **Información no clasificada:** Aquella información con propósito de uso interno o externo cuyos controles sean mínimos. Su descubrimiento o divulgación no impactaría a la organización.

- **Información de uso interno:** Aquella información de propósito de distribución interna que pudiese causar daño a la organización en caso de ser accedida por terceras partes.

- **Información de distribución restringida:** Aquella información sujeta a autorización para su acceso y de distribución controlada, ya sea para el personal externo o interno.

- **Información secreta:** Aquella información con el más alto grado de confidencialidad. De ser divulgada sin autorización, podría causar daños materiales significativos, poniendo n riesgo la viabilidad de las actividades de negocio de una organización**.**

3.1.4. Diseño de la infraestructura virtual

Una vez finalizado el proceso de inventario y análisis de la infraestructura física y de las aplicaciones, se procede al diseño de la infraestructura virtual, considerando sus componentes con más detalle.

Los criterios que deben tomarse en cuenta para componer una infraestructura virtual son los siguientes:

- Sistemas anfitriones
- Red
- Rendimiento
- Mecanismos de seguridad
- Procedimientos de recuperación de información
- Almacenamiento
- Procedimientos de respaldos

3.1.5. Evaluación de soluciones y retorno de inversión

Al momento de evaluar las posibles soluciones para su adquisición, la organización debe realizar una amplia investigación, basando su decisión en factores que incluyan, no solo costos, sino también la capacidad de gestión, migración y demás criterios de carácter tecnológico. Asimismo, una parte importante en la toma de decisiones es el historial establecido por el proveedor en materia de virtualización de servidores, un factor a ser considerado tomando en cuenta que la implementación de esta técnica representa un cambio a gran escala.

No obstante, a pesar de que la organización adquiera la solución más adecuada a sus necesidades y capacidades, tomando en consideración los costos, la migración a una infraestructura virtualizada es un proceso relativamente caro. Por lo que una manera de determinar si el proyecto de virtualización ofrece soluciones realistas a nivel económico, es calculando el retorno de inversión [23].

Para el cálculo de la recuperación de la inversión, la organización debe determinar los costos de mantener la infraestructura existente y restarlo en los costos estimados en el mantenimiento de la infraestructura virtual.

Por su parte, determinar los costos de mantenimiento en la infraestructura existente es sencillo, caso contrario al momento de estimar los mismos costos en una infraestructura virtual [24]. Para ello se procede a estimar los posibles ahorros de costo que se producirían en los siguientes planteamientos:

- Reducción en precios de compra de nuevos servidores
- Reducción en el consumo de energía y refrigeración
- Disminución en costos de gestión y mantenimiento
- Reducción en tiempos de desconexión (planificados y no planificados)
- Disminución en números de licencias de sistemas operativos
- Desincorporación de equipos obsoletos
- Reducción en espacio

Una vez evaluados cada uno de los parámetros establecidos anteriormente, se puede proceder a la adquisición de tecnologías para llevar a cabo el proyecto de virtualización de servidores.

3.2. Instalación, configuración y pruebas

La finalidad de esta etapa es la sostener la adquisición de las tecnologías de virtualización en base a tareas de investigación y documentación de la infraestructura física, de manera de poder llevar a cabo los respectivos procedimientos de instalación y configuración de las mismas, en función de las funcionalidades destacadas que pueden satisfacer con las necesidades de negocio.

El posterior análisis de los resultados obtenidos permitirá verificar la correcta adopción de las tecnologías y ofrecerá información que será usada para el fortalecimiento de la nueva plataforma virtual.

3.2.1. Selección de los candidatos a virtualizar

En base a lo expuesto en la etapa de planificación, los servidores y aplicaciones de la infraestructura física son categorizados en función de su nivel de criticidad, de manera de poder seleccionar candidatos para ser virtualizados. El objetivo de esta tarea es, no sólo consolidar los objetivos que se desean cumplir con respecto a dichos sistemas, sino también incorporar aquellas nuevas implementaciones que se desean incluir de manera directa en la plataforma virtual.

El selección dichos sistemas se basa en la clasificación del riesgo asignada y en los requerimientos de hardware y software que pueden ser soportados en una plataforma virtual, sin afectar su funcionamiento y permitiendo el cumplimientos de sus demandas.

3.2.2. Definición de entornos operativos

La definición de diferentes entornos operativos dependerá de la plataforma física y los recursos de hardware adquiridos para soportar los ambientes virtuales. Una de las ventajas de la virtualización es la de consolidar un centro de datos que albergue sistemas en diferentes fases operativas. Por ejemplo, pueden contarse con servidores en producción, servicios en etapa de desarrollo y aplicaciones en fase de pruebas.

Con la disposición de entornos operativos de producción, de desarrollo y de pruebas en un mismo centro de datos virtual, la asignación y aprovechamiento de recursos puede ser más eficiente, de manera de poder contar con una separación subyacente que permita contribuir en la seguridad de los ambientes albergados. La portabilidad de las máquinas virtuales, así como las funcionalidades de los programas de control, permiten la migración de servidores de un entorno a otro al cumplir con las etapas de su ciclo operativo, garantizando el dinamismo requerido en el mantenimiento de varios entornos.

El objetivo de esta tarea es identificar los recursos físicos disponibles a fin de definir diferentes entornos operativos, enumerando cada uno de los servidores candidatos a virtualizar y planificando su disposición en los mismos de acuerdo a sus requerimientos, objetivos y demandas a cubrir.

3.2.3. Instalación de la plataforma virtual

Una vez que la plataforma física destinada a alojar los sistemas virtuales se consolide en el centro de datos, luego de una serie de procedimientos de instalación, disposición y configuración se ejecuten, contando con el soporte del proveedor elegido, se procede a instalar los respectivos programas de control ó gestores de máquinas virtuales.

Esta tarea comprende el estudio y aplicación de cada uno de los procedimientos de instalación de las tecnologías de software adquiridas, así como el establecimiento de las respectivas comunicaciones entre dichas tecnologías y los sistemas físicos dedicados a alojar máquinas virtuales.

Dependiendo del nivel de experticia que se tenga al momento de llevar a cabo esta tarea, el proceso de instalación puede basarse en ensayo y error, tomándose un tiempo considerable en su implementación. Muchas de las instalaciones deben adaptarse a los recursos que se tengan y los requerimientos que se deseen satisfacer, por lo que se sugiere documentar todas las modificaciones realizadas en el proceso de adopción, de manera de poder consolidar una base de conocimiento que puede usarse en implementaciones futuras y que faciliten el proceso de gestión y mantenimiento de los sistemas.

3.2.4. Configuración de los sistemas de gestión

La instalación de las tecnologías para virtualizar es una tarea de suma importancia. Sin embargo, la tarea de configurar cada una de ellas es la base para la consolidación de una plataforma segura y estable. De acuerdo a toda tecnología de virtualización, la presencia de un sistema orquestador de servicios es obligatoria, desde que los programas de control deben ser gestionados por los administradores de sistemas.

El proceso de configuración, del mismo modo que el proceso de instalación, consiste en la ejecución de tareas que, en un principio, pueden tomarse un tiempo considerable con respecto a la experticia disponible. Básicamente, se busca consolidar un conjunto de aplicaciones que puedan satisfacer, en principio, con requerimientos de:

- Creación de máquinas virtuales
- Configuración y actualización de programas de control
- Aprovisionamiento y mantenimiento de máquinas virtuales
- Agrupación de entornos operativos
- Configuración del almacenamiento compartido
- Recopilación de información de componentes físicos
- Definición de mecanismos de seguridad, resguardo y recuperación
- Reportes y monitoreo

Estas herramientas pueden ser provistas por las tecnologías de software, de hardware ó una combinación de ambas. En caso de que se traten de clientes de gestión, los mismos deben instalarse en las estaciones de trabajo de los administradores delegados para la gestión del proyecto de virtualización, considerando políticas de seguridad asociadas a la autenticación y acceso a la información de los mismos.

3.2.5. Análisis de los resultados obtenidos

Luego que los servidores y aplicaciones virtuales se consolidan en la plataforma diseñada, se procede a analizar los resultados en términos de uso y aprovechamiento de recursos con el fin de determinar la mejor asignación posible de los mismos en función de las demandas que los sistemas requieran satisfacer.

Del mismo modo, se puede evaluar el uso de los recursos desde el punto de vista de los sistemas anfitriones y en función de los entornos operativos dispuestos, así como el almacenamiento compartido y repartido entre los mismos. El objetivo es consolidar una de las ventajas más importantes de la virtualización: garantizar la eficiencia en términos de procesamiento y aprovechamiento de los recursos.

Desde el punto de vista empresarial, el análisis de resultados puede basarse en la medición del crecimiento alcanzado en términos de cantidad de nuevos servicios y aplicaciones consolidadas. La actualización de sistemas, innovación y crecimiento son factores que contribuyen en el retorno de inversión esperado desde el inicio del proyecto y la adquisición de nuevas tecnologías.

3.3. Estrategia de mejores prácticas

Al culminar las etapas de planificación e instalación, el estado del proyecto de virtualización de servidores será avanzado pero no culminado, desde que la aplicación de una serie de consideraciones basadas en las mejores prácticas para virtualizar es un requerimiento, sobre todo tratándose de un proyecto de tecnologías de información organizacional.

Es importante considerar que el concepto asociado a “mejores prácticas” no está restringido sólo a aquellas consideraciones que deben seguirse a la hora de instalar y configurarse una determinada tecnología, sino que también abarca la recopilación de procesos inherentes a la planificación estratégica de un proyecto de tecnologías de una organización.

Es así como el objetivo de esta etapa es consolidar una estrategia destinada a las organizaciones para orientar en el proceso de planificación de un proyecto de virtualización de servidores y que recopile un conjunto de mejores prácticas de instalación, configuración, gestión, seguridad y mantenimiento de ambientes virtuales dedicados a satisfacer demandas empresariales.

Principalmente, esta estrategia debe comprender diferentes etapas que consoliden una serie de planteamientos que permitan orientar un proyecto de virtualización en la dirección correcta. Básicamente, el criterio para agrupar dichos lineamientos debe basarse en:

- **Definición de alcance:** La estrategia debe ofrecer diversos criterios para que una organización pueda plantear sus objetivos a cumplir en función de determinar si la virtualización es la solución a sus requerimientos y necesidades iniciales.

- **Toma de decisiones:** La estrategia debe recopilar información, tanto técnica como de negocio, que permita fundamentar la elección de una determinada tecnología de virtualización del mercado en función del retorno de inversión esperado y la consolidación de una plataforma segura, estable y preparada para el futuro.

- **Planificación:** La estrategia debe plantear una serie de etapas a cumplir que consoliden una planificación sólida en función de cumplimiento de objetivos bajo tiempos de ejecución definidos, uso de recursos y aplicación de políticas de seguridad de información, propios de una organización.

- **Consideración de riesgos:** Siguiendo con los lineamientos en función de políticas de seguridad organizacionales, la estrategia debe prestar especial atención en la identificación y categorización de los riesgos presentes en la migración a una nueva plataforma. De esta manera, aspectos como la autenticación, clasificación y estado de la información, seguridad de las comunicaciones y reconocimiento de vulnerabilidades pueden ser atendidos de manera individual.

- **Mejores prácticas:** Finalmente, la estrategia debe incluir una serie de procedimientos y lineamientos que deben considerarse en las tareas de instalación, configuración, gestión y resguardo de los sistemas virtuales. Estas consideraciones de mejores prácticas deben centrarse tanto en el hardware como el software adquirido, además de enfocarse en las máquinas virtuales y demás componentes de la infraestructura virtual.

El diseño e implementación de esta estrategia estará fundamentado en el conocimiento adquirido en el desarrollo y consolidación de un proyecto de virtualización de servidores realizado en una organización, el cual se expone en el siguiente capítulo.

4. Implementación

En este capítulo se plantean el conjunto de procedimientos que se llevaron a cabo en la consolidación del proyecto de virtualización de servidores de una organización. Dichos procedimientos describen los pasos seguidos de acuerdo a la planificación dispuesta en el capitulo anterior, particularizando los casos de estudio aplicados.

A continuación se exponen los pasos a seguir, de acuerdo a los requerimientos de la organización y mecanismos llevados a cabo.

4.1. Alcance

Este trabajo se proyecta como una implementación multidisciplinaria de carácter teórico y practica que viene dada por la intención de incorporar nuevos conceptos de tecnologías de información en una plataforma tecnológica ya existente en una organización en particular.

El carácter teórico se debe a la necesidad de documentar un conjunto de procedimientos orientados al sector empresarial que sirvan como base para la consolidación de una estrategia para un proyecto de virtualización de servidores en función de las mejores prácticas. Por su parte, el desarrollo práctico se basa en la instalación, configuración y pruebas de una tecnología de virtualización del mercado que sostenga los procedimientos descritos anteriormente, sin particular los lineamientos de la estrategia a desarrollar.

Las actividades realizadas siguieron una planificación establecida, expuesta en el capitulo anterior, la cual sugiere la ejecución de una serie de fases para la consolidación del proyecto. Parte de la información recopilada es propiedad de la organización que fue sometida a dicha planificación, la cual accedió a la disposición de la misma en el presente documento con las modificaciones necesarias para su publicación.

La consolidación de la estrategia de mejores prácticas para la virtualización empresarial planteada en este documento se basa en la ejecución de varias instalaciones y configuraciones de herramientas de gestión del mercado tecnológico en la plataforma tecnológica de la organización. Los resultados de las mismas se presentan para evaluar su alcance y validar sus planteamientos y estatutos.

Finalmente, el proyecto de virtualización de servidores requiere del establecimiento de una serie de objetivos y planteamientos que se desean alcanzar en la culminación del mismo. A continuación, se exponen los objetivos definidos por la organización:

- La infraestructura actual en el centro de datos presenta un tiempo de vida útil cercano a su finalización, por lo que la organización desea incursionar en el campo de la virtualización para hacer frente a esta situación. Además, la virtualización ha sido implementada por varias organizaciones, miembros de la marca global, por lo que esta técnica está en vías de estandarización.

- En principio se cuentan con 11 servidores físicos de propósito general, ubicados en el centro de datos de la oficina principal. Estos servidores atienden los requerimientos varios del día a día del personal activo de la organización, así como información de clientes y socios. Se requiere una categorización de cada uno de los servidores, servicios y aplicaciones por niveles de riesgo y criticidad, así como demás características de rendimiento, procesamiento y almacenamiento para determinar candidatos a ser virtualizados.

- La soluciones en el mercado elegidas para la implementación del proyecto son las siguientes:

- IBM BladeCenter S como plataforma física, con el fin de cambiar el paradigma de una infraestructura de servidores dispuestos en rack a una infraestructura sostenida por servidores blades que alojen varias instancias de sistemas operativos, conocidas como: máquinas virtuales.

- VMware como plataforma virtual, con el fin de alojar diversas máquinas virtuales bajo el sistema operativo de control: ESXi y la suite de productos vSphere para tareas de gestión y mantenimiento.

- El impacto de la virtualización en los usuarios debe ser mínimo en términos de migraciones de sistemas con periodos de inactividad cortos que no afecten con la continuidad de negocio. Con respecto a las actividades diarias, los sistemas virtuales deben ofrecer niveles de rendimientos similares e incluso superiores a los ofrecidos por los sistemas físicos, a fin de que los usuarios tengan el mayor impacto positivo disponible.

- El centro de datos debe estar capacitado para cumplir con los requerimientos de energía, espacio y enfriamiento de la plataforma física a adoptar, a fin de asegurar su correcto funcionamiento. Además, los componentes físicos (procesadores, memoria, discos, dispositivos de entrada y salida, entre otros) deben ser compatibles con los sistemas operativos usados.

- En la migración de sistemas, se deben contar con respaldos de configuración e información más recientes. Todas las características del servidor deben estar documentadas y disponible. Esta tarea debe ser ejecutada por personal capacitado, preferiblemente los administradores, asegurando el soporte técnico en caso de inconvenientes.

4.2. Infraestructura física

Una vez planteados los objetivos a alcanzar en el proyecto de virtualización, se requiere analizar cada uno de los servidores y aplicaciones involucrados en la infraestructura física. Dicho análisis debe contemplar una serie de parámetros que identifiquen y califiquen a estos servidores a fin de tomar la decisión de incorpóralos a la infraestructura virtual diseñada ó por el contrario, mantenerlos dentro de la organización inicial de la plataforma tecnológica.

Principalmente, el objetivo del análisis de servidores y aplicaciones es determinar su nivel de criticidad, un aspecto importante a la hora de tomar decisiones con respecto a los cambios que requieren en términos de funcionalidad, seguridad y mantenimiento. Una organización que establezca una categorización de sus sistemas podrá elevar los niveles de gestión de los mismos y garantizará retornos de inversión adecuados.

A continuación, en la tabla 4.1 se presentan los 11 servidores que conforman la infraestructura física de la organización, describiendo las aplicaciones y servicios que alojan, además del nivel de criticidad asociado. La categorización de los mismos se basa en la consideración de diferentes características, expuestas en la fase de análisis de servidores y aplicaciones de la planificación del proyecto de virtualización.

#	Servidor	Aplicaciones / Servicios	Nivel de criticidad
1	VZ-AD001	Active Directory (DHCP, DNS, File server, Printer Server, CA)	Crítico
2	VZ-LN001	Correo electrónico	Critico
3	VZ-SA001	Sistema de gestión empresarial	Critico
4	VZ-AD002	Active Directory Secundario y servidor Radius (Wi-Fi)	Alto
5	VZ-BC001	Sistema de gestión de clientes	Alto
6	VZ-GB001	Sistema de gestión bancaria	Alto
7	VZ-BD001	Bases de datos de propósito general a usuarios	Alto
8	VZ-SP001	Sistema de facturación	Alto
9	VZ-OR001	Sistema de Contabilidad	Alto
10	VZ-HW001	Control de acceso a instalaciones	Medio
11	VZ-MA001	Actualización de antivirus y cifrado de disco duro	Medio

Tabla 4.1: Nivel de criticidad de los servidores de la organización

Por cada servidor, se ofrece una descripción de su funcionalidad, rendimiento y características de la información procesada con el objetivo de categorizar el nivel de criticidad de los mismos.

4.2.1. Servidor de directorio activo

A continuación se presenta un breve resumen descriptivo acerca de este servidor, con el fin de cumplir con la etapa de análisis de infraestructura y aplicaciones, correspondiente a la planificación de este proyecto.

- **Nombre:** VZ-AD001
- **Ubicación:** oficina de Caracas
- **Descripción de aplicaciones:** el servidor cuenta con una instancia principal del sistema Active Directory de Microsoft que permite ofrecer servicios varios al personal de la organización. Además de las funciones de gestión de usuarios y máquinas pertenecientes a la organización, este servidor ofrece servicios de DHCP para direccionamiento interno de estaciones de trabajo, DNS para resolución de nombres de dominio de estaciones de trabajo y servidores , compartición de directorios para almacenamiento compartido en red, disposición de impresoras multifuncionales en red, servidor web (IIS) y entidad certificadora
- **Unidad de negocio:** toda la organización
- **Número de usuarios**: aproximadamente 600 usuarios
- **Sistema Operativo:** Windows Server 2008 R2
- **Cargas de trabajo:** Active Directory Certificate Services, Active Directory Domain Services, Active Directory Web Services, Network File System, Distributed File System Replication, DHCP, DNS, File Replication Service, File Server Resource Manager, Group Policy, IIS, Print Spooler, World Wide Web Publishing, entre otros
- **Estadísticas de uso:** el servidor cuenta con un procesador Xeon x333 Quad Core de 50 GHz con un promedio de 16% de uso y un 81% de frecuencia máxima. Cuenta con dos unidades de almacenamiento local de 70 GB y 400 GB respectivamente con un promedio de 49 Kbps de E/S y 15% en tiempo de actividad. Un promedio de 4Mbps de E/S en red y una memoria de 10GB con 31% de uso físico aproximado

En la figura 4.1 se muestran los resultados del monitor de recursos de Windows aplicado en el servidor durante un horario de actividad promedio.

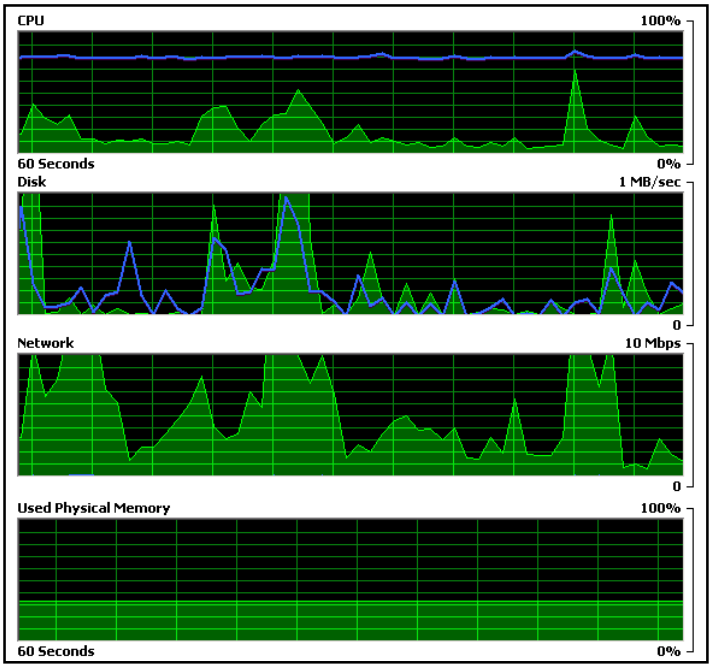

Figura 4.1: Estadísticas de uso del servidor de directorio activo

De acuerdo a la planificación, se requiere la clasificación de la información gestionada por este servidor, la cual se presenta a continuación:

- **Clasificación de la información:** información de distribución restringida
- **Confidencialidad:** el tipo de información procesada y almacenada es propiedad de la organización, la fuga de la misma tendría un impacto severo en el negocio y un impacto significativo en la reputación de la organización
- **Integridad:** la imprecisión de la información dentro de la organización tendría un impacto significativo en el negocio y en la reputación de la organización
- **Disponibilidad:** el tiempo de indisponibilidad sin causar impacto en la organización es de menos de 2 horas, provocando un impacto significativo en el negocio y en la reputación de la organización

Tomando en consideración los planteamientos expuestos anteriormente, el servidor de directorio activo de la organización es calificado con un nivel de criticidad crítico.

4.2.2. Servidor de correo electrónico

A continuación se presenta un breve resumen descriptivo acerca de este servidor, con el fin de cumplir con la etapa de análisis de infraestructura y aplicaciones, correspondiente a la planificación de este proyecto.

- **Nombre:** VZ-LN001
- **Ubicación:** oficina de Caracas
- **Descripción de aplicaciones:** es el servidor de correo electrónico interno de la oficina principal de la organización
- **Unidad de negocio:** personal de la oficina de Caracas
- **Número de usuarios:** aproximadamente 600 usuarios
- **Sistema operativo:** Windows Server 2003
- **Cargas de trabajo:** alrededor de 102 procesos, incluyendo los correspondientes al servidor de correo electrónico

- **Estadísticas de uso:** el servidor cuenta con un procesador Xeon de 3.80 GHz con un promedio de 5% de uso. Cuenta con una unidad de almacenamiento local de 68 GB con un promedio de 90% de uso aproximado. Un promedio de 2Mbps de E/S en red y una memoria de 2 GB con 58% de uso físico aproximado

En la figura 4.2 se muestran los resultados del gestor de tareas de Windows aplicado en el servidor durante un horario de actividad promedio.

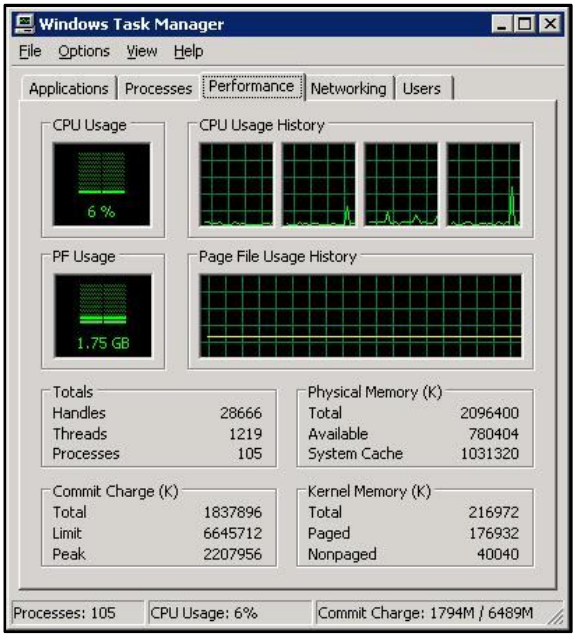

Figura 4.2: Estadísticas de uso del servidor de correo electrónico

De acuerdo a la planificación, se requiere la clasificación de la información gestionada por este servidor, la cual se presenta a continuación:

- **Clasificación de la información:** información de distribución restringida
- **Confidencialidad:** el tipo de información procesada y almacenada es propiedad de la organización, la fuga de la misma tendría un impacto severo en el negocio y un impacto significativo en la reputación de la organización
- **Integridad:** la imprecisión de la información dentro de la organización tendría un impacto significativo en el negocio y en la reputación de la organización
- **Disponibilidad:** el tiempo de indisponibilidad sin causar impacto en la organización es de menos de 2 horas, provocando un impacto significativo en el negocio y en la reputación de la organización

Tomando en consideración los planteamientos expuestos anteriormente, el servidor de correo electrónico de la oficina de Caracas es calificado con un nivel de criticidad crítico

4.2.3. Servidor de gestión empresarial

A continuación se presenta un breve resumen descriptivo acerca de este servidor, con el fin de cumplir con la etapa de análisis de infraestructura y aplicaciones, correspondiente a la planificación de este proyecto.

- **Nombre:** VZ-SA001
- **Ubicación:** Oficina de Caracas
- **Descripción de aplicaciones:** Este servidor se encarga de gestionar una aplicación dirigida al departamento de recursos humanos para el cálculo y pago de los salarios del personal de la organización
- **Unidad de negocio:** Recursos Humanos
- **Número de usuarios:** Aproximadamente 50 usuarios
- **Sistema Operativo:** Windows Server 2000
- **Cargas de trabajo:** alrededor de 94 procesos, incluyendo los servicios de la aplicación de gestión instalada
- **Estadísticas de uso:** el servidor cuenta con un procesador Intel Xeon e5310 de 1.60 GHz con un promedio de 2% de uso. Cuenta con dos unidades de almacenamiento local de 84 GB y 136 GB con un promedio de 64% y 96% de uso respectivamente. La memoria es de 3 GB con 86% de uso físico aproximado

En la figura 4.3 se muestran los resultados del gestor de tareas de Windows aplicado en el servidor durante un horario de actividad promedio.

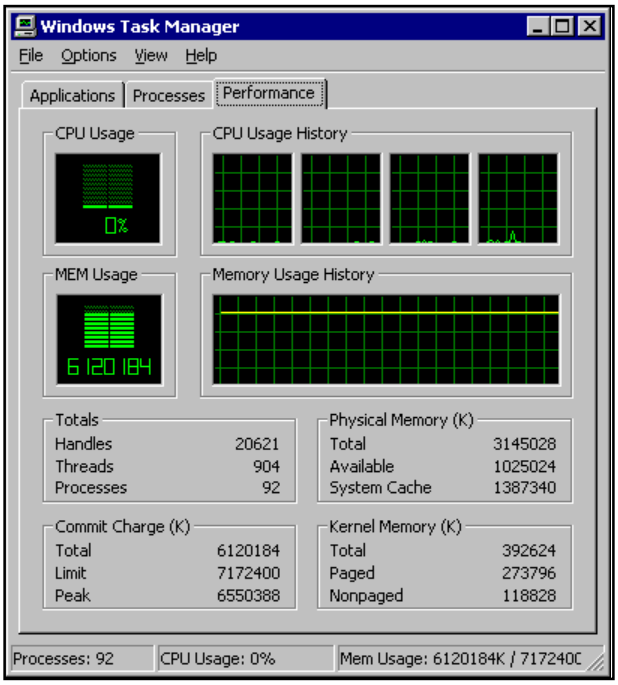

Figura 4.3: Estadísticas de uso del servidor de gestión empresarial

De acuerdo a la planificación, se requiere la clasificación de la información gestionada por este servidor, la cual se presenta a continuación:

- **Clasificación de la información:** Información de distribución restringida
- **Confidencialidad:** El tipo de información procesada y almacenada es propiedad de la organización, la fuga de la misma tendría un impacto significativo en el negocio y en la reputación de la organización
- **Integridad:** La imprecisión de la información dentro de la organización tendría un impacto significativo en el negocio y en la reputación de la organización
- **Disponibilidad:** El tiempo de indisponibilidad sin causar impacto en la organización es de dos a cuatro horas, provocando un impacto significativo en el negocio y en la reputación de la organización

Tomando en consideración los planteamientos expuestos anteriormente, este servidor es calificado con un nivel de criticidad crítico.

4.2.4. Servidor Radius

A continuación se presenta un breve resumen descriptivo acerca de este servidor, con el fin de cumplir con la etapa de análisis de infraestructura y aplicaciones, correspondiente a la planificación de este proyecto.

- **Nombre:** VZ-AD002
- **Ubicación:** Oficina de Caracas
- **Descripción de aplicaciones:** Este servidor está configurado en *modo espejo* para suplir las funciones de dominio y DNS del servidor de directorio activo. Además, incluye servicios de de acceso, autenticación y políticas de red para red Wi-Fi
- **Unidad de negocio:** Personal de la oficina de Caracas
- **Número de usuarios:** Aproximadamente 600 usuarios
- **Sistema operativo:** Windows Server 2003
- **Cargas de trabajo:** el servidor cuenta con una instancia secundaria del sistema Active Directory de Microsoft que permite ofrecer servicios varios al personal de la organización. Además de las funciones de gestión de usuarios y máquinas pertenecientes a la organización, este servidor ofrece servicios de políticas de grupo y autenticación de acceso a la red inalámbrica Wi-Fi
- **Estadísticas de uso:** el servidor cuenta con un procesador Intel Xeon de 3.80 GHz con un promedio de 2% de uso. Cuenta con dos unidades de almacenamiento local de 68 GB y 136 GB con un promedio de 90% y 80% de uso respectivamente. La memoria es de 2 GB con 50% de uso físico aproximado

En la figura 4.4 se muestran los resultados del gestor de tareas de Windows aplicado en el servidor durante un horario de actividad promedio.

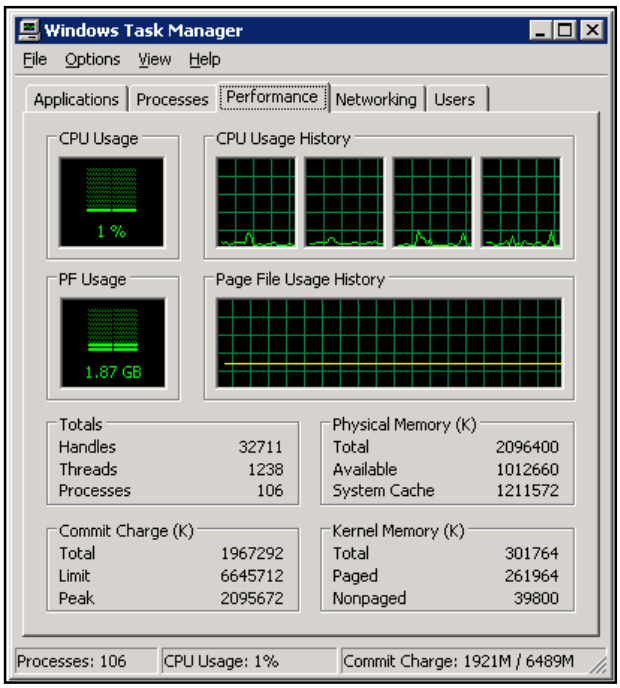

Figura 4.4: Estadísticas de uso del servidor Radius

De acuerdo a la planificación, se requiere la clasificación de la información gestionada por este servidor, la cual se presenta a continuación:

- **Clasificación de la información**: Información de distribución restringida
- **Confidencialidad:** El tipo de información procesada y almacenada es propiedad de la organización, la fuga de la misma tendría un impacto menor en el negocio y en la reputación de la organización
- **Integridad:** La imprecisión de la información dentro de la organización tendría un impacto significativo en el negocio y en la reputación de la organización
- **Disponibilidad:** El tiempo de indisponibilidad sin causar impacto en la organización es de 2 días, provocando un impacto severo en el negocio

Tomando en consideración los planteamientos expuestos anteriormente, el servidor Radius de la organización es calificado con un nivel de criticidad alto.

4.2.5. Servidor de gestión de clientes

A continuación se presenta un breve resumen descriptivo acerca de este servidor, con el fin de cumplir con la etapa de análisis de infraestructura y aplicaciones, correspondiente a la planificación de este proyecto.

- **Nombre:** VZ-BC001
- **Ubicación:** Oficina de Caracas
- **Descripción de aplicaciones:** Este servidor se encarga de la gestión de bases de datos con información de auditorías realizadas a clientes
- **Unidad de negocio:** Líneas de servicio particulares de la organización
- **Número de usuarios**: Aproximadamente 400 usuarios
- **Sistema operativo:** Windows Server 2003
- **Cargas de trabajo:** el servidor cuenta con una base de datos que aloja información de clientes, la cual es accedida a través de los clientes de correo electrónico instalado en las estaciones de trabajo. Básicamente, atiende operaciones de entrada y salida.
- **Estadísticas de uso:** el servidor cuenta con un procesador Intel Xeon de 3.80 GHz con un promedio de 40% de uso. Cuenta con dos unidades de almacenamiento local de 68 GB y 750 GB con un promedio de 20% y 70% de uso respectivamente. La memoria es de 8 GB con 22% de uso físico aproximado

En la figura 4.5 se muestran los resultados del gestor de tareas de Windows aplicado en el servidor durante un horario de actividad promedio.

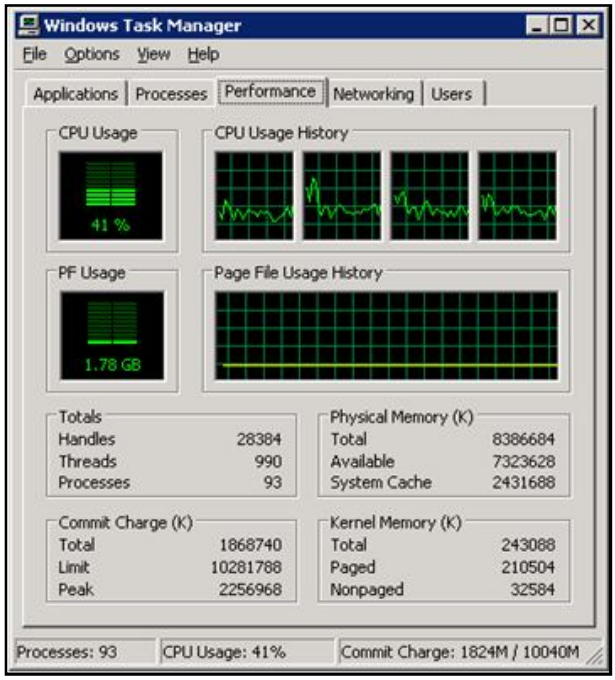

Figura 4.5: Estadísticas de uso del servidor de gestión de clientes

De acuerdo a la planificación, se requiere la clasificación de la información gestionada por este servidor, la cual se presenta a continuación:

- **Clasificación de la información:** Información de distribución restringida
- **Confidencialidad:** El tipo de información procesada y almacenada es propiedad de la organización, la fuga de la misma tendría un impacto significativo en el negocio y en la reputación de la organización
- **Integridad:** La imprecisión de la información dentro de la organización tendría un impacto severo en el negocio y en la reputación de la organización
- **Disponibilidad:** El tiempo de indisponibilidad sin causar impacto en la organización es de un día, provocando un impacto significativo en el negocio y en la reputación de la organización

Tomando en consideración los planteamientos expuestos anteriormente, este servidor es calificado con un nivel de criticidad alto.

4.2.6. Servidor de gestión bancaria

A continuación se presenta un breve resumen descriptivo acerca de este servidor, con el fin de cumplir con la etapa de análisis de infraestructura y aplicaciones, correspondiente a la planificación de este proyecto.

- **Nombre:** VZ-GB001
- **Ubicación:** Oficina de Caracas
- **Descripción de aplicaciones:** Este servidor se encarga de gestionar las bases de datos con información específica de auditorías realizadas a entidades bancarias
- **Unidad de negocio:** Líneas de servicio especificas de la organización
- **Número de usuarios:** Aproximadamente 50 personas
- **Sistema operativo:** Windows Server 2003
- **Cargas de trabajo:** el servidor cuenta con una base de datos que aloja información de bancos, la cual es accedida a través de los clientes de correo electrónico instalado en las estaciones de trabajo. Básicamente, atiende operaciones de entrada y salida.

- **Estadísticas de uso:** el servidor cuenta con un procesador Intel Xeon de 3.20 GHz con un promedio de 2% de uso. Cuenta con dos unidades de almacenamiento local de 68 GB y 100 GB con un promedio de 80% y 75% de uso respectivamente. La memoria es de 4 GB con 40% de uso físico aproximado.

En la figura 4.6 se muestran los resultados del gestor de tareas de Windows aplicado en el servidor durante un horario de actividad promedio.

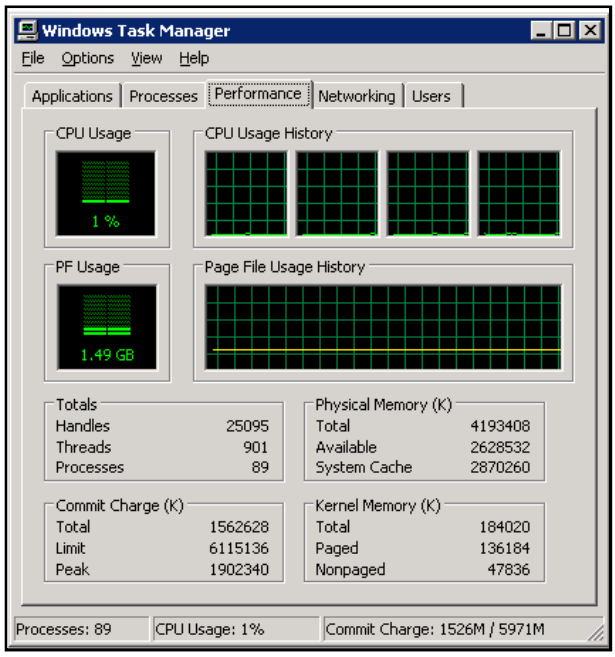

Figura 4.6: Estadísticas de uso del servidor de gestión bancaria

De acuerdo a la planificación, se requiere la clasificación de la información gestionada por este servidor, la cual se presenta a continuación:

- **Clasificación de la información:** Información de distribución restringido
- **Confidencialidad:** El tipo de información procesada y almacenada es propiedad de la organización, la fuga de la misma tendría un impacto significativo en el negocio y en la reputación de la organización
- **Integridad:** La imprecisión de la información dentro de la organización tendría un impacto severo en el negocio y en la reputación de la organización
- **Disponibilidad:** El tiempo de indisponibilidad sin causar impacto en la organización es de tres días, provocando un impacto significativo en el negocio y en la reputación de la organización

Tomando en consideración los planteamientos expuestos anteriormente, este servidor es calificado con un nivel de criticidad alto.

4.2.7. Servidor de base de datos (propósito general)

A continuación se presenta un breve resumen descriptivo acerca de este servidor, con el fin de cumplir con la etapa de análisis de infraestructura y aplicaciones, correspondiente a la planificación de este proyecto.

- **Nombre:** VZ-BD001
- **Ubicación:** Oficina de Caracas
- **Descripción de aplicaciones:** Este servidor se encarga de gestionar las bases de datos de aplicaciones de propósito general, integradas al servicio de mensajería interna. Además, se encarga de gestionar envío y recibo de correos electrónicos externos al personal de la organización
- **Unidad de negocio:** Toda la organización
- **Número de usuarios:** Aproximadamente 900 usuarios
- **Sistema operativo:** Windows Server 2003
- **Cargas de trabajo:** el servidor cuenta con un conjunto de bases de datos que alojan información general de la organización, la cual es accedida a través de los clientes de correo electrónico instalado en las estaciones de trabajo. Básicamente, atiende operaciones de entrada y salida.
- **Estadísticas de uso:** el servidor cuenta con un procesador Intel Xeon de 3.20 GHz con un promedio de 15% de uso. Cuenta con dos unidades de almacenamiento local de 68 GB y 250 GB con un promedio de 80% y 90% de uso respectivamente. La memoria es de 3 GB con 75% de uso físico aproximado.

En la figura 4.7 se muestran los resultados del gestor de tareas de Windows aplicado en el servidor durante un horario de actividad promedio.

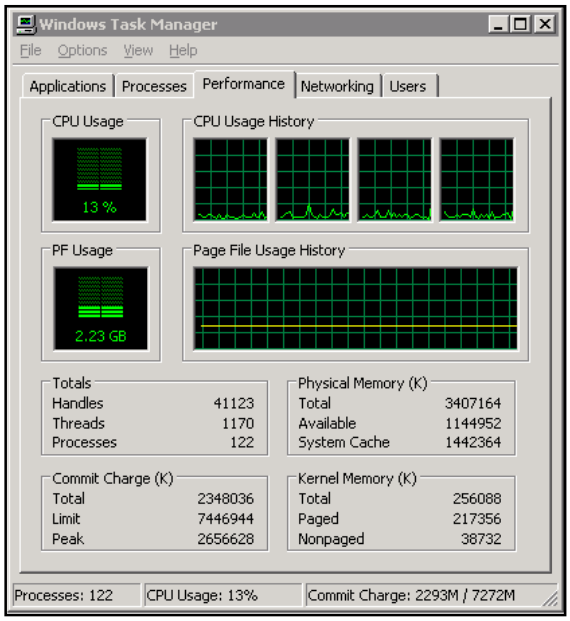

Figura 4.7: Estadísticas de uso del servidor de bases de datos (propósito general)

De acuerdo a la planificación, se requiere la clasificación de la información gestionada por este servidor, la cual se presenta a continuación:

- **Clasificación de la información:** Información de uso interno
- **Confidencialidad:** El tipo de información procesada y almacenada es propiedad de la organización, la fuga de la misma tendría un impacto severo en el negocio y en la reputación de la organización
- **Integridad:** La imprecisión de la información dentro de la organización tendría un impacto mínimo en el negocio y en la reputación de la organización
- **Disponibilidad:** El tiempo de indisponibilidad sin causar impacto en la organización es de dos a cuatro horas, provocando un impacto significativo en el negocio y en la reputación de la organización

Tomando en consideración los planteamientos expuestos anteriormente, este servidor es calificado con un nivel de criticidad alto.

4.2.8. Servidor de facturación

A continuación se presenta un breve resumen descriptivo acerca de este servidor, con el fin de cumplir con la etapa de análisis de infraestructura y aplicaciones, correspondiente a la planificación de este proyecto.

- **Nombre:** VZ-SP001
- **Ubicación:** Oficina de Caracas
- **Descripción de aplicaciones:** Este servidor aloja una aplicación desarrollada por la organización usando herramientas como Microsoft Visual Studio y SQL Server, basada en varios modelos de gestión de proyectos relacionados a hojas de tiempo, gastos, recibos, cuentas por pagar, reportes de estadísticas y administración de seguridad
- **Unidad de negocio:** Toda la organización
- **Número de usuarios:** Aproximadamente 900 usuarios
- **Sistema operativo:** Windows Server 2003
- **Cargas de trabajo:** el servidor cuenta con la instancia principal del sistema de facturación de la organización, en conjunto con una serie de bases de datos. También aloja ofrece un servicio que permite a los usuarios acceder al sistema vía web y gestionar la información referente a carga de horas laborales, anticipos y vacaciones.
- **Estadísticas de uso:** el servidor cuenta con un procesador Intel Xeon de 3.20 GHz con un promedio de 27% de uso. Cuenta con dos unidades de almacenamiento local de 68 GB y 50 GB con un promedio de 90% y 60% de uso respectivamente. La memoria es de 4 GB con 50% de uso físico aproximado.

En la figura 4.8 se muestran los resultados del gestor de tareas de Windows aplicado en el servidor durante un horario de actividad promedio.

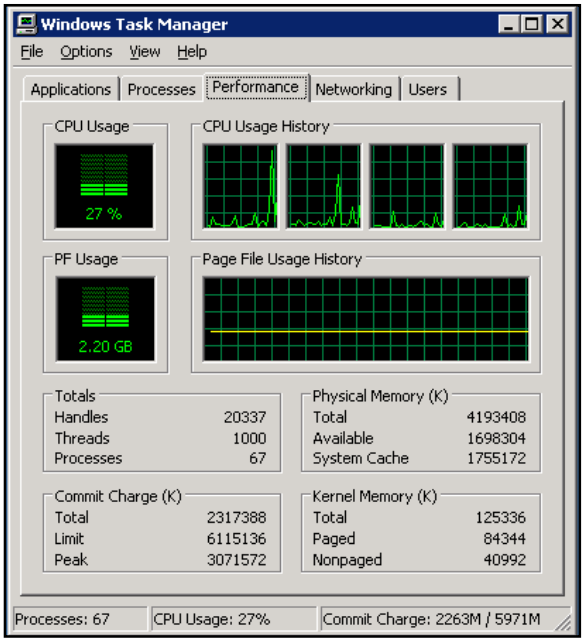

Figura 4.8: Estadísticas de uso del servidor de facturación

De acuerdo a la planificación, se requiere la clasificación de la información gestionada por este servidor, la cual se presenta a continuación:

- **Clasificación de la información:** Información de uso distribución restringida
- **Confidencialidad:** El tipo de información procesada y almacenada es propiedad de la organización, la fuga de la misma tendría un impacto severo en el negocio y en la reputación de la organización
- **Integridad:** La imprecisión de la información dentro de la organización tendría un impacto significativo en el negocio y en la reputación de la organización
- **Disponibilidad:** El tiempo de indisponibilidad sin causar impacto en la organización es de dos a cuatro horas, provocando un impacto severo en el negocio y en la reputación de la organización

Tomando en consideración los planteamientos expuestos anteriormente, este servidor es calificado con un nivel de criticidad alto.

4.2.9. Servidor de contabilidad

A continuación se presenta un breve resumen descriptivo acerca de este servidor, con el fin de cumplir con la etapa de análisis de infraestructura y aplicaciones, correspondiente a la planificación de este proyecto.

- **Nombre:** VZ-OR001
- **Ubicación:** Oficina de Caracas
- **Descripción de aplicaciones:** Este servidor aloja un sistema de contabilidad que gestiona registros contables y pagables
- **Unidad de negocio:** Personal de contabilidad de la información
- **Número de usuarios:** Aproximadamente 200 usuarios
- **Sistema operativo:** Windows Server 2003
- **Cargas de trabajo:** el servidor cuenta con la instancia principal del sistema de contabilidad de la organización, en conjunto con una serie de bases de datos.
- **Estadísticas de uso:** el servidor cuenta con un procesador Intel Xeon de 2.53 GHz con un promedio de 27% de uso. Cuenta con dos unidades de almacenamiento local de 80 GB y 244 GB con un promedio de 85% y 60% de uso respectivamente. La memoria es de 6 GB con 30% de uso físico aproximado.

En la figura 4.9 se muestran los resultados del gestor de tareas de Windows aplicado en el servidor durante un horario de actividad promedio.

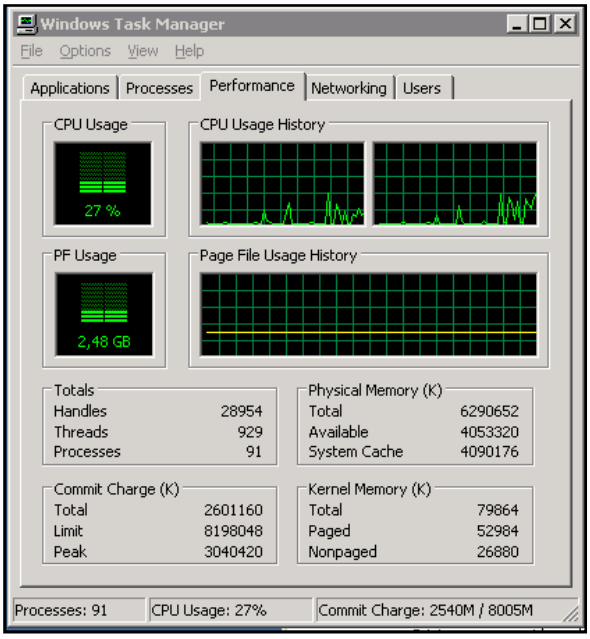

Figura 4.9: Estadísticas de uso del servidor de contabilidad

De acuerdo a la planificación, se requiere la clasificación de la información gestionada por este servidor, la cual se presenta a continuación:

- **Clasificación de la información:** Información de distribución restringida
- **Confidencialidad:** El tipo de información procesada y almacenada es propiedad de la organización, la fuga de la misma tendría un impacto severo en el negocio y en la reputación de la organización
- **Integridad:** La imprecisión de la información dentro de la organización tendría un impacto severo en el negocio y en la reputación de la organización
- **Disponibilidad:** El tiempo de indisponibilidad sin causar impacto en la organización es de dos horas, provocando un impacto severo en el negocio y en la reputación de la organización

Tomando en consideración los planteamientos expuestos anteriormente, este servidor es calificado con un nivel de criticidad alto.

4.2.10. Servidor de control de acceso a instalaciones

A continuación se presenta un breve resumen descriptivo acerca de este servidor, con el fin de cumplir con la etapa de análisis de infraestructura y aplicaciones, correspondiente a la planificación de este proyecto.

- **Nombre:** VZ-HW001
- **Ubicación:** Oficina de Caracas
- **Descripción de aplicaciones:** Este servidor se encarga de administrar el control de acceso al edificio de la oficina principal de la organización
- **Unidad de negocio:** Personal de la oficina de Caracas
- **Número de usuarios:** Aproximadamente 600 usuarios
- **Sistema operativo:** Windows Server 2003
- **Cargas de trabajo:** el servidor cuenta con la instancia principal del sistema de acceso a las instalaciones de la organización. Es accedido por el personal de seguridad de la misma para el control de acceso, restricciones y demás operaciones de seguridad.

- **Estadísticas de uso:** el servidor cuenta con un procesador Intel Xeon de 3.20 GHz con un promedio de 27% de uso. Cuenta con dos unidades de almacenamiento local de 20 GB y 50 GB con un promedio de 95% y 90% de uso respectivamente. La memoria es de 3 GB con 75% de uso físico aproximado.

En la figura 4.10 se muestran los resultados del gestor de tareas de Windows aplicado en el servidor durante un horario de actividad promedio.

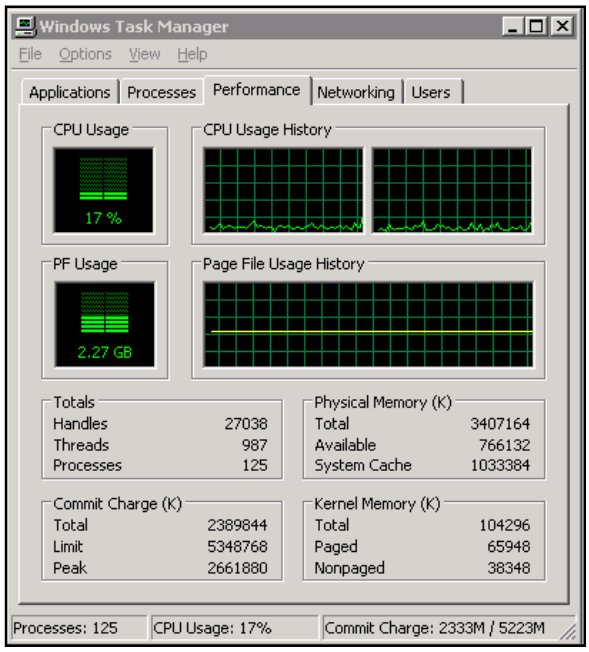

Figura 4.10: Estadísticas de uso del servidor de contabilidad

De acuerdo a la planificación, se requiere la clasificación de la información gestionada por este servidor, la cual se presenta a continuación:

- **Clasificación de la información:** Información de distribución restringida
- **Confidencialidad:** El tipo de información procesada y almacenada es propiedad de la organización, la fuga de la misma tendría un impacto menor en el negocio y en la reputación de la organización
- **Integridad:** La imprecisión de la información dentro de la organización tendría un impacto severo en el negocio y en la reputación de la organización
- **Disponibilidad:** El tiempo de indisponibilidad sin causar impacto en la organización es de más de una semana, provocando un impacto menor en el negocio y en la reputación de la organización

Tomando en consideración los planteamientos expuestos anteriormente, el servidor de control de acceso a instalaciones es calificado con un nivel de criticidad medio.

4.2.11. Servidor de actualización de antivirus y cifrado de discos

A continuación se presenta un breve resumen descriptivo acerca de este servidor, con el fin de cumplir con la etapa de análisis de infraestructura y aplicaciones, correspondiente a la planificación de este proyecto.

- **Nombre:** VZ-MA001
- **Ubicación:** Oficina de Caracas
- **Descripción de aplicaciones:** Este servidor aloja la instancia principal de una aplicación capaz de actualizar los sistemas antivirus de la estaciones de trabajo y servidores, además de cifrar los discos duro de los mismos, cumpliendo con las políticas de seguridad de activos de información de la organización
- **Unidad de negocio:** Toda la organización
- **Número de usuarios:** Aproximadamente 900 usuarios
- **Sistema operativo:** Windows Server 2003
- **Cargas de trabajo:** el servidor cuenta con la instancia principal de un sistema orquestador de servicios que se encarga de gestionar las actualizaciones de los programas anti-virus de las estaciones de trabajo. Del mismo modo, se encarga de instalar un programa de seguridad que cifra el contenido del disco duro de las mismas, por lo que se encuentra en constante interacción con los usuarios de la organización.
- **Estadísticas de uso:** el servidor cuenta con un procesador Intel Xeon de 2.00 GHz con un promedio de 2% de uso. Cuenta con una unidad de almacenamiento local de 300 GB con un promedio de 35% de uso respectivamente. La memoria es de 3 GB con 90% de uso físico aproximado.

En la figura 4.11 se muestran los resultados del gestor de tareas de Windows aplicado en el servidor durante un horario de actividad promedio.

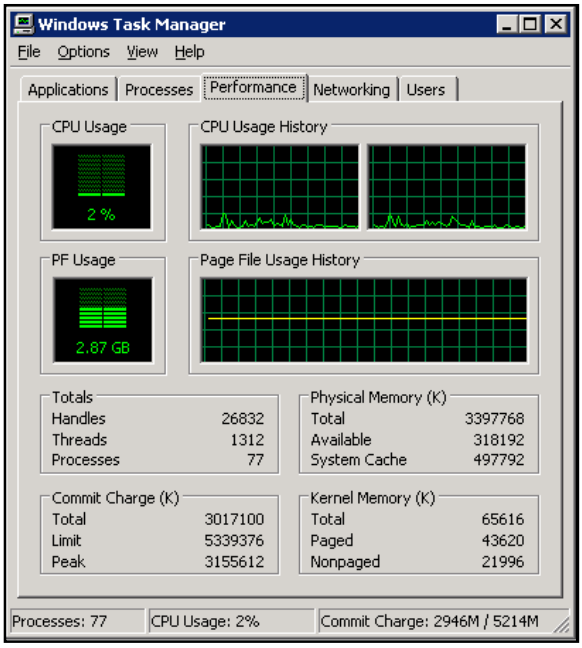

Figura 4.11: Estadísticas de uso del servidor de actualización de anti-virus y cifrado de discos

De acuerdo a la planificación, se requiere la clasificación de la información gestionada por este servidor, la cual se presenta a continuación:

- **Clasificación de la información**: Información de distribución restringido
- **Confidencialidad:** El tipo de información procesada y almacenada es propiedad de la organización, la fuga de la misma tendría un impacto menor en el negocio y en la reputación de la organización
- **Integridad:** La imprecisión de la información dentro de la organización tendría un impacto menor en el negocio y en la reputación de la organización

- **Disponibilidad:** El tiempo de indisponibilidad sin causar impacto en la organización es de más de una semana, provocando un impacto severo en el negocio y en la reputación de la organización

Tomando en consideración los planteamientos expuestos anteriormente, este servidor es calificado con un nivel de criticidad medio.

4.3. Servidores candidatos a virtualizar

Continuando con la planificación del proyecto, la siguiente etapa es considerar aspectos particulares en los diferentes servidores para determinar si realmente es necesaria su migración a un entorno virtual. Muchos de estos aspectos son los cambios en la funcionalidad, tiempos de inactividad entre migraciones e impacto de las mismas [37], incluyendo la categorización de la criticidad y el impacto de estos servidores sobre las actividades de negocio.

A continuación se presentan los lineamientos estudiados en los servidores de propósito general de la organización con respecto a su incorporación en la plataforma virtual:

- El servidor de directorio activo es uno de los componentes críticos más importantes de la infraestructura tecnológica de la organización, por lo que su indisponibilidad puede acarrear un impacto negativo en las actividades de negocio. A pesar de que cuenta con recursos compatibles con la virtualización, no es considerado un candidato para ser incorporado en la infraestructura virtual.

- Los componentes de los servidores Radius, gestión de clientes y de correo electrónico de la oficina principal están cercanos a la finalización de su vida útil, por lo que se consideran candidatos directos a una migración. La virtualización de estos servidores pueden aprovecharse para actualizar a un sistema operativo más reciente y hacer uso de más recursos, con tan sólo horas de indisponibilidad.

- Los sistemas de gestión bancaria, actualización de antivirus y de bases de datos de propósito general son dos de los servidores más antiguos de la organización. Su compatibilidad con una infraestructura virtual no está completamente asegurada, además de que cuentan con un nivel de criticidad alto y son usados a diario de manera ininterrumpida. Cuentan con contratos de mantenimiento y soporte adecuados que los descalifican como candidatos a ser virtualizados.

- Los sistemas de gestión empresarial y facturación requieren de una pronta actualización, tanto de sistema operativo como de sus componentes funcionales. Sin embargo, esto requiere que personal externo se involucre en el proceso a manera de soporte para prevenir los cambios de funcionalidad que se pueden presentar. Las nuevas instancias de estos servidores, las cuales estarán en fase de prueba, son candidatos a ser sistemas virtuales.

- El servidor de contabilidad cumple con las características que requiere una migración a un ambiente virtual. Además, se tiene planificado su actualización (en conjunto con los sistemas de gestión empresarial y finanzas), por lo que una instancia de pruebas también debe ser considerada para su incorporación en la plataforma virtual.

- Finalmente, el servidor de control de acceso a instalaciones esta cercano a su desincorporación de la infraestructura. Particularmente, requiere de una restructuración completa que no está planificada dentro de la línea de tiempo considerada en este documento. Por lo tanto, no es candidato a ser virtualizado.

Es así como en la tabla 4.2 se muestran los servidores que son descartados para su migración a la plataforma virtual, de manera de no comprometer su funcionalidad y disponibilidad, basándose en las características anteriormente expuestas.

#	Servidor	Aplicaciones / Servicios	Nivel de criticidad
1	VZ-AD001	Active Directory (DHCP, DNS, File server, Print Server, CA)	Critico
2	VZ-SA001	Sistema de gestión empresarial	Critico
3	VZ-BD001	Bases de datos de propósito general a usuarios	Alto
4	VZ-SP001	Sistema de facturación	Alto
5	VZ-HW001	Control de acceso a instalaciones	Medio
6	VZ-MA001	Actualización de antivirus y cifrado de disco duro	Medio

Tabla 4.2: Servidores descartados para la virtualización

De esta manera se demuestra que no todos los servidores consolidados en una plataforma sometida a un proyecto de virtualización son candidatos directos a ser virtualizados. Se debe tomar en cuenta de que se trata de una tecnología que trae consigo una diversidad de cambios de los cuales no es posible garantizar la total compatibilidad de los sistemas.

Particularmente, de acuerdo a los lineamientos establecidos anteriormente, de los 13 servidores presentes en la organización, 5 de ellos serán sometidos a una migración. En la tabla 4.3 lista dichos servidores:

#	Servidor	Aplicaciones / Servicios	Nivel de criticidad
1	VZ-LN001	Correo electrónico	Critico
2	VZ-AD002	Active Directory secundario y servidor Radius (Wi-Fi)	Alto
3	VZ-BC001	Sistema de gestión de clientes	Alto
4	VZ-GB001	Sistema de gestión bancaria	Alto
5	VZ-OR001	Sistema de contabilidad	Alto

Tabla 4.3: Servidores físicos candidatos a virtualizar

Durante la migración de los sistemas presentados anteriormente, la organización presentó una serie de requerimientos que correspondían a la consolidación de varios servidores de propósito general, con el fin de aumentar su productividad añadiendo nuevas tecnologías.

Dados los requisitos de estos servidores, los mismos fueron dispuestos en la plataforma virtual de manera directa. A continuación se presentan los parámetros que fueron considerados en el análisis de criticidad.

4.3.1. Servidor Proxy

A continuación se presenta un breve resumen descriptivo acerca de este servidor, con el fin de cumplir con la etapa de análisis de infraestructura y aplicaciones, correspondiente a la planificación de este proyecto.

- **Nombre:** VZ-TM001
- **Ubicación:** Oficina de Caracas
- **Descripción de aplicaciones:** El servidor cuenta con la instancia principal de un Gateway de seguridad basado en web, destinado para asegurar el acceso a Internet
- **Unidad de negocio:** Toda la organización
- **Número de usuarios:** Aproximadamente 900 usuarios

De acuerdo a la planificación, se requiere la clasificación de la información gestionada por este servidor, la cual se presenta a continuación:

- **Clasificación de la información:** Información de distribución restringida
- **Confidencialidad:** El tipo de información procesada y almacenada es propiedad de la organización, la fuga de la misma tendría un impacto severo en el negocio y en la reputación de la organización
- **Integridad:** La imprecisión de la información dentro de la organización tendría un impacto significativo en el negocio y en la reputación de la organización
- **Disponibilidad:** El tiempo de indisponibilidad sin causar impacto en la organización es de menos de 2 horas, provocando un impacto significativo en el negocio y en la reputación de la organización

Tomando en consideración los planteamientos expuestos anteriormente, el servidor Proxy de la organización es calificado con un nivel de criticidad crítico.

4.3.2. Servidor de actualización de aplicaciones y sistemas operativos

A continuación se presenta un breve resumen descriptivo acerca de este servidor, con el fin de cumplir con la etapa de análisis de infraestructura y aplicaciones, correspondiente a la planificación de este proyecto.

- **Nombre:** VZ-SW001
- **Ubicación:** Oficina de Caracas
- **Descripción de aplicaciones:** Este servidor se encarga de instalar y actualizar aplicaciones a las estaciones de trabajo conectadas a la red interna. De igual forma, se encarga de administrar las actualizaciones de los sistemas operativos adoptados en la organización
- **Unidad de negocio**: Toda la organización
- **Número de usuarios:** Aproximadamente 900 usuarios

De acuerdo a la planificación, se requiere la clasificación de la información gestionada por este servidor, la cual se presenta a continuación:

- **Clasificación de la información:** Información de distribución restringida
- **Confidencialidad:** El tipo de información procesada y almacenada es propiedad de la organización, la fuga de la misma tendría un impacto menor en el negocio y en la reputación de la organización
- **Integridad:** La imprecisión de la información dentro de la organización tendría un impacto severo en el negocio y en la reputación de la organización
- **Disponibilidad:** El tiempo de indisponibilidad sin causar impacto en la organización es de menos de una semana, provocando un impacto severo en el negocio y en la reputación de la organización

Tomando en consideración los planteamientos expuestos anteriormente, el servidor de distribución de aplicaciones y actualización de sistemas operativos de la organización es calificado con un nivel de criticidad alto.

4.3.3. Servidor de correo en dispositivos móviles (Android y Apple)

A continuación se presenta un breve resumen descriptivo acerca de este servidor, con el fin de cumplir con la etapa de análisis de infraestructura y aplicaciones, correspondiente a la planificación de este proyecto.

- **Nombre:** VZ-GD001
- **Ubicación:** Oficina de Caracas
- **Descripción de aplicaciones:** Este servidor se encarga de transmitir los correos electrónicos, contactos y calendario del personal gerencial de la organización hacia dispositivos móviles con sistemas operativos Android y IOS.
- **Unidad de negocio:** Personal gerencial de la organización
- **Número de usuarios**: Aproximadamente 50 personas

De acuerdo a la planificación, se requiere la clasificación de la información gestionada por este servidor, la cual se presenta a continuación:

- **Clasificación de la información**: Información de distribución restringida
- **Confidencialidad:** El tipo de información procesada y almacenada es propiedad de la organización, la fuga de la misma tendría un impacto severo en el negocio y en la reputación de la organización
- **Integridad:** La imprecisión de la información dentro de la organización tendría un impacto menor en el negocio y en la reputación de la organización
- **Disponibilidad:** El tiempo de indisponibilidad sin causar impacto en la organización es de más de un día, provocando un impacto menor en el negocio y en la reputación de la organización

Tomando en consideración los planteamientos expuestos anteriormente, este servidor es calificado con un nivel de criticidad medio.

4.3.4. Servidor de correo en dispositivos móviles (Blackberry)

A continuación se presenta un breve resumen descriptivo acerca de este servidor, con el fin de cumplir con la etapa de análisis de infraestructura y aplicaciones, correspondiente a la planificación de este proyecto.

- **Nombre:** VZ-BB001
- **Ubicación:** Oficina de Caracas
- **Descripción de aplicaciones:** Este servidor se encarga de transmitir los correos electrónicos, contactos y calendario del personal gerencial de la organización hacia dispositivos móviles Blackberry
- **Unidad de negocio:** Personal gerencial de la organización
- **Número de usuarios:** Aproximadamente 200 personas

De acuerdo a la planificación, se requiere la clasificación de la información gestionada por este servidor, la cual se presenta a continuación:

- **Clasificación de la información**: Información de distribución restringida
- **Confidencialidad:** El tipo de información procesada y almacenada es propiedad de la organización, la fuga de la misma tendría un impacto severo en el negocio y en la reputación de la organización
- **Integridad:** La imprecisión de la información dentro de la organización tendría un impacto menor en el negocio y en la reputación de la organización
- **Disponibilidad:** El tiempo de indisponibilidad sin causar impacto en la organización es de más de un día, provocando un impacto menor en el negocio y en la reputación de la organización

Tomando en consideración los planteamientos expuestos anteriormente, este servidor es calificado con un nivel de criticidad medio.

4.3.5. Servidor de mensajería instantánea

A continuación se presenta un breve resumen descriptivo acerca de este servidor, con el fin de cumplir con la etapa de análisis de infraestructura y aplicaciones, correspondiente a la planificación de este proyecto.

- **Nombre:** VZ-SM001
- **Ubicación:** Oficina de Caracas
- **Descripción de aplicaciones:** Este servidor se encarga de gestionar la mensajería instantánea corporativa entre las diferentes oficinas de la organización
- **Unidad de negocio:** Toda la organización
- **Número de usuarios:** Aproximadamente 900 usuarios

De acuerdo a la planificación, se requiere la clasificación de la información gestionada por este servidor, la cual se presenta a continuación:

- **Clasificación de la información:** Información de uso interno
- **Confidencialidad:** El tipo de información procesada y almacenada es propiedad de la organización, la fuga de la misma tendría un impacto menor en el negocio y en la reputación de la organización
- **Integridad:** La imprecisión de la información dentro de la organización tendría un impacto menor en el negocio y en la reputación de la organización
- **Disponibilidad:** El tiempo de indisponibilidad sin causar impacto en la organización es de más de una semana, provocando un impacto menor en el negocio y en la reputación de la organización

Tomando en consideración los planteamientos expuestos anteriormente, este servidor es calificado con un nivel de criticidad bajo.

Es así como un total de 5 servidores virtuales son incorporados en la plataforma virtual. Sin embargo, la implementación del proyecto de virtualización requiere la instalación de una aplicación orquestadora de servicios para gestión de ambientes virtuales, lo que sugiere la implementación de un servidor adicional en el esquema planteado.

Finalmente, dadas las condiciones de 3 de los servidores físicos descartados para la migración (sistema de gestión empresarial, facturación y contabilidad), la organización solicitó la implementación de 3 nuevos servidores destinados a la sustitución de los anteriormente nombrados, los cuales no estarán sujetos a una fase de análisis de criticidad hasta su total implementación.

Es así como un total de 9 servidores serán incluidos directamente en la infraestructura como servidores virtuales. Los mismos se encuentran listados en la tabla 4.4, dispuesta a continuación:

#	Servidor	Aplicaciones / Servicios	Nivel de criticidad
1	VZ-TM001	Proxy (Políticas de acceso a Internet)	Critico
2	VZ-SW001	Distribución de aplicaciones y actualizaciones de SO	Alto
3	VZ-GD001	Correo electrónico en dispositivos móviles (Android, Apple)	Medio
4	VZ-BB001	Correo electrónico en dispositivos móviles (Blackberry)	Medio
5	VZ-SM001	Mensajería instantánea	Bajo
6	VZ-SA002	Sistema de gestión empresarial	*Fase de prueba*
7	VZ-SP002	Sistema de facturación	*Fase de prueba*
8	VZ-OR002	Sistema de contabilidad	*Fase de prueba*
9	VZ-VC001	VMware vCenter	*Por definir*

Tabla 4.4: Servidores implementados directamente en la plataforma virtual

4.4. Infraestructura virtual

Una vez identificados los servidores a ser virtualizados, el siguiente paso dentro de la planificación del proyecto es la de consolidar el diseño de la infraestructura virtual que albergará dichos sistemas. El diseño debe considerar los componentes más importantes de la infraestructura a fin de poder consolidar una estructura funcional y estable.

Con respecto a los sistemas anfitriones, la organización cuenta con cinco servidores blades dispuestos en la plataforma IBM BladeCenter S, expuesta en secciones anteriores de este documento. Este sistema está dispuesto en el centro de datos de la oficina principal de la organización. En la tabla 4.5 se exponen las características los servidores blades utilizados:

#	Modelo	Procesamiento	Memoria	Almacenamiento
1	BladeCenter HS22	Dos procesadores Xeon E5530 Quad Core de 2.53 GHz	28 GB de memoria RAM	1 disco duro de 146 GB, generación SAS 10K
2	BladeCenter HS22	Dos procesadores Xeon E5530 Quad Core de 2.53 GHz	28 GB de memoria RAM	1 disco duro de 146 GB, generación SAS 10K
3	BladeCenter HS22	Dos procesadores Xeon x5675 Six Core de 3.06 GHz	48 GB de memoria RAM	1 disco duro de 300 GB, generación SAS 10K
4	BladeCenter HS22	Dos procesadores Xeon x5675 Six Core de 3.06 GHz	48 GB de memoria RAM	1 disco duro de 300 GB, generación SAS 10K
5	BladeCenter HS22	Dos procesadores Xeon x5675 Six Core de 3.06 GHz	48 GB de memoria RAM	1 disco duro de 300 GB, generación SAS 10K

Tabla 4.5: Características de servidores blades usados

Es importante considerar las características de procesamiento, memoria y almacenamiento de los sistemas anfitriones ya que una de las bases de la virtualización es la compartición de recursos. Con respecto al almacenamiento compartido, la organización cuenta con diez unidades de discos duros generación SAS 15K de 600 GB cada uno, consolidando unos 5840,4 GB aproximados, dispuestos para almacenamiento SAN que puede ser usado por los mecanismos de respaldos y recuperación usados por la organización.

Finalmente, la distribución de los ambientes virtuales sobre los sistemas anfitriones dependerá de factores como su uso, recursos necesarios, niveles de criticidad y estado de los mismos. Una forma de poder gestionarlos de una manera distribuida es disponer de varios entornos operativos

basados en funcionalidad. De esta forma, la organización es capaz de distribuir las labores de gestión sobre una plataforma organizada que no desperdicio espacio ni recursos, garantizando el retorno de la inversión.

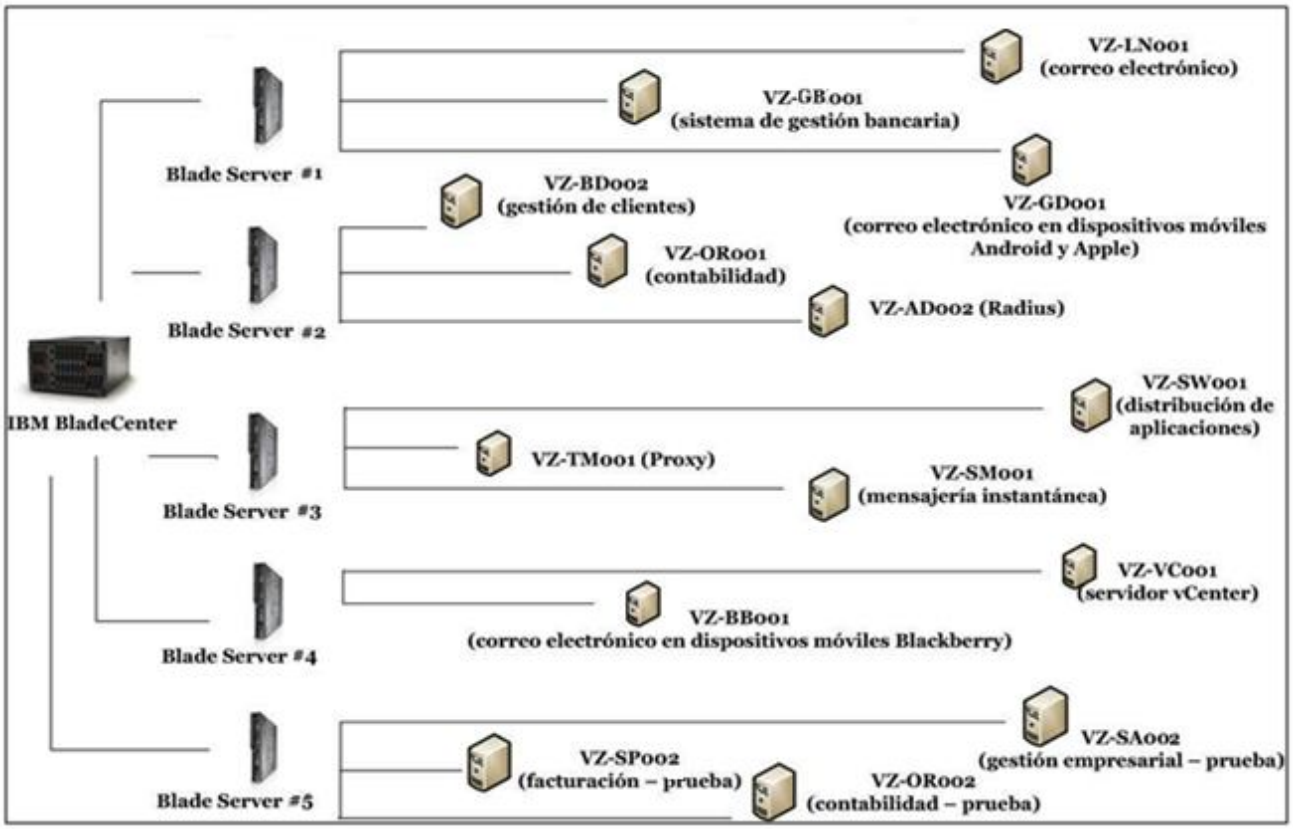

Figura 4.12: Distribución de servidores virtuales

En la figura 4.12 se muestra la distribución lógica de los servidores virtuales con respecto a los sistemas anfitriones. Dicha distribución corresponde a la propuesta ofrecida por el departamento de tecnologías de información de la organización, la cual estipula el establecimiento de tres entornos operativos: entorno de desarrollo, entorno de producción y entorno de pruebas.

El establecimiento de cada uno de dichos entornos se basa en las características físicas de los sistemas anfitriones, mientras que la disposición de los sistemas virtuales se hace de acuerdo a los planteamientos de sus respectivos administradores. A continuación, se presentan las especificaciones técnicas de cada uno de ellos.

4.4.1. Entorno de desarrollo

El entorno de desarrollo está conformado por dos de los servidores blades con menos recursos disponibles (identificados como “blade server #1” y “blade server #2”). Dicho entorno es dedicado a la disposición de sistemas que alojan aplicaciones que pueden o no, formar parte del uso diario del personal de la organización, que se encuentren en fase de desarrollo con respecto sus componentes y la funcionalidad de los mismos.

El primer componente del entorno de desarrollo es un servidor blade que cuenta con las siguientes características:

- 8 unidades de procesamiento Intel Xeon de 2.53 GHz, repartidas en 2 sockets de 4 núcleos cada uno.
- 16 procesadores lógicos configurados para permitir concurrencia (*hyperthreading*)
- 28 GB de memoria RAM compartida
- 131 GB de formato VMFS como unidad de almacenamiento local
- 3 unidades de almacenamiento SAN

Dicho servidor cuenta con 3 máquinas virtuales. Las características de las mismas se describen en la tabla 4.6, dispuesta a continuación:

Máquinas virtuales	Características
VZ-LN001 (servidor de correo electrónico)	**Sistema operativo:** Microsoft Windows Server 2008 R2 (64-bit) **Procesador:** 2 **Memoria:** 8 GB **Almacenamiento:** 1 unidad de almacenamiento SAN de 300 GB
VZ-GB001 (sistema de gestión bancaria)	**Sistema operativo:** Microsoft Windows Server 2003 (Enterprise) **Procesador:** 1 **Memoria:** 4 GB **Almacenamiento:** 2 unidades de almacenamiento SAN (100 GB para configuración y 260 GB para datos e información)
VZ-GD001 (servidor de correo en dispositivos móviles Android y Apple)	**Sistema operativo:** Microsoft Windows Server 2008 R2 (64-bit) **Procesador:** 2 **Memoria:** 4 GB **Almacenamiento:** 85 GB de almacenamiento local

Tabla 4.6: Primer componente del entorno de desarrollo

El segundo componente del entorno de desarrollo es un servidor blade que cuenta con las siguientes características:

- 8 unidades de procesamiento Intel Xeon de 2.53 GHz, repartidas en 2 sockets de 4 núcleos cada uno.
- 16 procesadores lógicos configurados para permitir concurrencia (*hyperthreading*)
- 28 GB de memoria RAM compartida
- 131 GB de formato VMFS como unidad de almacenamiento local
- 6 unidades de almacenamiento SAN

Dicho servidor cuenta con 3 máquinas virtuales. Las características de las mismas se describen en la tabla 4.7, dispuesta a continuación:

Máquinas virtuales	Características
VZ-BC001 (servidor de base de datos para gestión de clientes)	**Sistema operativo:** Microsoft Windows Server 2003 (Enterprise) **Procesador:** 2 **Memoria:** 6 GB **Almacenamiento:** 3 unidades de almacenamiento SAN (80 GB para configuración, 350 GB para datos e información y 265 GB para información de clientes anteriores)
VZ-OR001 (sistema de contabilidad)	**Sistema operativo:** Microsoft Windows Server 2003 (Enterprise) **Procesador:** 2 **Memoria:** 6 GB **Almacenamiento:** 2 unidades de almacenamiento SAN (90 GB para configuración y 250 GB para datos e información)
VZ-AD002 (Active Directory secundario y servidor Radius)	**Sistema operativo:** Microsoft Windows Server 2008 R2 (64-bit) **Procesador:** 1 **Memoria:** 4 GB **Almacenamiento:** 100 GB de almacenamiento local

Tabla 4.7: Segundo componente del entorno de desarrollo

4.4.2. Entorno de producción

El entorno de producción está conformado por dos de los tres servidores blades con más recursos disponibles (identificados como “blade server #3” y “blade server #4”). Dicho entorno es dedicado a la disposición de sistemas que alojan aplicaciones de uso diario que no se encuentren en estado de desarrollo o de pruebas.

El primer componente del entorno de producción es un servidor blade que cuenta con las siguientes características:

- 12 unidades de procesamiento Intel Xeon de 3.07 GHz, repartidas en 2 sockets de 6 núcleos cada uno.
- 24 procesadores lógicos configurados para permitir concurrencia (*hyperthreading*)
- 48 GB de memoria RAM compartida
- 275 GB de formato VMFS como unidad de almacenamiento local
- 1 unidad de almacenamiento SAN

Dicho servidor cuenta con 3 máquinas virtuales. Las características de las mismas se describen en la tabla 4.8, dispuesta a continuación:

Máquinas virtuales	Características
VZ-SW001 (servidor de actualización de aplicaciones y sistemas operativos)	**Sistema operativo:** Microsoft Windows Server 2008 R2 (64-bit) **Procesador:** 4 **Memoria:** 10 GB **Almacenamiento:** 1 unidad de almacenamiento SAN de 300 GB
VZ-TM001 (servidor Proxy)	**Sistema operativo:** Microsoft Windows Server 2008 R2 (64-bit) **Procesador:** 2 **Memoria:** 6 GB **Almacenamiento:** 110 GB de almacenamiento local
VZ-SM001 (servidor de mensajería instantánea)	**Sistema operativo:** Microsoft Windows Server 2008 R2 (64-bit) **Procesador:** 1 **Memoria:** 4 GB **Almacenamiento:** 20 GB de almacenamiento local

Tabla 4.8: Primer componente del entorno de producción

El segundo componente del entorno de producción es un servidor blade que cuenta con las siguientes características:

- 12 unidades de procesamiento Intel Xeon de 3.07 GHz, repartidas en 2 sockets de 6 núcleos cada uno.
- 24 procesadores lógicos configurados para permitir concurrencia (*hyperthreading*)
- 48 GB de memoria RAM compartida
- 275 GB de formato VMFS como unidad de almacenamiento local

Dicho servidor cuenta con 2 máquinas virtuales. Las características de las mismas se describen en la tabla 4.9, dispuesta a continuación:

Máquinas virtuales	Características
VZ-VC001 (servidor VMware vCenter)	**Sistema operativo:** Microsoft Windows Server 2008 R2 (64-bit) **Procesador:** 4 **Memoria:** 5 GB **Almacenamiento:** 70 GB de almacenamiento local
VZ-BB001 (servidor de correo en dispositivos móviles Blackberry)	**Sistema operativo:** Microsoft Windows Server 2008 R2 (64-bit) **Procesador:** 1 **Memoria:** 4 GB **Almacenamiento:** 90 GB de almacenamiento local

Tabla 4.9: Segundo componente del entorno de producción

4.4.3. Entorno de pruebas

El entorno de prueba está conformado por un único servidor blade (identificado como “blade server #5”), el cual es usado para alojar aquellos sistemas en fase de pruebas y que sus funcionalidades no son estrictamente requeridas por las actividades diarias de la organización. Una vez que los sistemas superen la fase de pruebas, deben ser migrados al entorno de desarrollo o producción, dependiendo del caso.

El único componente del entorno de pruebas es un servidor blade que cuenta con las siguientes características:

- 12 unidades de procesamiento Intel Xeon de 3.07 GHz, repartidas en 2 sockets de 6 núcleos cada uno.
- 24 procesadores lógicos configurados para permitir concurrencia (*hyperthreading*)
- 48 GB de memoria RAM compartida
- 275 GB de formato VMFS como unidad de almacenamiento local
- 3 unidades de almacenamiento SAN

Dicho servidor cuenta con 3 máquinas virtuales. Las características de las mismas se describen en la tabla 4.10, dispuesta a continuación:

Máquinas virtuales	Características
VZ-SA002 (sistema de gestión empresarial en fase de prueba)	**Sistema operativo:** Microsoft Windows Server 2008 R2 (64-bit) **Procesador:** 4 **Memoria:** 8 GB **Almacenamiento:** 90 GB de almacenamiento local y una unidad de almacenamiento SAN de 365 GB
VZ-SP002 (sistema de facturación en fase de prueba)	**Sistema operativo:** Microsoft Windows Server 2008 R2 (64-bit) **Procesador:** 1 **Memoria:** 6 GB **Almacenamiento:** 90 GB de almacenamiento local y una unidad de almacenamiento SAN de 345 GB
VZ-OR002 (sistema de contabilidad en fase de prueba)	**Sistema operativo:** Microsoft Windows Server 2003 (Enterprise) **Procesador:** 1 **Memoria:** 6 GB **Almacenamiento:** 90 GB de almacenamiento local y una unidad de almacenamiento SAN de 200 GB

Tabla 4.10: Entorno de pruebas

Finalmente, una vez especificadas las características de cada uno de los servidores virtuales, la fase de planificación del proyecto culmina para dar inicio a la fase de instalación y configuración de los sistemas que sostendrán la infraestructura virtual. Las primeras instalaciones corresponden a las de los sistemas operativos de los sistemas anfitriones.

4.5. Instalación del programa de control

ESXi es el sistema operativo hypervisor de tipo 1 ó bare-metal diseñado por VMware y adoptado por la organización para alojar y gestionar las máquinas virtuales en los diferentes sistemas anfitriones. Tiene la particularidad de no instalarse sobre un sistema operativo de propósito general, sino que es embebido en el hardware del computador en donde es instalado. En este caso, ESXi es instalado en cada uno de los servidores blades de la plataforma IBM BladeCenter.

Antes de dar inicio a la instalación de un sistema operativo de control de virtualizaciones, se requiere conocer los requerimientos de hardware del mismo para poder garantizar su correcto funcionamiento. En particular, la versión más reciente de VMware ESXi requiere que el hardware del host cumpla con los siguientes requerimientos principales [33]:

- Procesador de 64 bits con al menos dos núcleos.
- Mínimo de 2GB de memoria RAM
- Uno ó más controladores Ethernet de 1 Gbps a 10 Gbps
- Adaptadores SCSI, de canal de fibra ó controladores RAID
- Discos locales SATA, discos SCSI ó discos RAID para instalación y almacenamiento de máquinas virtuales

Otro de los aspectos importantes en la instalación, es el control sobre el hardware por parte del usuario que lleve a cabo este proceso. Normalmente, las plataformas diseñadas para alojar servidores cuentan con módulos de interacción con el usuario que permiten desplegar interfaces graficas, tales como conmutadores KVM.

La plataforma IBM BladeCenter no es la excepción, ya que cuenta con un módulo KVM que permite controlar los servidores blades que aloja, por lo que es la primera opción a usar para realizar las instalaciones de los sistemas operativos.

Por lo general, las plataformas físicas ofrecen aplicaciones los bastante útiles para llevar a cabo tareas de gestión sencillas. Tal es el caso del módulo de gestión avanzada de IBM, una interfaz web que le permite al usuario consultar el estado de los componentes físicos del blade, así como ofrecer acceso remoto a los sistemas operativos instalados en cada uno de los servidores blades.

En la figura 4.13 se muestra una de las pantallas del módulo de gestión avanzada de IBM.

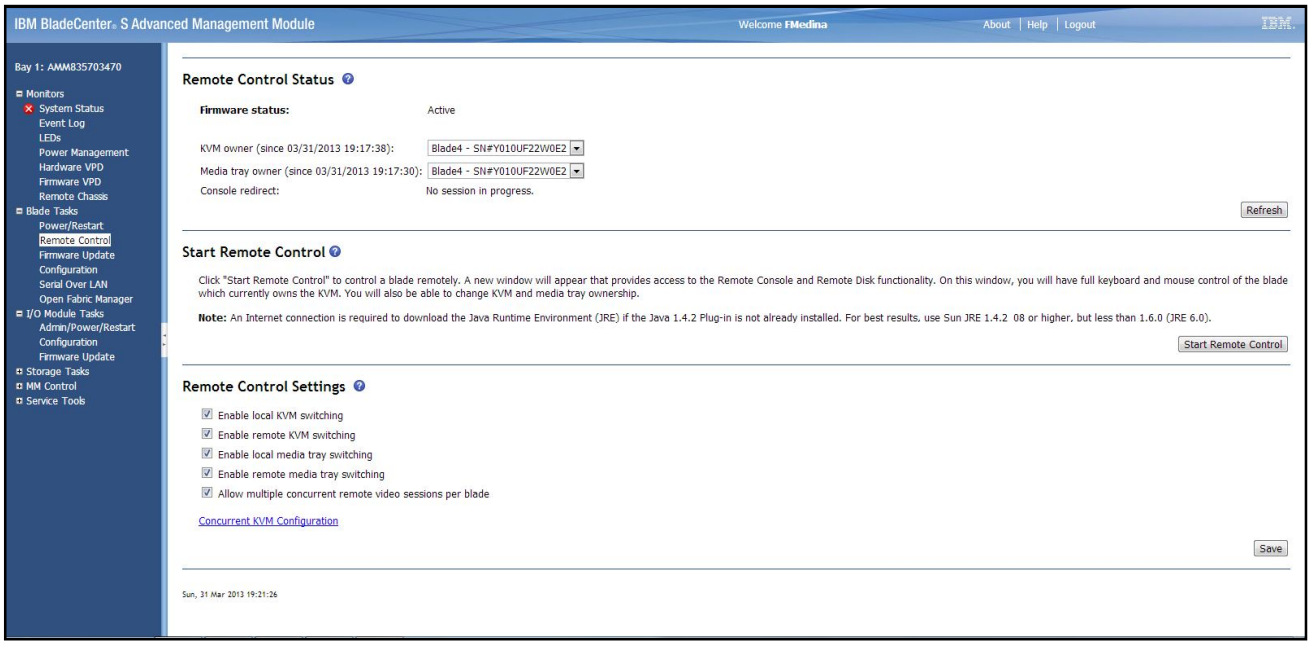

Figura 4.13: Módulo de gestión avanzada de IBM

Es importante destacar que antes de dar inicio a la instalación, debe asegurarse de que las herramientas seleccionadas para la interacción con los sistemas anfitriones sean compatibles en términos de idioma y teclado con las opciones disponibles en el menú de arranque.

Los archivos de instalación del sistema ESXi se descargan del sitio web oficial de VMware, el cual ofrece una imagen ISO que puede ser dispuesta en un CD, DVD o unidad flash de arranque, que debe ser conectada al sistema anfitrión (en este caso, servidor blade) y reiniciarlo. Este procedimiento dará inicio al menú de arranque. En la figura 4.14 se muestran las opciones del menú de arranque de ESXi.

Figura 4.14: Menú de arranque de VMware ESXi

Al seleccionar la opción de instalación, el programa procede a cargar una serie de archivos necesarios para la instalación del sistema operativo. Una vez cargados los componentes, el proceso muestra un mensaje de bienvenida y solicita al usuario la tarea a ejecutar. Las opciones dispuestas son: instalar, reparar ó cancelar. En la figura 4.15 se muestra el mensaje de bienvenida correspondiente a la instalación de ESXi versión 4.1.0.

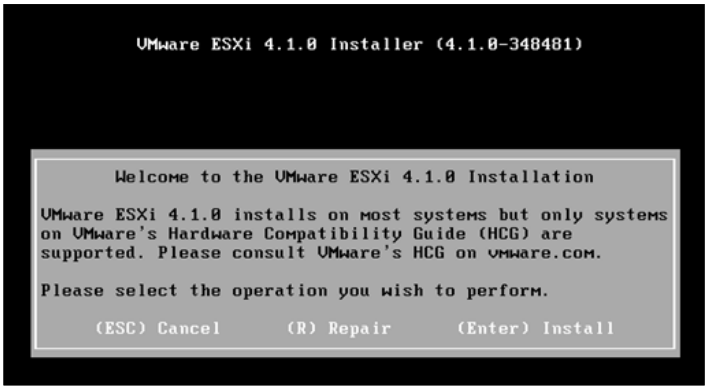

Figura 4.15: Mensaje de bienvenida

Luego de aceptar los acuerdos de licencia correspondientes, el proceso de instalación lleva a cabo una detección de discos y unidades de almacenamiento disponibles, detectando tanto los discos locales (disco duro del servidor blade) como los volúmenes remotos de almacenamiento disponibles a través del módulo de conectividad SAN y el módulo controlador SAS RAID del sistema IBM BladeCenter.

El proceso de detección de discos no sólo informa acerca de la localidad de las unidades de almacenamientos (locales ó remotas), sino que también ofrece información particular de cada unidad tal y como: modelo y vendedor, identificador del disco, identificador lógico LUN (si se trata de un volumen remoto), capacidad y ruta asignada por el sistema de archivos de ESXi. En la figura 4.16 se muestra la información de una unidad de disco local.

Figura 4.16: Información de disco

Luego de seleccionar la unidad de almacenamiento en donde el sistema operativo será instalado, el proceso informa al usuario que se encuentra listo para dar formato a todo el contenido de la partición seleccionada, eliminando todo rastro de información presente y consolidando un sistema de archivos propio de VMware. Una vez confirmado, el proceso de instalación da comienzo, teniendo una duración proporcional al tamaño del disco seleccionado. Al terminar la instalación, el proceso muestra un mensaje que indica la culminación de la misma, solicitando al usuario reiniciar el servidor, retirando el CD de instalación.

ESXi es un sistema operativo bastante ligero que no requiere de una interfaz gráfica para iniciar sus componentes e interactuar con el usuario. Al iniciar el servidor, se carga una pantalla inicial que

lista todos los componentes que son cargados durante el arranque del mismo. Cuando finalmente es encendido, se muestra una única pantalla que indica un resumen de las características físicas del mismo.

En la figura 4.17 se muestra la información que un sistema operativo ESXi 4.1.0 ofrece en relación a un servidor blade en donde es instalado.

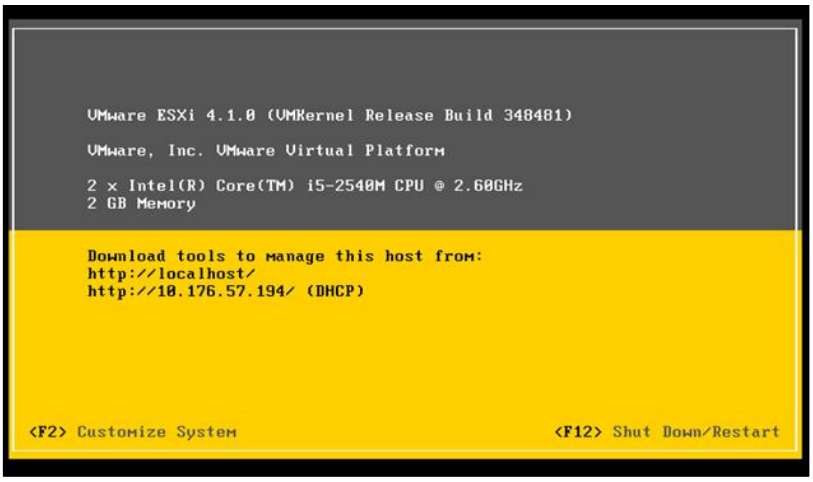

Figura 4.17: Información de servidor

4.5.1. Actualización del programa de control

Unos de las tareas más comunes es la de actualizar los sistemas de gestión, por lo que debe ser considerada como parte importante del mantenimiento de los sistemas. Particularmente, existen varias versiones de ESXi disponibles, siendo la versión 5.1 la más reciente hasta ahora. El proceso de actualización de una versión anterior a una más reciente es una tarea muy común que no requiere de un proceso de instalación como el descrito anteriormente. Sin embargo, el proceso de migración es bastante similar al proceso de instalación. De hecho, requiere que, nuevamente, el servidor arranque desde el CD de instalación de la versión de ESXi a la que se desea actualizar, cediendo el control del mismo a través del módulo de gestión avanzada del IBM BladeCenter.

El proceso de migración no afecta el funcionamiento de las máquinas virtuales alojadas en el servidor. Sin embargo, estas deben ser apagadas durante el transcurso del mismo, ya que el servidor se encontrará fuera de servicio.

Al iniciar el proceso, se cargan un conjunto de componentes y servicios necesarios para la migración. Luego de aceptar los mensajes de bienvenida y los acuerdos de licencia, se lleva a cabo una detección de discos. Al momento de seleccionar la unidad que aloja la versión de ESXi descontinuada, el proceso detecta la presencia de una versión de ESXi y presenta 3 opciones:

- Forzar la migración de ESXi, preservando los archivos VMFS
- Instalar ESXi, preservando los archivos VMFS
- Instalar ESXi, sobrescribiendo los archivos VMFS

En la figura 4.18 se muestra el mensaje de información al usuario al detectar una versión de ESXi instalada.

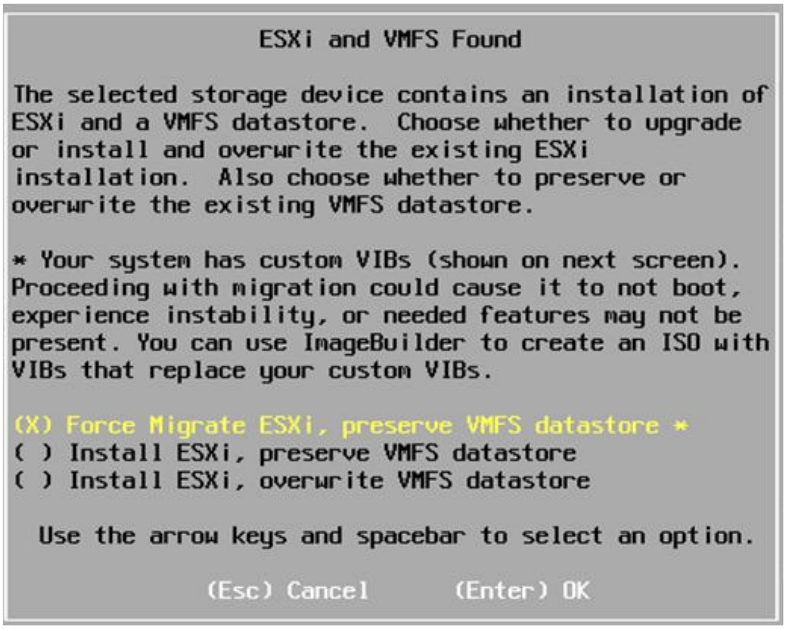

Figura 4.18: Migración de ESXi

VMFS son las siglas de Virtual Machine File System, el sistema de archivos de VMware usado por ESXi y que está diseñado para almacenar las imágenes de las máquinas virtuales, así como los archivos de instalación propios de ESXi. Para migrar el sistema operativo ESXi, preservando el estado de las máquinas virtuales alojadas, se debe seleccionar la primera opción.

Dependiendo de la instancia de ESXi que se desee actualizar, el proceso muestra un mensaje de advertencia, como el de la figura 4.19, señalando que hay archivos VIB contenidos en el sistema operativo que no tendrán sustituto una vez realizada la actualización.

Figura 4.19: Advertencia de archivos VIB

Un archivo VIB es un conjunto de controladores que usa el sistema, conforme a los dispositivos presente en el hardware [34]. Es importante determinar si los archivos VIB señalados en la advertencia son innecesarios ó si existe una forma de sustituirlos una vez que la actualización se realice.

Al confirmar la acción, el proceso de actualización da inicio, teniendo una duración proporcional al tamaño de la partición seleccionada. Al finalizar, el proceso indica la culminación exitosa de la migración, solicitando reiniciar el servidor, retirando el CD de instalación.

Otra de las tareas más comunes es la de aplicar parches de seguridad en los sistemas operativos, un proceso que solventa muchas de las vulnerabilidades encontradas durante su exposición al mercado. Existen muchas maneras de aplicar dichos parches, por ejemplo, se puede hacer uso de una herramienta que se encargue de adquirirlos e instalarlos de manera automática. Particularmente, ESXi permite aplicar parches de seguridad con interacción directa sobre su sistema de archivos.

El proceso consiste en adquirir acceso remoto a la consola del servidor ESXi, proceso que puede lograrse a través del establecimiento de una conexión SSH con credenciales administrativas. Los parches de seguridad pueden descargarse de la página oficial de VMware, la cual dispone las versiones más recientes de los mismos y se encarga de actualizarlos periódicamente. El primer requisito es que estos parches sean descargados vía web y dispuestos dentro de un directorio del sistema de archivos, de manera que puedan ser usados por la consola de servicios.

Como se trata de un proceso que involucra la modificación del sistema operativo, se recomienda que el servidor mantenga un tiempo de indisponibilidad para atender a peticiones de usuarios, por lo que el segundo requisito es que las máquinas virtuales seas apagadas durante el transcurso del mismo.

Una vez obtenido el acceso a la consola, la aplicación de los parches de seguridad se limita a la ejecución de líneas de códigos que difieren entre una versión y otra. En el código 4.1 se exponen las diferencias conforme a la versión del sistema operativo.

```
#Aplicación de parches de seguridad en sistemas VMware ESXi 4.1
        esxupdate --bundle=<ubicación_del_parche_de_seguridad>.zip update

#Aplicación de parches de seguridad en sistemas VMware ESXi 5.0 y 5.1
        esxcli software vib install --depot=<ubicación_del_parche_de_seguridad>.zip
```

Código 4.1: Aplicación de parches de seguridad en sistemas ESXi

La ejecución de la línea de código debe hacerse por cada parche descargado, mientras que el proceso de actualización tarda unos minutos aproximadamente. Una vez aplicadas las actualizaciones, el servidor debe reiniciarse, proceso que no afecta la disposición de máquinas virtuales, las cuales deben encenderse nuevamente, reanudando los servicios ofrecidos en la organización.

4.6. Gestión de host y máquinas virtuales

Una vez instalados los sistemas operativos en los anfitriones, se requieren de herramientas que permitan la creación de máquinas virtuales. En particular, ESXi es un sistema simple que sólo está orientado a alojar instancias virtuales, no dispone de herramientas de gestión, salvo una consola de servicios. Sin embargo, VMware dispone de una variedad de herramientas para la gestión de sistemas operativos ESXi, así como de las máquinas virtuales que puede alojar.

Se trata de la suite VMware vSphere, un conjunto de aplicaciones que pueden ser instaladas tanto en servidores como estaciones de trabajo, diseñadas para ejecutar diferentes tareas de gestión de sistemas virtuales [38]. La herramienta más usada es el cliente vSphere, el cual puede ser descargado directamente de la página oficial de VMware. Esta herramienta permite gestionar hosts ESXi, máquinas virtuales y, opcionalmente, la central vCenter Server.

Puede ser instalado en ambientes Windows ó Linux que se encuentren en la misma red en la que el servidor ESXi esté dispuesto. El proceso de instalación es bastante sencillo, siendo instalado en el directorio *C:\Program Files\VMware\Infrastructure* en ambientes Windows de 32 bits y en *C:\Program Files (x86)\VMware\Infrastructure* en ambientes Windows de 64 bits. La aplicación requiere que la estación de trabajo en donde será instalada tenga instalada el componente Microsoft .NET Framework 3.5 SP1 para su correcto funcionamiento [39]. Una vez instalada la aplicación, se puede realizar una conexión vía SSL con el servidor ESXi. Sólo basta conocer su dirección IP y las credenciales de acceso al mismo. Por defecto, ESXi está configurado con el usuario "root" sin contraseña. La misma debe ser configurada por el usuario en el menú de configuración de ESXi.

En la figura 4.20 se muestra la vista inicial del cliente vSphere antes, solicitando la información de acceso al servidor ESXi.

Figura 4.20: Inicio de sesión en VMware vSphere Client

Al ingresar al cliente vSphere, se muestra una interfaz de usuario con el resumen de los estados de cada uno de los componentes físicos del host, así como el de las máquinas virtuales alojadas. El cliente ofrece una gran variedad de opciones dedicadas a la gestión de recursos y mejoramiento en el rendimiento de los sistemas. En la figura 4.21 se muestra la vista principal del cliente VMware vSphere.

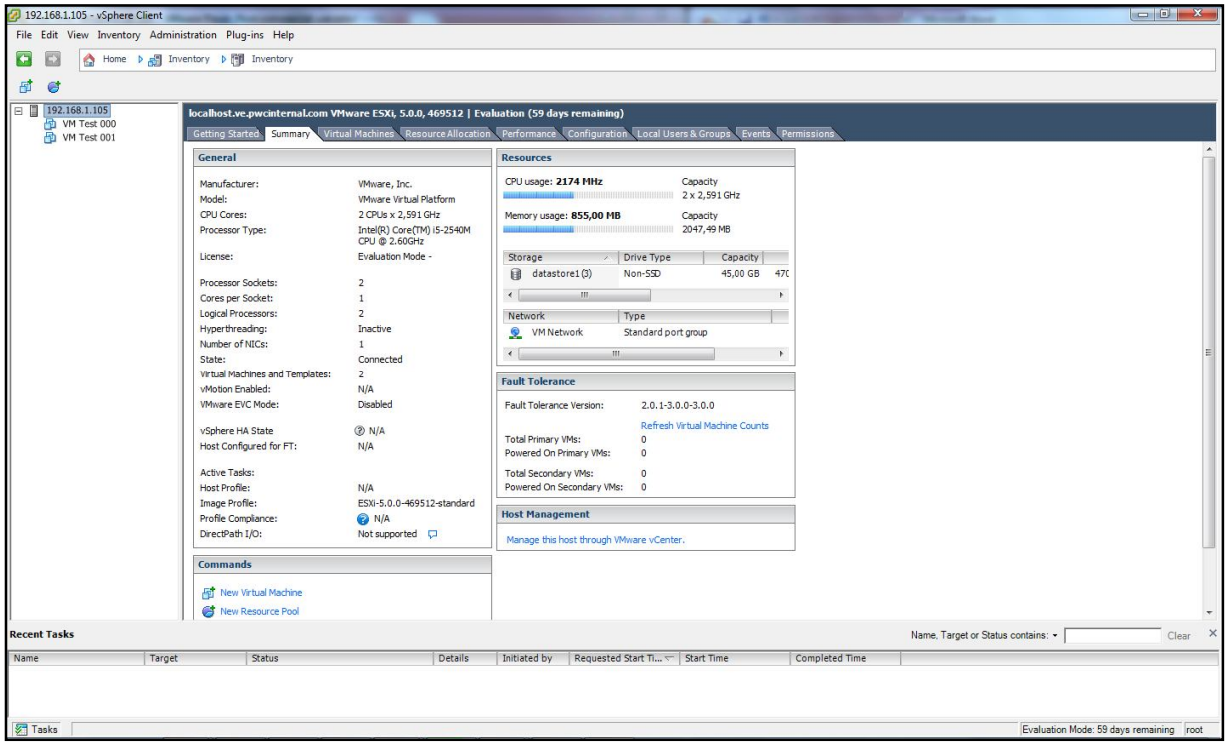

Figura 4.21: VMware vSphere Client

Otra de las herramientas de gestión es la interfaz de línea de comandos, la cual permite gestionar y configurar máquinas virtuales. Es una interfaz potente y fácil de usar, ya que está basada en la tecnología de PowerShell de Microsoft. Con esta interfaz se pueden gestionar hosts ESXi a través de scripts, realizando las mismas tareas que se realizan con el cliente VMware vSphere.

PowerCLI es generalmente instalada en una estación de trabajo Windows por los administradores de las instancias vSphere. Al ser instalada, PowerCLI tiene acceso al API de vSphere de la misma manera en como el cliente vSphere lo hace a través de puertos y credenciales de acceso. Para poder ser instalada, la aplicación requiere de Windows .NET Framework y Windows PowerShell. Particularmente, Windows PowerShell V2 está integrada en los sistemas operativos Windows 7 y Windows 2008 R2.

Antes de instalar la aplicación, PowerShell debe estar configurada para habilitar la ejecución de scripts. Esto se hace a través de la habilitación de la “política de ejecución” de PowerShell (Execution Policy). Para ello, se debe ejecutar Windows PowerShell (sesiones de 32 y 64 bits, respectivamente) con permisos administrativos y ejecutar el comando: *Set-ExecutionPolicy RemoteSigned*.

Luego de cumplir con este requerimiento, se procede a instalar la aplicación VMware vSphere PowerCLI. El archivo de instalación pude obtenerse de manera gratuita a través del sitio oficial de VMware. Una vez descargado, se da inicio al proceso de instalación, el cual es un proceso bastante sencillo. Una vez completado el proceso de instalación, la aplicación estará disponible para su ejecución. La gestión de los hosts ESXi y de máquinas virtuales se hace a través de una línea de comando y mediante la ejecución de scripts en consola [40]. La figura 4.22 muestra la vista principal de VMware vSphere PowerCLI

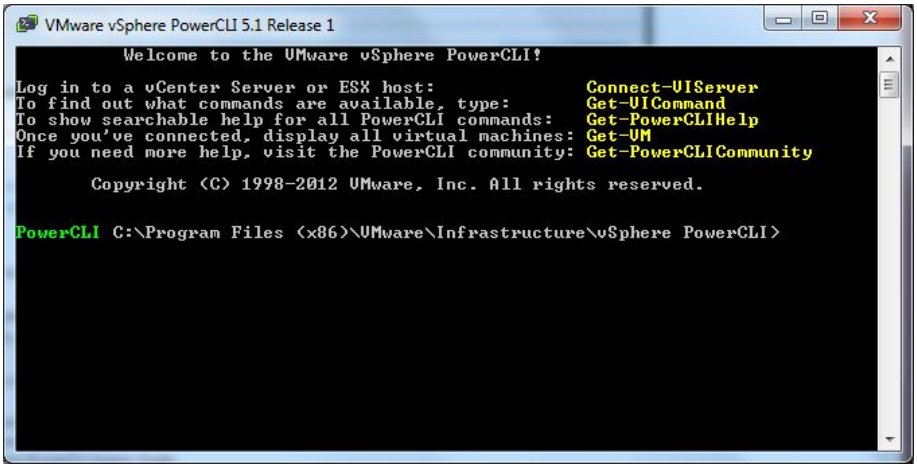

Figura 4.22: VMware vSphere PowerCLI

Finalmente, la última herramienta de gestión que provee la suite vSphere es la instancia de VMware vCenter Server, una aplicación orquestadora de servicios de gestión centralizada de hosts ESXi y de sus máquinas virtuales. Para gestionar un host ESXi con vCenter Server se necesita una licencia de VMware vCenter Agent, incluida en todas las ediciones licenciadas de vSphere.

VMware vCenter Server es la herramienta de gestión principal de la suite VMware vSphere. Su objetivo es mejorar la continuidad de negocio y maximizar la eficiencia en las operaciones, con funciones como: migración de máquinas virtuales en ejecución, balanceo de carga automático, protección frente a fallas de hardware, restauración y respaldo de máquinas virtuales, entre otras.

Para realizar la instalación e implementación de las herramientas principales de vSphere, se requiere de un servidor dedicado Windows Server 2008 R2 (puede ser una máquina virtual alojada en un host ESXi) que cumpla con las siguientes características principales [35]:

- Dos procesadores de 64 bits con dos núcleos
- Al menos 4 GB de memoria RAM
- Al menos 4 GB de almacenamiento en disco
- Microsoft SQL Server 2008 R2
- Conexión de 1 Gbps (Recomendado)

Dentro de la gestión de usuarios y grupos del servidor Windows, se requiere crear un usuario particular para la gestión de las herramientas de vSphere. Este usuario debe ser designado como propietario de las bases de datos que usarán dichas herramientas.

El primer paso es crear una base de datos para la instancia principal de VMware vSphere, es decir, vCenter Server. Para ello, se inicia sesión en SQL Server Management Studio y se crea dicha base de datos.

Luego de crear la base de datos de vCenter Server, se procede a crear una conexión ODBC para que la aplicación pueda acceder a dicha base de datos. Para ello se ejecuta la herramienta de Windows Server: Data Source (ODBC). La base de datos por defecto debe ser la base de datos de vCenter Server y las credenciales para la autenticación SQL deben ser iguales a las del usuario propietario de la misma.

Particularmente, vSphere provee de un mecanismo de autenticación SSO (Single Sign On), es decir, permite acceder a sus aplicaciones usando las mismas credenciales usadas al iniciar una sesión en el servidor Windows. Para asegurar el funcionamiento de esta mecanismo, se requiere crear una base de datos para SSO, usando un script SQL genérico llamado:

rsaIMSLiteMSSQLSetupTablespaces, el cual se encuentra ubicado en el CD de instalación de la suite vSphere, en el directorio: *Single Sign On\DBScripts\SSOServer\schema\mssql*.

Este script requiere de una serie de modificaciones para que se ajuste a la configuración del servidor. Dichas modificaciones se hacen en la ruta de acceso de los archivos que requiere la base de datos a crear, de manera que cada una de las rutas estén configuradas en *C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA*, tal y como se muestran en el código 4.2.

```
-- PROJECT     IMS
-- MODEL       IDENTITY MANAGEMENT SERVICE
-- COMPANY     RSA, the Security Division of EMC
-- DATABASE    MSSQL

USE MASTER
GO
------------------------------------------------------------------------------
CREATE DATABASE RSA ON PRIMARY(
   NAME='RSA_DATA',
   FILENAME='C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA\RSA_DATA.mdf',
   SIZE=10MB,
   MAXSIZE=UNLIMITED,
   FILEGROWTH=10%),
FILEGROUP RSA_INDEX(
   NAME='RSA_INDEX',
   FILENAME='C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA\RSA_INDEX.ndf',
   SIZE=10MB,
   MAXSIZE=UNLIMITED,
   FILEGROWTH=10%)
LOG ON(
   NAME='translog',
   FILENAME='C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA\translog.ldf',
   SIZE=10MB,
   MAXSIZE=UNLIMITED,
   FILEGROWTH=10% )
GO

-- Set recommended perform settings on the database
EXEC SP_DBOPTION 'RSA', 'autoshrink', true
GO
EXEC SP_DBOPTION 'RSA', 'trunc. log on chkpt.', true
GO

CHECKPOINT
GO

------------------------------------------------------------------------------
-- To drop the database, the commands is:
------------------------------------------------------------------------------
-- DROP DATABASE RSA
```

Código 4.2: Script SQL para generar la base de datos de vCenter Server

Al compilar y ejecutar el script anterior en SQL Management Studio, se crea una base de datos llamada RSA, la cual será usada para las funciones de SSO. Adicionalmente, esta base de datos requiere de una configuración de dos cuentas de usuario para el acceso de los servicios de vSphere. Estas cuentas de usuario deben tener permisos de propietario sobre la base de datos.

Al haber completado los pasos previos descritos anteriormente, se procede a instalar por separado, cada uno de los componentes de VMware vSphere [36]. Los cuales son los siguientes:

- VMware vCenter Single Sign On
- VMware vCenter Inventory Service
- VMware vCenter Server
- VMware vSphere Client
- VMware vSphere Web Client

La instalación de Single Sign On se basa en la creación de un nodo primario que se comunicará con la base de datos previamente creada. La conexión se hace a través del puerto 1433 y con las dos credenciales propietarias de dicha base de datos.

Por su parte, Inventory Service es una herramienta que permite gestionar los objetos en el inventario del cliente web de vSphere y atiende cada una de las consultas del usuario con respecto al estado de los componentes de vSphere.

La instalación de todos los componentes de vSphere se basa en la definición de puertos para el acceso a través de la red, definición de direcciones URL y rutas de instalación. En resumen, el proceso de instalación es rápido y sencillo. Al finalizar, el operador de red será capaz de iniciar sesión en el cliente web vSphere y visualizar el estado de cada uno de los sistemas anfitriones ESXi, así como las máquinas virtuales alojadas y unidades de almacenamiento usadas.

4.7. Centro de datos virtual

Las ventajas de instalar un orquestador de servicios es la de centralizar toda la gestión de los ambientes virtuales una única instancia. En el caso particular de vCenter, es un sistema de inventariado que agrupa centros de datos, hosts, clústeres, redes, almacenamiento y máquinas virtuales.

Una de las primeras actividades luego de instalar el programa orquestador es definir un centro de datos virtual. Esta estructura lógica será el contenedor primario de todos los objetos inventariados, principalmente hosts y máquinas virtuales. Se pueden crear tantos centros de datos como lo requiera una organización, generalmente, su disposición dependerá de las unidades de negocio presentes. En la figura 4.23 se describen los componentes de un centro de datos.

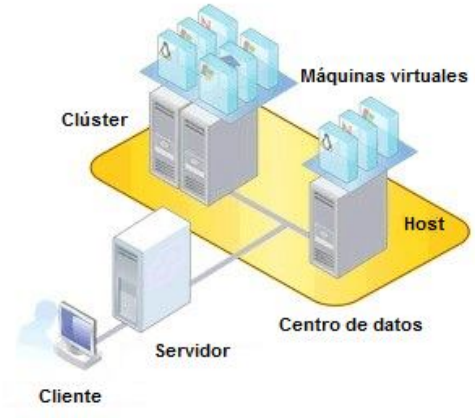

Figura 4.23: Centro de datos virtual

Uno de los componentes principales del centro de datos son los clústeres. Un clúster es un grupo de hosts. Cuando un host es incluido en un clúster, sus recursos forman un conjunto compartido entre los demás miembros del mismo. Es así como deben definirse 3 clústeres dentro

del centro de datos virtual del proyecto: entorno de producción, entorno de desarrollo y entorno de pruebas. Finalmente, el siguiente paso es incluir los hosts en sus respectivos clústeres.

4.7.1. Máquinas virtuales

Una vez que los hosts son agrupados, el siguiente paso es crear las respectivas máquinas virtuales. Esta tarea puede ser ejecutada tanto a nivel de servidor como a nivel de cliente, dependiendo de la tecnología usada.

La creación de máquinas virtuales es un proceso sencillo, estandarizado por la mayoría de las tecnologías del mercado en términos de sus requerimientos. Fundamentalmente, lo que se necesita para cumplir con esta tarea es contar con los archivos de instalación del sistema operativo que se desee virtualizar y una herramienta que permita configurarla de acuerdo a:

- Procesadores
- Memoria
- Controladores
- Disco duro
- Adaptadores de red
- Dispositivos de E/S

En términos generales, el proceso de creación de una máquina virtual es similar al proceso de creación de un archivo de configuración ó plantilla, de ahí su capacidad de ser portable. Particularmente, las máquinas virtuales de VMware son archivos de tipo VMDK [41] que conviven en el sistema de archivos de ESXi y pueden ser trasladadas a otros ambientes, sin importar su origen. De hecho, una práctica muy común es que las organizaciones dispongan de máquinas virtuales con sistema operativos pre-configurados con una serie de parámetros que pueden ser usados más de una vez al momento de requerir implementar nuevos servidores virtuales. Esto permite ahorrar tiempo en configuraciones repetitivas y se aprovecha la portabilidad que otorga el usar máquinas virtuales como plantillas.

Si por el contrario, se desea migrar un entorno físico a un entorno virtual, la situación no es tan sencilla en términos de ahorro de tiempo [44]. Por lo general, una aplicación consolidada en un entorno físico presenta configuraciones que deben ser reproducidas en una máquina virtual, lo cual requiere tiempo en el cual el servidor original debe permanecer inactivo mientras se verifica el funcionamiento de su correspondiente versión virtual.

Este proceso debe llevarse a cabo con la colaboración de los responsables de las aplicaciones, ya que pueden ofrecer información de soporte que ayude en las labores de re-instalación y re-configuración. Muchas aplicaciones que son dispuestas en servidores ofrecen capacidades de respaldo en sus configuraciones, lo que puede facilitar el proceso. De acuerdo a las mejores prácticas, la organización debe contar con documentación de soporte y gestión de conocimiento que permita realizar estas labores en el menor tiempo posible [45], esto facilitará la gestión de los sistemas y hará que los mismos sean más receptivos al cambio.

Adicionalmente, las soluciones para virtualizar también pueden ofrecer funcionalidades para atender este tipo de requerimientos. En el caso de VMware se cuenta con VMware Converter [42], una aplicación que reproduce el estado del disco duro en donde es instalada, realizando una copia exacta de su configuración y contenido en un archivo único con formato VMDK, es decir, una máquina virtual portable. La desventaja de este tipo de soluciones radica en que el disco no debe ser sometido a cambios durante el proceso de conversión, por lo que el servidor debe mantenerse fuera de línea por varias horas.

4.7.2. Unidades de almacenamiento

Como en toda infraestructura de servidores, el almacenamiento juega un papel crucial, ya que los mismos están sujetos a las capacidades que el centro de datos pueda proveer. En el caso de la virtualización de servidores, el paradigma sólo varía en términos de ubicación. Normalmente, en una infraestructura organizacional, el almacenamiento viene dado por dos componentes: los discos locales y el almacenamiento en red. Para el caso de estudio de este proyecto, el almacenamiento local de los hosts es provisto por los discos duro de los servidores blades, mientras que el almacenamiento compartido viene dado por una red SAN [43] conformada por 12 unidades agrupadas en el sistema BladeCenter. Lo importante a considerar es que el programa de control situado en cada host, debe hacer uso de los recursos del mismo, por lo que debe ser instalado en el disco local.

La particularidad de ESXi como programa de control es que usa VMFS, un sistema de archivos propio de VMware que ofrece muchas ventajas como:

- Almacena máquinas virtuales como imágenes de disco
- Permite almacenar clones de máquinas virtuales
- Múltiples máquinas virtuales pueden acceder al sistema de archivos simultáneamente
- Los volúmenes pueden expandirse lógicamente, agrupando varias unidades

Muchas de estas ventajas pueden aprovecharse en la gestión del espacio de almacenamiento con respecto a la disposición de máquinas virtuales, desde que las unidades de la red SAN también pueden ser formateadas con este sistema de archivos ó al menor las particiones requeridas. Es decir, se pueden sostener máquinas virtuales en ejecución almacenadas tanto en discos locales como en almacenamiento compartido.

Este paradigma permite realizar tareas como migraciones de máquinas virtuales entre hosts y clonaciones. Solo basta con designar unidades compartidas entre hosts y con el sistema de archivos VMFS en común, actividad que puede ejecutarse a través de los clientes de gestión respectivos.

Finalmente, la organización deberá determinar si las máquinas virtuales se almacenarán de manera local ó compartida durante su ejecución, en función de sus requerimientos y almacenamiento disponible. En la tabla 4.11 se muestra la distribución de máquinas virtuales aplicada en el proyecto.

Servidor	Aplicaciones / Servicios	Local	Compartido
VZ-LN001	Correo electrónico		**X**
VZ-BC001	Sistema de gestión de clientes		**X**
VZ-OR001	Sistema de contabilidad		**X**
VZ-GB001	Sistema de gestión bancaria		**X**
VZ-TM001	Proxy (Políticas de acceso a Internet)		**X**
VZ-SW001	Distribución de aplicaciones y actualizaciones de SO		**X**
VZ-AD002	Active Directory Secundario y servidor Radius		**X**
VZ-GD001	Correo electrónico en dispositivos móviles (Android, Apple)	**X**	
VZ-BB001	Correo electrónico en dispositivos móviles (Blackberry)	**X**	
VZ-SM001	Mensajería instantánea	**X**	
VZ-SA002	Sistema de gestión empresarial	**X**	
VZ-SP002	Sistema de facturación	**X**	
VZ-OR002	Sistema de contabilidad	**X**	
VZ-VC001	VMware vCenter	**X**	

Tabla 4.11: Almacenamiento de máquinas virtuales por servidor

4.7.3. Red virtual

A pesar de que la virtualización es una tecnología principalmente enfocada en la compartición de recursos, no excluye en su totalidad los parámetros y configuraciones de red implícitos en el proceso de migración. De hecho, muchas tecnologías de virtualización proponen nuevos esquemas de red que pueden ser aprovechados tanto por los sistemas anfitriones como por las máquinas virtuales. Entre los servicios más comunes se encuentran:

- Conectividad entre máquinas virtuales dispuestas en único host
- Conectividad de máquinas virtuales en la red física
- Conectividad de servicios propios de la tecnología de virtualización adoptada en la red física

La conexión de los sistemas anfitriones con la red física es el primer paso a consolidar. Esta debe hacerse de acuerdo a los procedimientos establecidos por la plataforma física adoptada y de acuerdo al direccionamiento usado. Particularmente, el sistema ESXi permite configurar los parámetros de red a través de su interfaz de usuario principal.

Una vez que un host es conectado, las máquinas virtuales alojadas pueden comunicarse entre sí a través de un conmutador virtual dispuesto por el sistema operativo, el cual provee de los mismos protocolos usados en los conmutadores físicos tradicionales. Así mismo, podrán conectarse con la red física y demás sistemas presentes.

5. Análisis de Resultados

La implementación de la virtualización sugiere la adopción de nuevos modelos de gestión. Por lo que la evaluación de los resultados obtenidos permite a una organización determinar si esta tecnología cumple con los requerimientos establecidos en las primeras fases del proyecto. En este capítulo se exponen los resultados obtenidos en la virtualización de los servidores descritos anteriormente.

5.1.1. Respecto a ambientes virtualizados

Como se estableció anteriormente, se determinaron una serie de servidores candidatos a ser virtualizados. La virtualización de estos servidores permitió redefinir su aprovisionamiento de recursos en función de sus demandas diarias.

El servidor de correo electrónico VZ-LN001 pasó de estar alojado en un sistema operativo Windows Server 2003 a la versión Windows Server 2008 R2. Tiene dos procesadores en lugar de uno, así como una memoria RAM de 8GB en lugar de una de 2GB. Las unidades de almacenamiento aumentaron en capacidad, 100 GB para almacenamiento local (anteriormente de 68 GB) y una unidad adicional de 200 GB para almacenamiento compartido. En la figura 5.1 se muestran las estadísticas de procesamiento, memoria, disco y red observadas durante un mes.

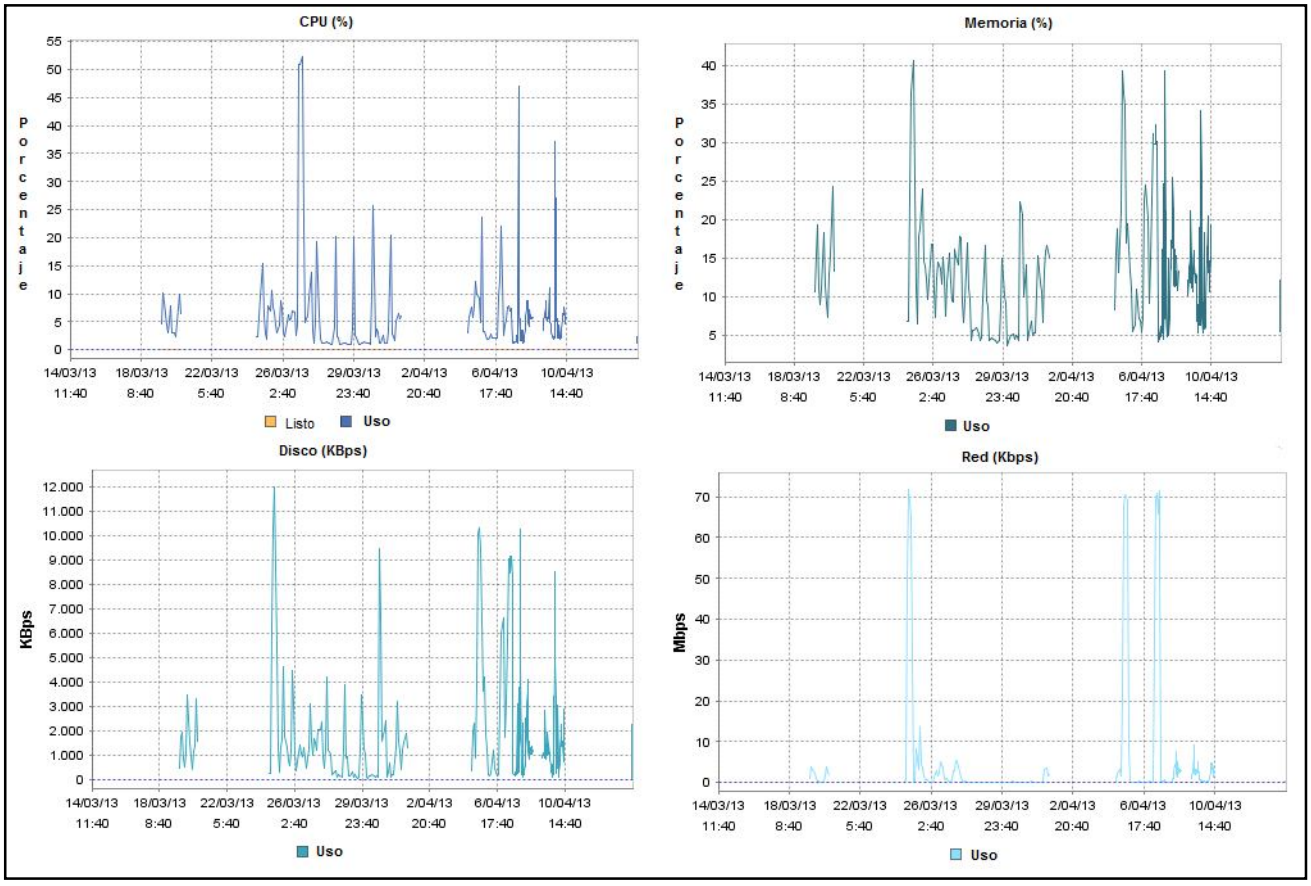

Figura 5.1: Estadísticas de uso del servidor de correo electrónico virtual

El uso de los dos procesadores virtuales es de 405 MHz aproximado, representando casi un 20% de capacidad de procesamiento. El uso de la memoria es de 36% aproximado, casi unos 3GB. Por su parte, el almacenamiento está dispuesto en su totalidad en la red SAN, consolidando un

98,8% de uso en la unidad principal y un 99,3% de uso en la unidad destinada al almacenamiento de los datos.

Por otro lado, el servidor Radius (VZ-AD002) pasó de estar alojado en un sistema operativo Windows Server 2003 a la versión Windows Server 2008 R2. Se mantiene con un único procesador, pero con una memoria RAM de 4 GB (anteriormente de 2 GB). Cuenta con una única unidad de almacenamiento local de 100 GB, permitiendo liberar espacio para futuras implementaciones. En la figura 5.2 se muestran las estadísticas de procesamiento, memoria, disco y red observadas durante un mes.

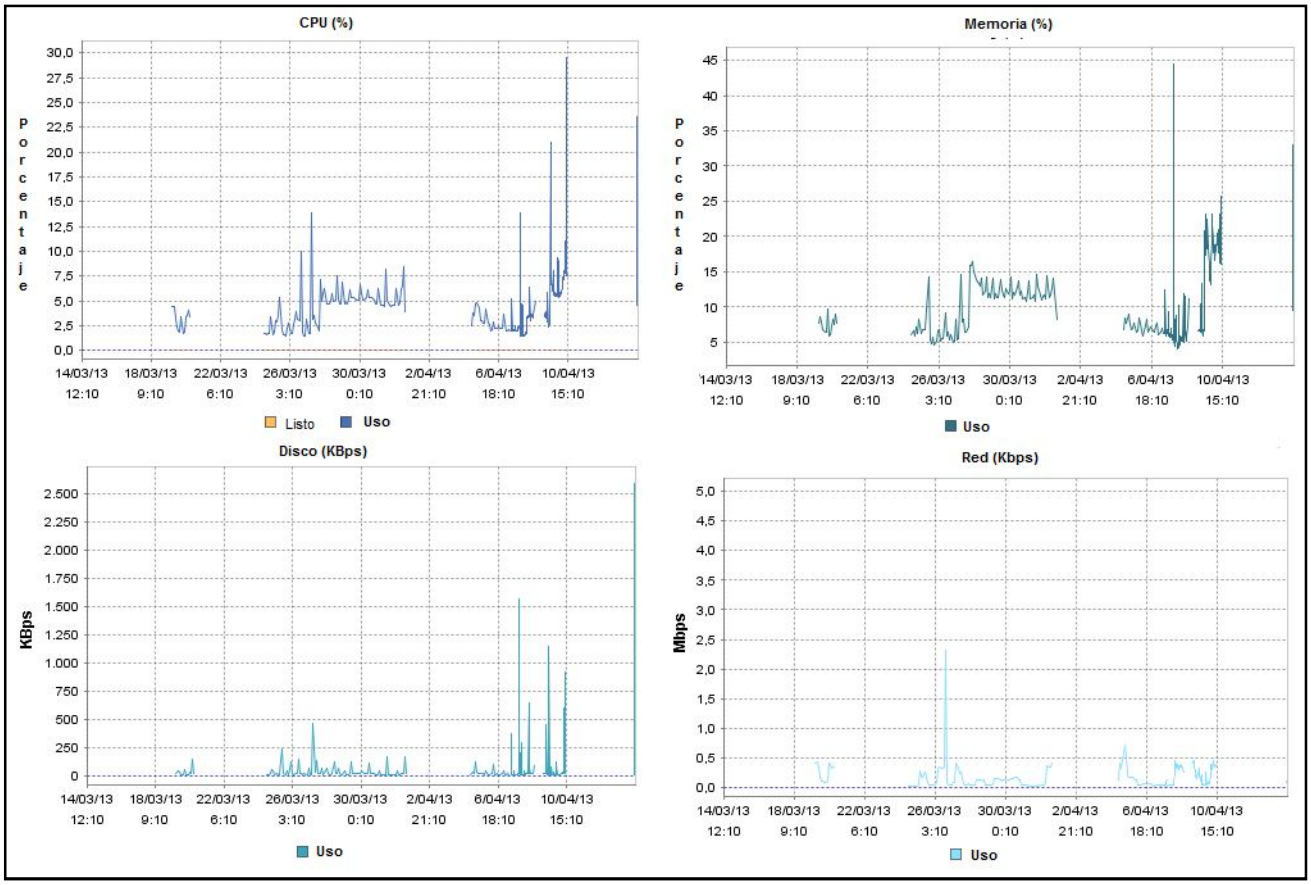

Figura 5.2: Estadísticas de uso del servidor Radius virtual

El uso del procesador virtual es de 75 MHz aproximado, representando casi un 5% de capacidad de procesamiento. El uso de la memoria es de 10% aproximado (450 MB). Por su parte, el almacenamiento está dispuesto en su totalidad en la red SAN, consolidando un 75% de uso en la unidad principal.

El servidor de gestión de clientes (VZ-BC001) se mantiene alojado en un sistema operativo Windows Server 2003 por razones de compatibilidad. Sin embargo, el servidor cuenta con dos procesadores en lugar de uno y 6 GB de memoria RAM (2 GB menos de su antecesor). El almacenamiento es compartido a través de tres unidades de 80 GB, 265 GB y 350 GB respectivamente. En la figura 5.3 se muestran las estadísticas de procesamiento, memoria, disco y red observadas durante un mes.

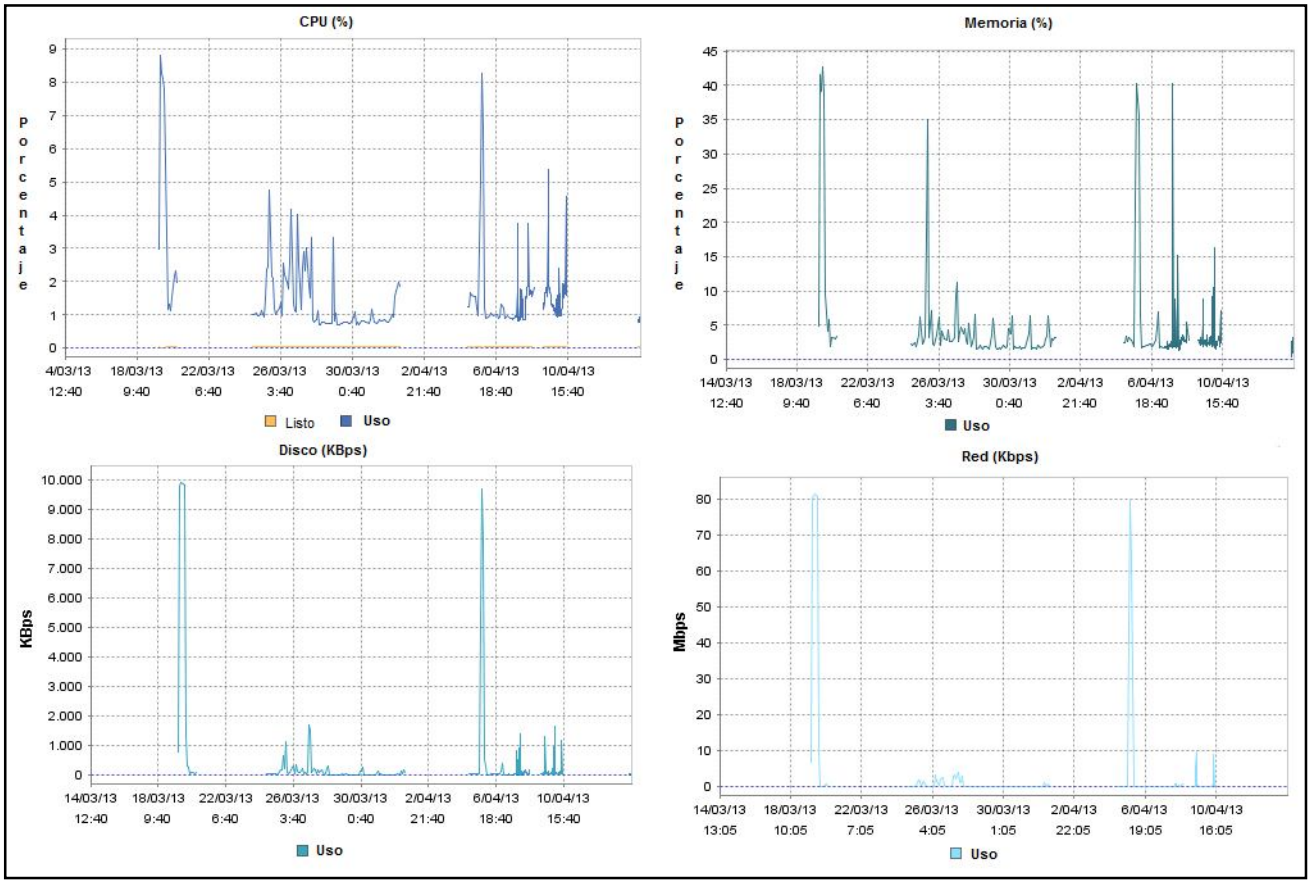

Figura 5.3: Estadísticas de uso del servidor de gestión de clientes virtual

El uso de los procesadores virtuales es de 25 MHz aproximadamente, representando casi un 4% de capacidad de procesamiento. El uso de la memoria es de 8% aproximado (491 MB). Por su parte, el almacenamiento está dispuesto en su totalidad en la red SAN, consolidando un 95.5% de uso en la unidad principal, así como 99% en las unidades secundarias.

Por su parte, El servidor de gestión bancaria (VZ-GB001) se mantiene alojado en un sistema operativo Windows Server 2003 por razones de compatibilidad. Del mismo modo, cuenta con un único procesador y memoria RAM de 4 GB. El almacenamiento es compartido a través de dos unidades de 100 GB y 260 GB respectivamente, aumentando sus capacidades de almacenamiento con respecto a su versión anterior. En la figura 5.4 se muestran las estadísticas de procesamiento, memoria, disco y red observadas durante un mes.

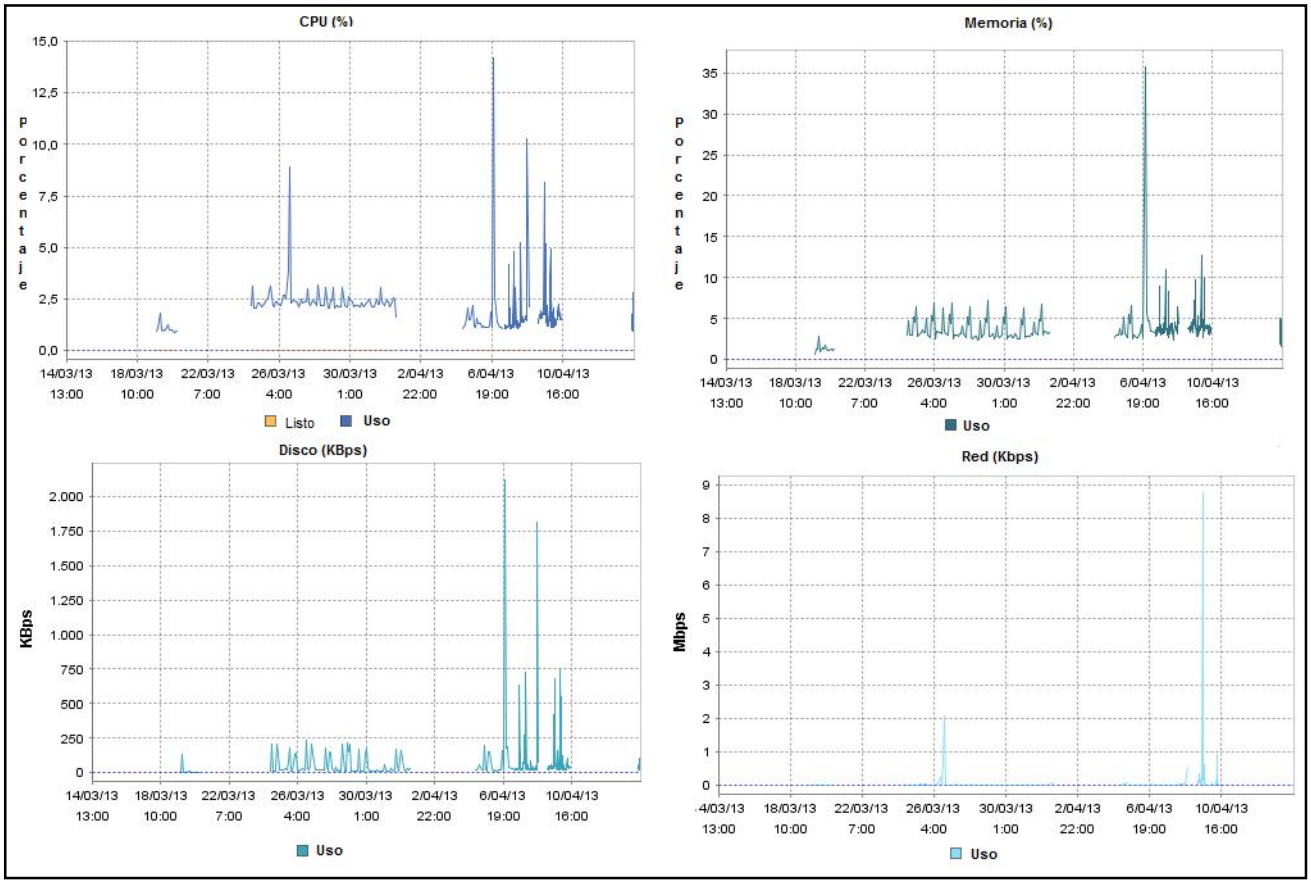

Figura 5.4: Estadísticas de uso del servidor de gestión bancaria virtual

El uso de los procesadores virtuales es de 126 MHz aproximadamente, representando casi un 5% de capacidad de procesamiento. El uso de la memoria es de 6% aproximado (245 MB). Por su parte, el almacenamiento está dispuesto en su totalidad en la red SAN, consolidando un 98% de uso en la unidad principal, así como 99% en la unidad secundaria.

Finalmente, el servidor de contabilidad (VZ-OR001) se mantiene alojado en un sistema operativo Windows Server 2003 por razones de compatibilidad. Utiliza dos procesadores en lugar de uno y 6 GB de memoria RAM. Cuenta con dos unidades de almacenamiento local de 90 GB y 250 GB respectivamente. En la figura 5.5 se muestran las estadísticas de procesamiento, memoria, disco y red observadas durante un mes.

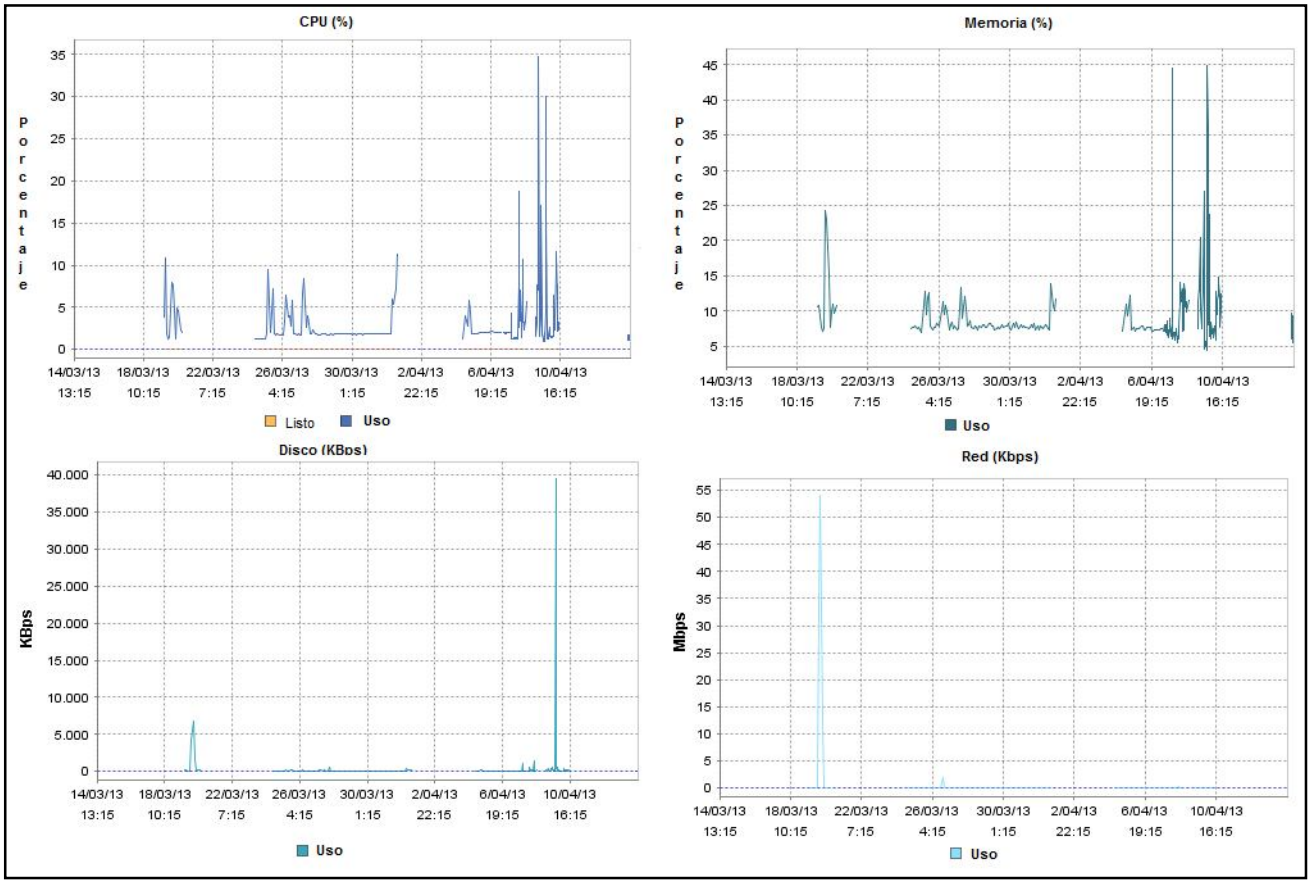

Figura 5.5: Estadísticas de uso del servidor de contabilidad virtual

El uso de los procesadores virtuales es de 25 MHz aproximadamente, representando casi un 10% de capacidad de procesamiento. El uso de la memoria es de 8% aproximado (491 MB). Por su parte, el almacenamiento está dispuesto en su totalidad en la red SAN, consolidando un 93% de uso en la unidad principal, así como 99% en la unidad secundaria.

De esta manera se puede concluir que la virtualización de estos servidores permitió una reasignación de recursos basados en sus requerimientos. Esta asignación se realiza de manera dinámica, por lo que está sujeta a modificación en caso de alertas de uso inapropiadas.

5.1.2. Respecto a nuevas implementaciones

El proyecto de virtualización permitió a la organización crecer en términos de consolidación de nuevos servicios para sus actividades de negocio. De hecho, durante la ejecución del mismo se implementaron nueve servidores directamente sobre la plataforma virtual, los cuales fueron descritos anteriormente. En la tabla 5.1 se exponen las características de los mismos en función del uso promedio de sus recursos.

Servidor	Sistema Operativo	Uso de CPU	Uso de memoria
VZ-TM001	Windows Server 2008 R2	2 CPU, 61 MHz usados	6144 MB, 368 MB usados
VZ-SW001	Windows Server 2008 R2	4 CPU, 9995 MHz usados	10240 MB, 2048 MB usados
VZ-GD001	Windows Server 2008 R2	2 CPU, 75 MHz usados	4096 MB, 450 MB usados
VZ-BB001	Windows Server 2008 R2	1 CPU, 183 MHz usados	4096 MB, 901 MB usados
VZ-SM001	Windows Server 2008 R2	1 CPU, 61 MHz usados	4096 MB, 286 MB usados
VZ-SA002	Windows Server 2008 R2	4 CPU, 30 MHz usados	8192 MB, 245 MB usados
VZ-SP002	Windows Server 2008 R2	3 CPU, 122 MHz usados	6144 MB, 491 MB usados
VZ-OR002	Windows Server 2003	1 CPU, 150 MHz usados	6144 MB, 184 MB usados
VZ-VC001	Windows Server 2008 R2	4 CPU, 705 MHz usados	5120 MB, 2560 MB usados

Tabla 5.1: Sistemas operativos y recursos de los nuevos sistemas

La incorporación de estos sistemas representó un crecimiento notable en la infraestructura de la organización. Inicialmente se contaban con 11 servidores físicos, de los cuales 6 fueron descartados para la virtualización (representando un 55% de la población), mientras que el 45% de los mismos fueron virtualizados (5 servidores). Así mismo, se implementaron 9 nuevos servidores virtuales, representando un 81% de crecimiento en la población, consolidando un total de 20 servidores en la infraestructura tecnológica de la organización.

En la figura 5.6 se expone un gráfico que representa el porcentaje de adopción de servidores físicos y virtuales de la organización luego de aplicar el proyecto de virtualización.

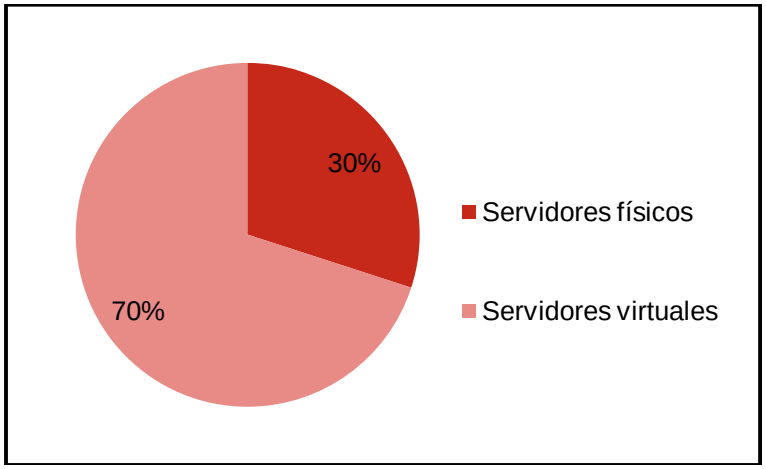

Figura 5.6: Porcentaje de adopción de servidores virtuales

Es así como el 70% de la infraestructura (14 servidores) está conformada por servidores virtuales y el 30% (6 servidores) son servidores físicos. Del mismo modo, la virtualización permitió a la organización avanzar en la adopción de un sistema operativo más reciente y con mejores prestaciones, tal es el caso de Windows Server 2008 R2. De los 11 servidores físicos iniciales, nueve de ellos alojaban el sistema operativo Windows Server 2003 (82%), un único servidor con Windows Server 2000 (9%) y una sola instancia de Windows Server 2008 (9%).

En la figura 5.7 se expone un gráfico que contempla las versiones de los sistemas operativos adoptados por los 20 servidores que conforman la infraestructura tecnológica luego de la culminación del proyecto de virtualización.

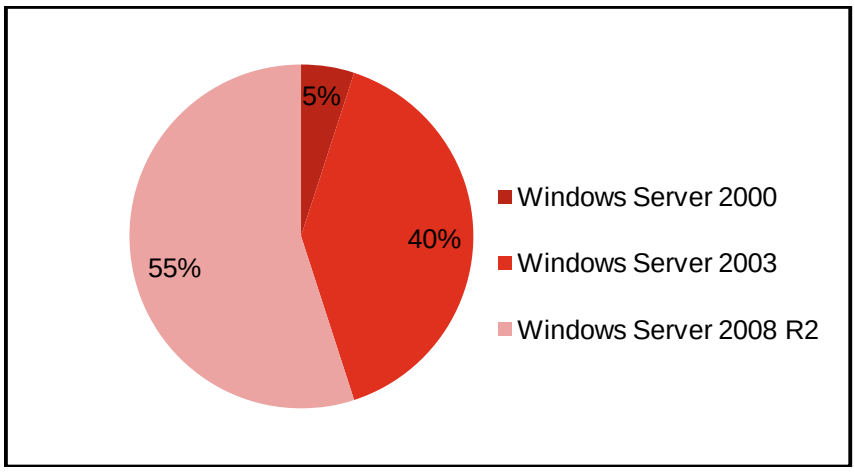

Figura 5.7: Porcentaje de adopción de versiones de sistemas operativos

Como se expone anteriormente, el sistema operativo Windows Server 2008 posee un porcentaje de adopción del 55% (11 servidores), alcanzando la mayoría con respecto a Windows Server 2003 con un 40% (8 servidores) y una única instancia de Windows Server 2000 (5%).

5.1.3. Respecto a entornos operativos

La implementación del proyecto de virtualización permitió a la organización disponer de tres ambientes de ejecución para la disposición de sus ambientes virtuales, de manera de poder distribuirlos en función de los recursos requeridos y la funcionalidad ofrecida para sostener las actividades de negocio. En total se consolidaron tres entornos operativos: desarrollo, producción y pruebas.

Respecto al entorno de desarrollo, el mismo está conformado por dos servidores blades, el primero de ellos cuenta con una capacidad de procesamiento de 20 GHz a través de 16 procesadores lógicos, de los cuales se hace uso de de 324 MHz aproximados. Cuenta con 28 GB de memoria con 17 GB usados por las 3 máquinas virtuales alojadas. El almacenamiento total es de 790 GB con 95% de uso a través de una unidad local y tres unidades de almacenamiento compartido SAN.

En la figura 5.8 se exponen las estadísticas de uso de recursos observadas durante un mes en el primer servidor blade correspondiente al entorno de desarrollo.

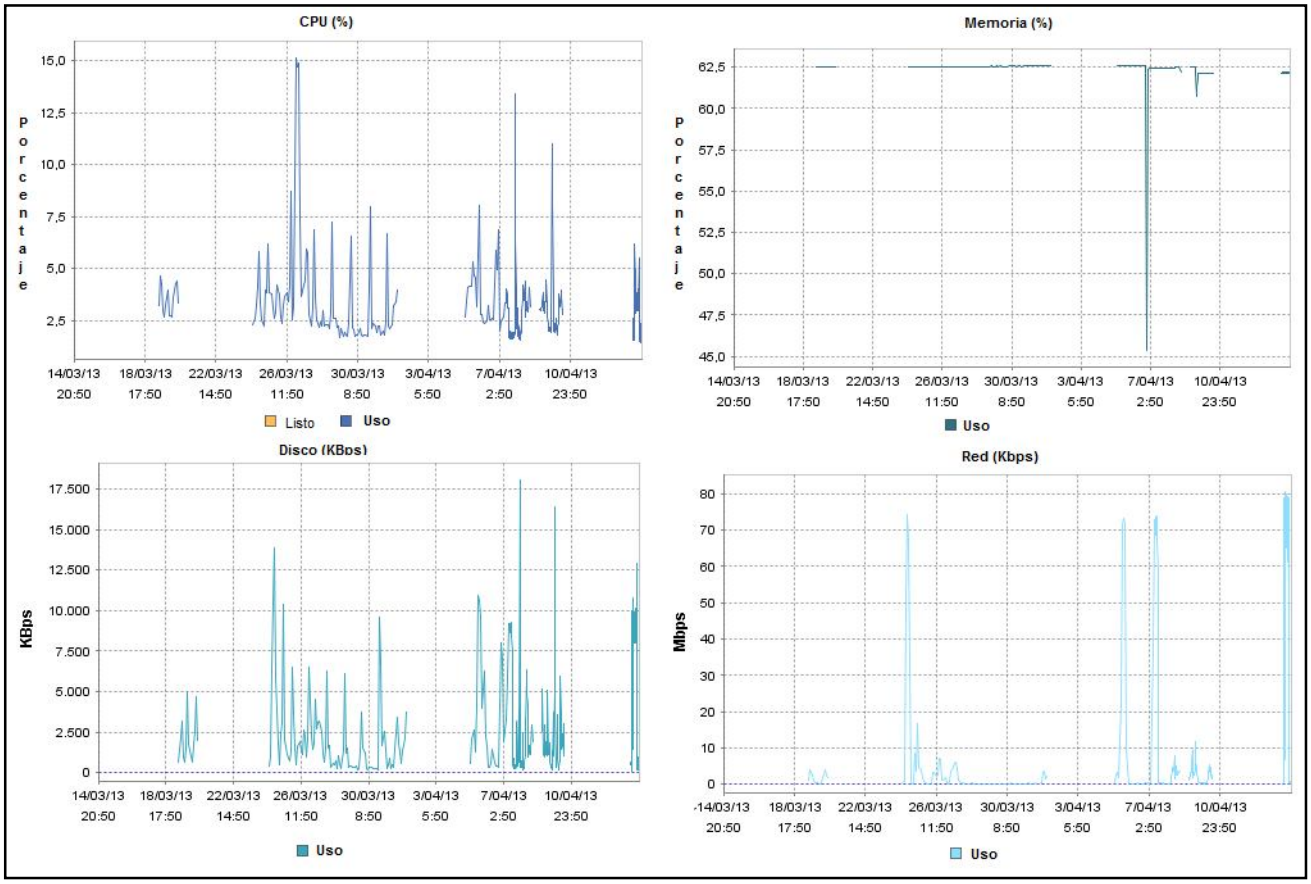

Figura 5.8: Estadísticas de uso del primer servidor blade de desarrollo

El segundo servidor blade cuenta con una capacidad de procesamiento de 20 GHz a través de 16 procesadores lógicos, de los cuales se hace uso de de 396 MHz aproximados. Cuenta con 28 GB de memoria con 17 GB usados por las 3 máquinas virtuales alojadas. El almacenamiento total es de 1 TB con 85% de uso a través de una unidad local y 6 unidades de almacenamiento compartido SAN. En la figura 5.9 se exponen las estadísticas de uso de recursos observadas durante un mes en dicho servidor.

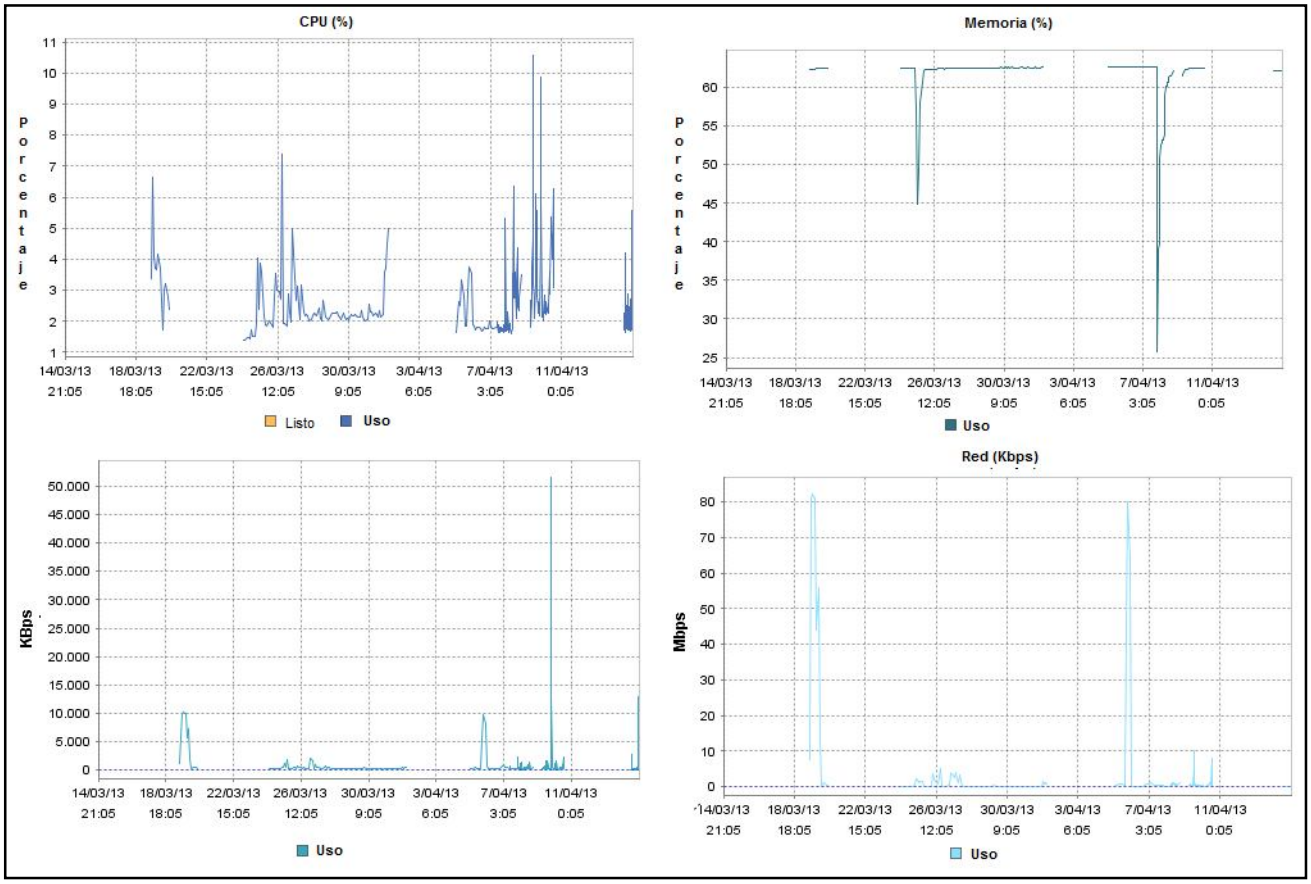

Figura 5.9: Estadísticas de uso del segundo servidor blade de desarrollo

El entorno de producción está conformado por dos servidores blades, el primero de ellos cuenta con una capacidad de procesamiento de 37 GHz a través de 24 procesadores lógicos, de los cuales se hace uso de de 651 MHz aproximados. Cuenta con 48 GB de memoria con 20 GB usados por las 3 máquinas virtuales alojadas. El almacenamiento total es de 1 TB con 96% de uso a través de una unidad local y una unidad de almacenamiento compartido SAN.

En la figura 5.10 se exponen las estadísticas de uso de recursos observadas durante un mes en el primer servidor blade correspondiente al entorno de producción.

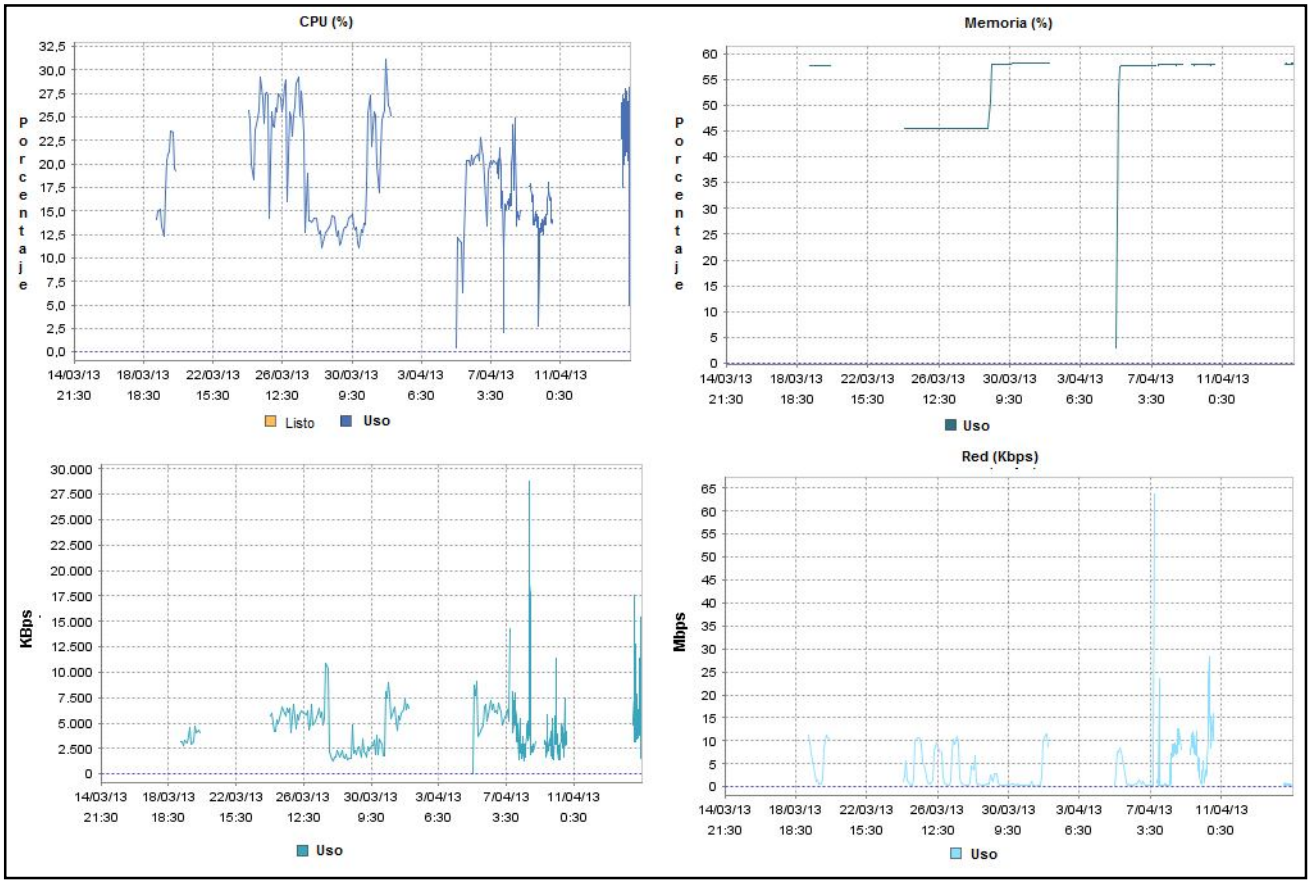

Figura 5.10: Estadísticas de uso del primer servidor blade de producción

El segundo servidor blade cuenta con una capacidad de procesamiento de 36 GHz a través de 24 procesadores lógicos, de los cuales se hace uso de de 754 MHz aproximados. Cuenta con 48 GB de memoria con 10 GB usados por las 2 máquinas virtuales alojadas. El almacenamiento total es de 674 GB con 96% de uso a través de la unidad local del servidor blade. En la figura 5.11 se exponen las estadísticas de uso de recursos observadas durante un mes en dicho servidor.

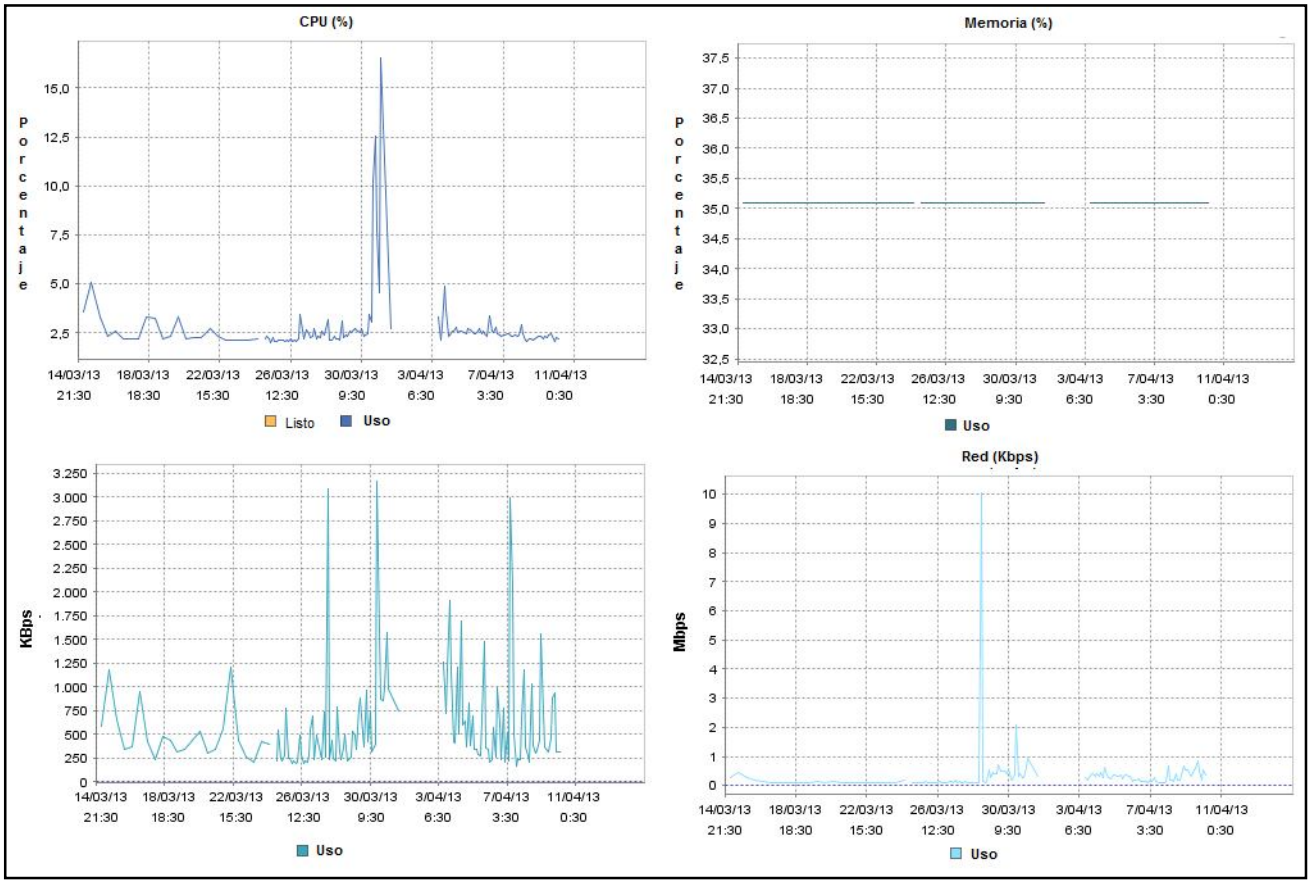

Figura 5.11: Estadísticas de uso del segundo servidor blade de producción

Finalmente, el entorno de pruebas está conformado por un único servidor blade, el cual cuenta con una capacidad de procesamiento de 37 GHz a través de 24 procesadores lógicos, de los cuales se hace uso de de 279 MHz aproximados. Cuenta con 48 GB de memoria con 20 GB usados por las 3 máquinas virtuales alojadas. El almacenamiento total es de 1 TB con 85% de uso a través de una unidad local y cuatro unidades de almacenamiento compartido SAN. En la figura 5.12 se exponen las estadísticas de uso de recursos observadas durante un mes en dicho servidor.

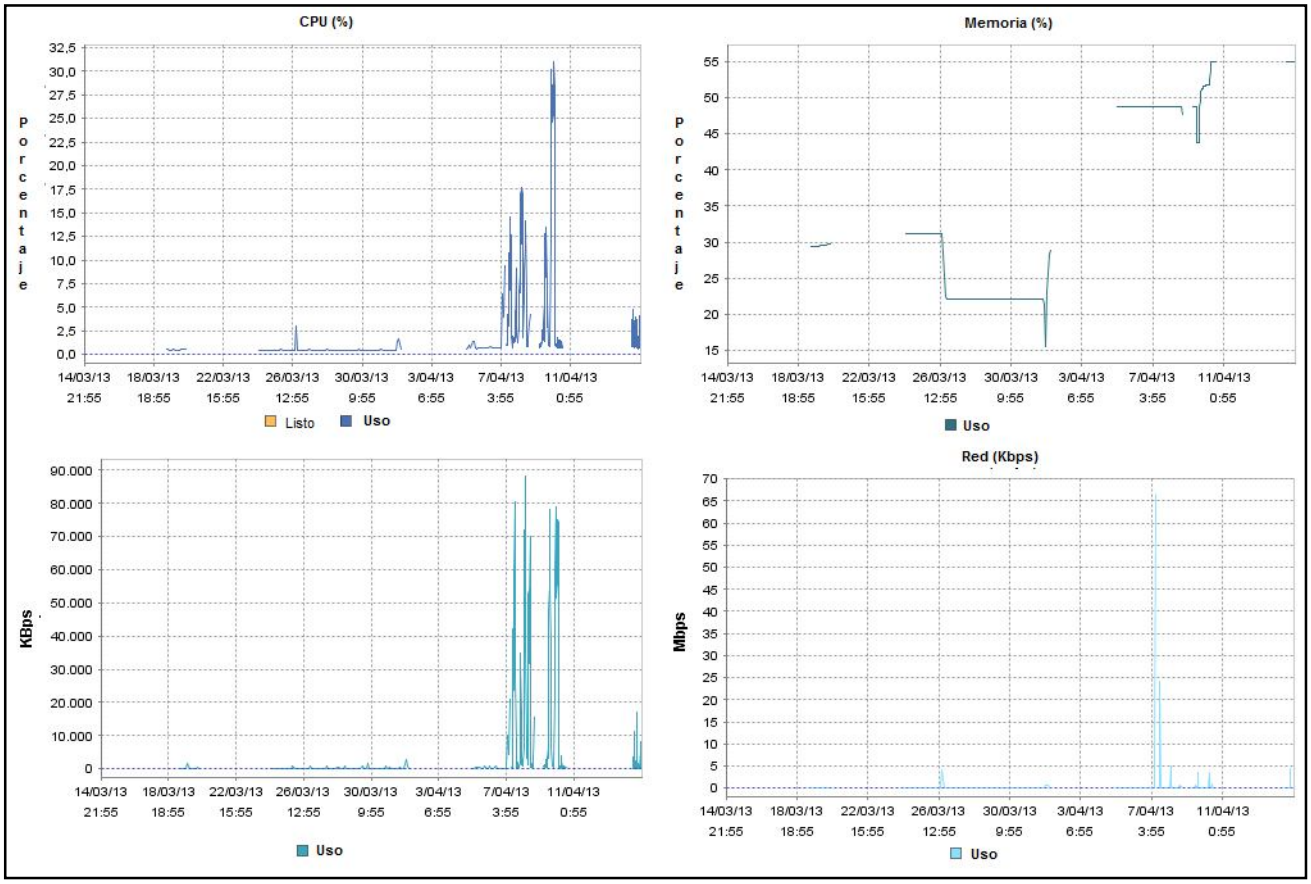

Figura 5.12: Estadísticas de uso del servidor blade de pruebas

La disposición de diferentes entornos operativos permite distribuir adecuadamente las cargas de trabajo de acuerdo a la naturaleza de los sistemas. Esta distribución permite mejorar el modelo de gestión de la organización al evaluar el rendimiento de los sistemas y permitir sus traslados una vez que su respectiva fase de implementación pase de ser considerada una prueba a ser puesta en desarrollo, así como un desarrollo pase a formar parte de un entorno en producción.

5.1.4. Respecto al almacenamiento

De acuerdo al planteamiento de la infraestructura, las máquinas virtuales cuentan con dos ambientes en donde pueden disponer de su almacenamiento. La primera de ellas es el almacenamiento local, provisto por las unidades de disco presentes en cada servidor blade. La segunda corresponde a los volúmenes de almacenamiento dispuestos en la red SAN, mapeados directamente a los hosts que lo necesiten.

De esta manera, el almacenamiento de las máquinas virtuales, tanto su configuración como los datos que manejen, pueden ser situados directamente en el host, en la red SAN ó en una combinación de ambos. En la figura 5.13 presenta el porcentaje de uso en los discos de los cinco servidores blades dispuestos en la infraestructura.

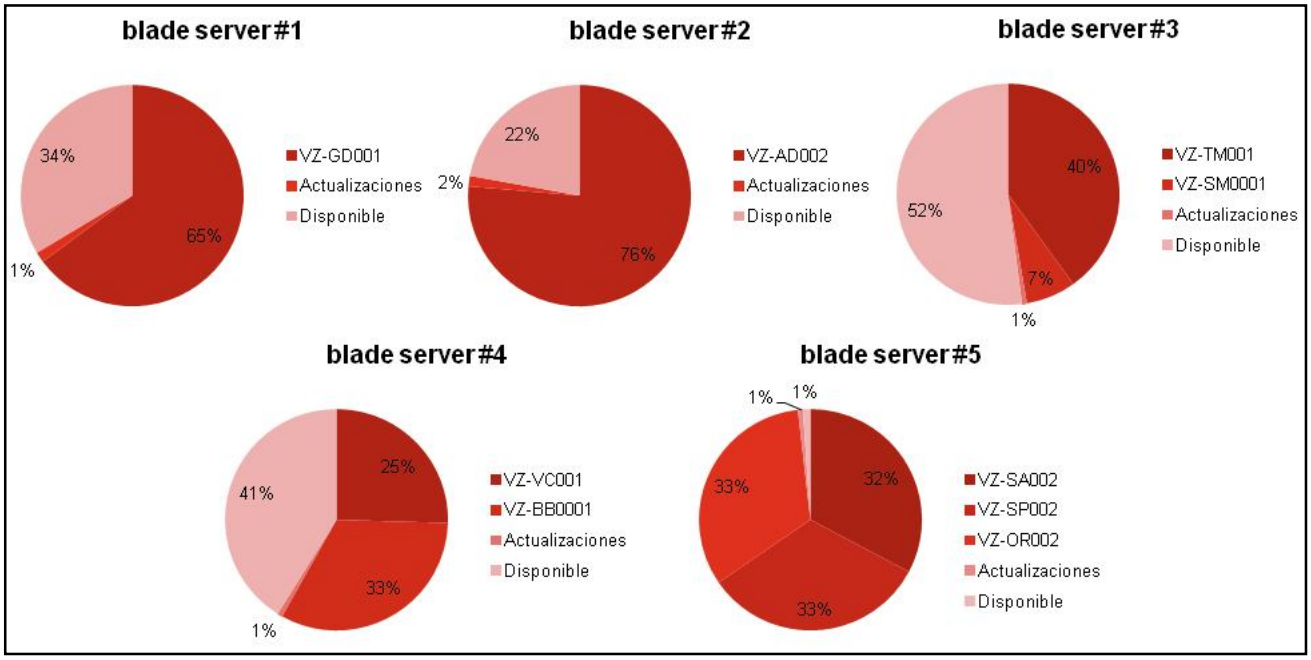

Figura 5.13: Uso de almacenamiento local en servidores blades

Los 262 GB de almacenamiento combinado del entorno de desarrollo son usados en un promedio de 72% por sólo dos servidores y los parches de seguridad de los respectivos hosts, dejando un aproximado de 73 GB para futuras implementaciones. Por su parte, el entorno de producción, compuesto por 550 GB de almacenamiento combinado es usado en un 54% por 4 servidores, lo que corresponde a 253 GB disponibles aproximadamente. Finalmente, el entorno de prueba cuenta con el porcentaje más alto de uso con un 99% sobre el total de su capacidad.

Por otra parte, la red de almacenamiento SAN está compuesta por 10 discos compartidos y dispuestos en el sistema BladeCenter, gestionados a través de la herramienta IBM Storage Configuration Manager.

De acuerdo a sus requerimientos, el almacenamiento de ocho servidores virtuales fue dispuesto en dicha red, habilitando la posibilidad de que más de un servidor pudiese acceder a un determinado contenido. En la figura 5.14 se muestra un gráfico en donde se presentan el número de unidades por servidor y la cantidad de almacenamiento requerido en cada una.

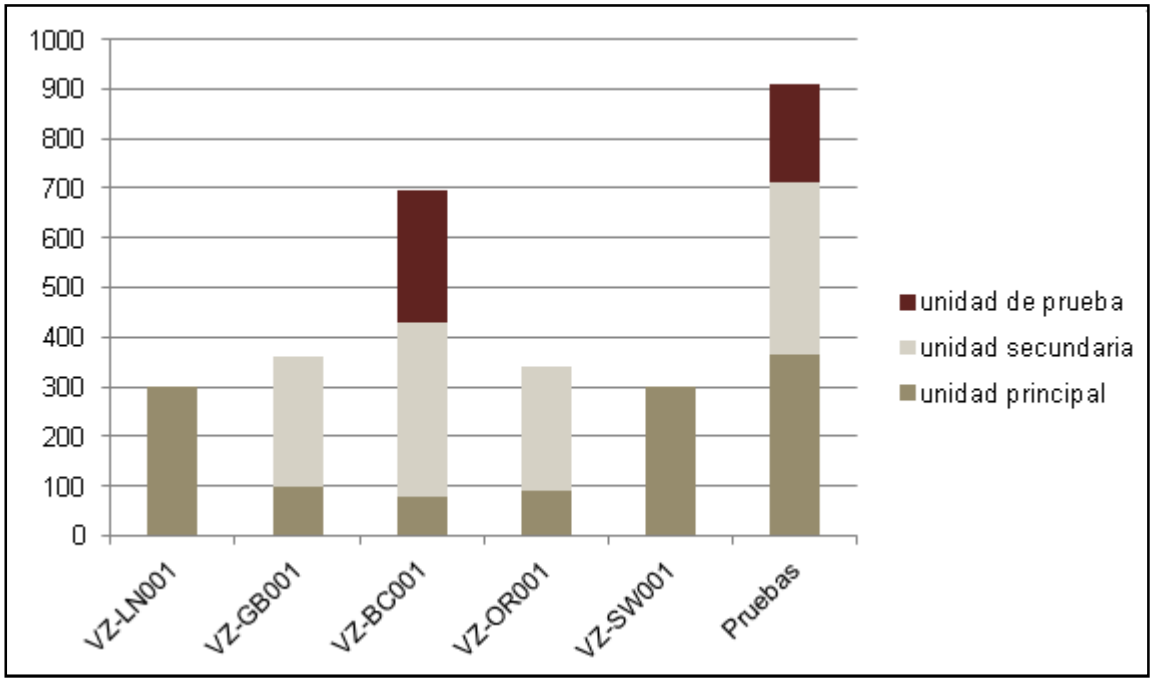

Figura 5 14: Unidades de almacenamiento compartido por servidor

Cabe destacar que la mayoría de los servidores expuestos requieren de más de una unidad de almacenamiento, las cuales fueron identificadas como unidad principal, unidad secundaria y unidad de prueba. El tamaño de cada una unidad depende de los requerimientos de la aplicación alojada. Por su parte, la sección identificada como pruebas corresponde a las tres máquinas virtuales identificadas anteriormente (VZ-SA002, VZ-SP002, VZ-OR002).

La capacidad total de la red SAN viene dada por las 10 unidades de almacenamiento que cuentan con 600 GB cada una, lo que da un resultado de 5840 GB disponibles para el uso de máquinas virtuales. La misma es segmentada en volúmenes, los cuales son creados a través del IBM Storage Configuration Manager y respectivamente mapeados a los servidores blades que los requieran. La figura 5.15 expone el porcentaje de uso de la red SAN por volúmenes de almacenamiento.

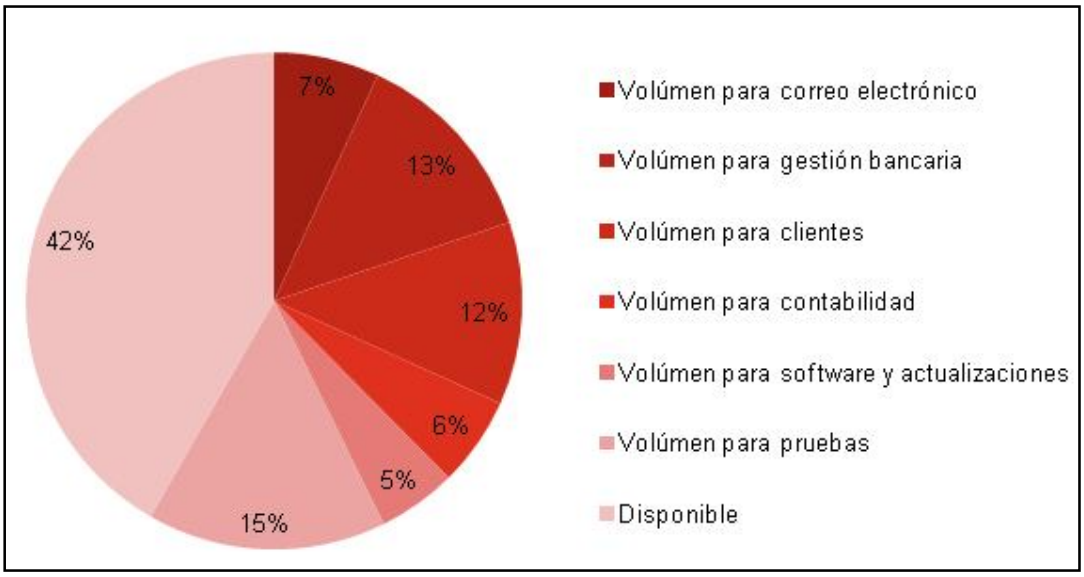

Figura 5.15: Volúmenes de almacenamiento compartido SAN

En total se crearon siete volúmenes de almacenamiento, los volúmenes de correo electrónico y actualizaciones cuentan con 300 GB cada uno, el volumen de gestión bancaria se divide en 2 unidades que conforman 360 GB en total y tres unidades conforman el volumen para clientes, consolidando unos 695 GB.

Por su parte, el volumen de contabilidad aloja 340 GB divididos en dos unidades y finalmente, el volumen de pruebas dispuesto para 3 servidores, agrupa un almacenamiento de 910 GB en total, siendo este último, el volumen con mayor requerimiento de espacio.

Es así como la red de almacenamiento SAN es usada en un 58%, dejando un aproximado de 2.3 TB disponibles para futuras implementaciones.

6. Estrategia Desarrollada

En este capítulo se plantea una estrategia para la implementación de la virtualización con el fin de alcanzar la consolidación y centralización de servidores que cumplan con los controles y políticas de seguridad de información propias de una organización. Los planteamientos desarrollados en la misma se basan en la experiencia obtenida al llevar a cabo un proyecto de virtualización de servidores en un entorno empresarial, usando herramientas del mercado tecnológico actual y siguiendo con las consideraciones de seguridad explicitas.

De acuerdo a los resultados obtenidos, se demuestra que el cumplimiento de los objetivos planteados fue posible gracias a la ejecución del marco metodológico expuesto a lo largo de este documento. Por lo que los lineamientos expuestos a continuación conforman una propuesta de soluciones diseñadas para orientar en el proceso de implementación, configuración y mantenimiento de una infraestructura basada en servidores virtuales.

La estrategia diseñada consta de 5 pasos fundamentales que abarcan las etapas involucradas en un proyecto de virtualización de servidores, conformando una serie de planteamientos orientados al desarrollo de una implementación adecuada y basada en las mejores prácticas actuales. Dichos pasos consisten en:

1) Definir el alcance: Consiste en identificar los componentes involucrados en el proyecto de virtualización de servidores de la organización, a fin de determinar cuáles son los procedimientos y mecanismos que deben ser ejecutados en la implementación, de acuerdo a una planificación previamente planteada.

2) Estudiar las tecnologías del mercado: Para una organización, la selección de una determinada solución tecnológica depende de varios factores, siendo el retorno de inversión uno de los más importantes. Es por ello que el estudio de las diferentes opciones debe estar orientado en la consolidación de los objetivos planteados, satisfacer las demandas del negocio y asegurar un crecimiento a nivel competitivo que permita escalar a proyectos de más alto impacto a futuro.

3) Desarrollar una planificación: Sin duda, una de las tareas más relevantes. Todo el proyecto depende de una adecuada planificación. La misma debe contemplar los objetivos planteados, el tiempo de ejecución de los procedimientos de instalación y configuración de las soluciones adquiridas, así como el análisis de los resultados obtenidos en las pruebas. Determinando si el proyecto satisface con los requerimientos indicados por la organización.

4) Categorizar los riesgos: Desde el punto de vista de seguridad de la información, una categorización de los riesgos permite identificar los niveles de criticidad que representan los diferentes cambios implícitos en el proceso de migración a una infraestructura virtual. Esto influye en la toma de decisiones y redefine el alcance inicialmente planteado.

5) Mejores prácticas en la virtualización: Finalmente, este último paso representa la aplicación de una serie de configuraciones particulares a los diferentes componentes de la virtualización de servidores, como el hardware, programa de control, máquinas virtuales y el resto de la infraestructura, conformando así un conjunto de mejores prácticas para la virtualización organizacional.

A continuación, se exponen con más detalle cada uno de los pasos expuestos anteriormente.

6.1. Alcance

Los procedimientos de seguridad para asegurar un entorno virtual de una organización deben incluir los entornos físicos ya que estos tienen un alcance notorio en las políticas de seguridad de

información de la misma. Deben considerarse diferentes opciones en la configuración de máquinas virtuales como servidores, así como las consideraciones de seguridad necesarias para el cumplimiento de las mismas. Dichas consideraciones incluyen tanto conceptos técnicos como tareas de soporte.

El objetivo es identificar y describir cada uno de los componentes de una infraestructura virtual, pensando en mejorar la seguridad de la información y la reducción de los riesgos en la organización.

Particularmente, toda organización que desee implementar las virtualización de servidores de acuerdo a los lineamientos propuestos en el presente documento debe plantearse un conjunto de requerimientos técnicos y de negocio tales como:

- Consolidación de servidores, aplicaciones y servicios de misión crítica en diversos tipos de hardware, logrando niveles altos de escalabilidad y confiabilidad, propios de servidores de tipo empresarial

- Implantación de una infraestructura virtual con tiempos de respuesta adecuados con respecto a las demandas del negocio, a través de la asignación dinámica de recursos a las máquinas virtuales, de acuerdo a las necesidades de la organización.

- Establecimiento de nuevos mecanismos de recuperación ante desastres, a través de capacidades de nivel empresarial como confiabilidad, escalabilidad y alto rendimiento.

- Soporte para varias tecnologías de almacenamiento y de comunicaciones.

Para garantizar el cumplimiento de estos requerimientos, la organización debe ejecutar una metodología de planificación que permita definir los objetivos a cumplir, diseñar una plataforma y adquirir una solución en el mercado.

6.2. Tecnologías en el mercado

El proceso de selección de una solución tecnológica no es tarea fácil ya que requiere de un conocimiento previo de los términos usados. Se sugiere evaluar más de una opción, considerando tanto elementos de negocio como elementos técnicos y de soporte que no comprometan la compatibilidad de los sistemas existentes.

La virtualización de servidores basada en host, comúnmente denominada virtualización de servidores es la arquitectura predominante en el mercado de virtualización de servidores actual cuyo paradigma es la de consolidar sistemas anfitriones enteros (es decir, considerando todos sus componentes como memoria, procesadores, adaptadores de red, adaptadores de video, controles de almacenamiento, etc.) como entidades lógicas independientes, lo que permite la disposición de máquinas virtuales como una colección de archivos que pueden residir en cualquier sistema físico que soporte su formato.

Existen muchos proveedores que ofrecen soluciones para la virtualización de servidores, tales como VMware, Microsoft, Xen, Novell, Linux Red Hat, IBM PowerVM, entre otras. Siendo VMware la empresa líder en el mercado, la cual ha proporcionado productos de virtualización de arquitecturas x86 desde el año 2000 y, más recientemente, productos basados en x64. Su sistema operativo ESXi y la suite de productos vSphere cuentan con altos niveles de aceptación, ya que ofrece características comúnmente exigidas por el sector empresarial de hoy en día, tales como la migración en vivo, tolerancia a fallos y distribución planificada de recursos. Además de que cuenta con el soporte de muchos vendedores de software independiente especializados en aplicaciones de servidores, anti-virus y herramientas de respaldo.

Microsoft inicialmente entró en el mercado de la virtualización de servidores con Microsoft Virtual Server, cuando Windows Server 2008 Hyper-V fue introducida en esta tecnología. Las características de Hyper-V incluyen tolerancia a fallos dinámica, agrupación geográfica y soporte de controlador de dispositivos Windows y Linux virtuales [46].

Los vendedores restantes que ofrecen soluciones de virtualización de servidores generalmente están asociados a la distribución de soluciones basadas en código abierto, tal es el caso de Xen, Novell y Linux Red Hat.

Adicionalmente, la metodología de trabajo presentada en capítulos anteriores recopila una serie de consideraciones respecto a los elementos técnicos que soportan la elección de una tecnología respecto a sus competidores. Características como el soporte de ejecución de diferentes tipos de sistemas operativos, amplia adopción de controladores de hardware y la facilidad de gestión y soporte son factores importantes a considerar. Con respecto al hardware, este debe ofrecer funcionalidades de valor agregado en términos de optimización y compatibilidad que los diferencie de otros competidores, así como garantizar una aceptable propuesta en función de energía, espacio y rendimiento.

A pesar de que, desde el punto de vista de negocio, cuando una organización invierte en la compra de una determinada tecnología, se busca cumplir con las demandas a un bajo costo. Sin embargo, el proceso de migrar a una infraestructura virtual es un proceso costoso. Por lo que el enfoque inicial debe estar basado en el retorno de inversión y no en “hacer más con menos”.

En definitiva, son muchos los aspectos que deben considerarse en la toma de decisiones para adquirir tanto soluciones para virtualizar como en plataformas físicas de alojamiento. Sin embargo, no hay que olvidar que la virtualización es una técnica basada en la compartición de recursos, por lo que términos como disponibilidad, confiabilidad y rendimiento deben ser críticos a la hora de elegir una tecnología, sin olvidar los costos asociados a la adquisición en función del retorno de la inversión que puede obtenerse, sobre todo con respecto a las actividades de negocio involucradas.

6.3. Desarrollo de la planificación

Toda estrategia es diseñada para alcanzar objetivos y el desarrollo de la misma implica varios elementos que deben llevarse a cabos a través de una planificación basada en etapas. En el caso de la virtualización, la planificación debe consistir en lo siguiente:

- **Identificar la organización:** Desde reconocer las capacidades con las que se cuentan y los recursos disponibles, identificando las actividades acertadas y las que no, de manera de detectar las oportunidades de mejoramiento a través de una evaluación general.

- **Declaración de objetivos:** Definiendo lo que la organización desea cumplir para atender a los requerimientos de sus actividades de negocio y la necesidad de mejorar los servicios ofrecidos a su personal y clientes.

- **Preparar lo necesario para el cumplimiento de los objetivos:** A través de la evaluación de las capacidades de la organización con análisis internos y externos basados en el estudio del entorno operativo de la misma, así como las soluciones en el mercado que pueden ser adquiridas para lograr los objetivos.

- **Elaborar un plan:** Detallando las acciones a ejecutar, las capacidades a desarrollar, recursos requeridos, cambios que se deben producir y usuarios afectados.

- **Toma de decisiones:** Consiste en emprender acciones anteriormente planeadas para obtener los resultados esperados. Incluye la instalación y configuración de los sistemas de acuerdo a

las decisiones acordadas. La ejecución de estas acciones es un tema delicado ya que requiere generar muchos cambios, modificar la estructura de trabajo, roles y capacidades. Para ello se requiere entrenamiento, cambiar paradigmas, enfrentar nuevos desafíos y hacer las cosas de manera diferente.

- **Evaluación de los resultados:** Implicando la revisión de las acciones ejecutadas y evaluando si los objetivos fueron alcanzados o no, determinando las razones de ello. Esta información es fundamental para mejorar y perfeccionar la metodología usada, en caso de que sea necesario.

En el proceso de implementación deben participar todos los integrantes que formen parte de una manera u otra de las actividades diarias de gestión y administración de sistemas y comunicaciones de la organización. Esta actividad es de carácter continuo que se nutre de las experiencias de todo el capital humano involucrado, de los resultados obtenidos, de las capacidades desarrolladas, de los cambios en el entorno operativo y de los resultados ofrecidos a usuarios.

Del mismo modo, deben medirse los resultados en todos los procesos ejecutados. Lo más recomendable es evaluarlos en ciclos cortos, de acuerdo al tipo de actividad y de la organización. De esta forma es más sencillo detectar fallas y corregirlas, determinando si el proyecto da los resultados esperados y si es necesario hacer ajustes, cancelarlo o reforzarlo.

En definitiva, son muchas las acciones que deben seguirse durante el diseño y desarrollo de una estrategia de virtualización organizacional. Sin embargo, las recomendaciones que pueden tomarse en cuenta se resumen en:

- Analizar las capacidades e insuficiencias internas a través de un análisis honesto, sin olvidar el sentido común en la elaboración de planes para determinar lo que se hace bien y lo que se mal, siendo este planteamiento un elemento clave.

- Definir objetivos reales, ambiciosos pero posibles de lograr, a través de pasos alcanzables y claramente establecidos.

- Realizar una evaluación muy detallada y objetiva de la metodología usada que incluya diversos indicadores de aspectos tangibles e intangibles.

Es así como se determinan los aspectos metodológicos que pueden considerarse durante el desarrollo de un proyecto de virtualización organizacional. Esto permitirá un desenvolvimiento lógico y estructurado de las actividades realizadas que beneficiarán a la organización en términos de escalabilidad y disposición de proyectos futuros. A continuación se presentan los elementos técnicos de instalación, configuración y de seguridad que pueden considerarse en la implementación del proyecto.

6.4. Riesgos de seguridad

Cuando se trata de virtualizaciones, la seguridad es uno de los aspectos más cruciales, sobre todo al considerar los diferentes riesgos a lo que son expuestos los sistemas candidatos a ser virtualizados.

Debido a que la implementación de la virtualización en el centro de datos de una organización conlleva a la aplicación de nuevos términos y técnicas, es común determinar que la mayoría de los servidores virtualizados son menos seguros que los servidores físicos a los que sustituyen. La razón de este planteamiento se debe a la existencia de diversas áreas en la que los entornos virtualizados pueden ser vulnerables [46]. Dichas áreas son las siguientes:

- Seguridad de la información
- Capa de abstracción entre sistema anfitrión y máquinas virtuales
- Red de comunicaciones entre máquinas virtuales
- Cargas de trabajo
- Control de acceso
- Control y seguridad de la red

Así como muchas de las herramientas de gestión centralizada de servidores virtuales también presentan riesgos de seguridad que requieren de controles adicionales, tales como:

- Instalación de anti-virus
- Definición de políticas de seguridad locales y restrictivas
- Creación de conexiones de red para la comunicación entre servidores virtuales y herramientas de gestión que estén separadas y cifradas
- Presentar una capa adicional de autenticación para la administración y gestión

En definitiva, la seguridad es un tema que debe abordarse en varias etapas, considerando los diferentes elementos que conforman una infraestructura virtual. De hecho, la capa de virtualización juega un papel importante en la plataforma de tecnologías de información dado el nivel privilegiado que posee un programa de control sobre la infraestructura, por lo que es susceptible a ataques que pueden comprometer potencialmente todas las cargas de trabajo alojadas.

Desde una perspectiva de seguridad y gestión, la capa de virtualización debe ser protegida cuyo sistema operativo anfitrión (incluidas las aplicaciones) debe ser periódicamente actualizado con los parches de seguridad más recientes. Es de suma importancia que se establezcan pautas y guías para su configuración.

El ataque a uno de los sistemas virtuales principales podría permitir la ejecución de código malicioso por parte de un sistema invitado, con el fin de obtener privilegios elevados y obtener acceso al programa de control y sus máquinas virtuales. A partir de ahí, el atacante podría realizar diversos ataques orientados a la denegación de servicio.

En la tabla 6.1 se presenta una visión general de algunas de las formas más comunes de ataques a nivel de programa de control. La misma no representa una lista completa, pero pretende destacar aquellos que pueden ser considerados como más comunes.

Tipo de ataque	Descripción	Impacto	Opciones para frustrar el ataque
Denegación de servicio	Los ataques y aplicaciones de este tipo intentan explotar las vulnerabilidades descubiertas en el programa de control, así como sondear los puertos de administración más comunes	Interrupción del servicio para todas las aplicaciones de las máquinas virtuales alojadas	El sistema operativo debe ser configurado para no consumir la totalidad de cualquiera de los recursos físicos
Explotación del servicio ó vulnerabilidades en la configuración	Un método por el cual un atacante es capaz de elevar privilegios	El riesgo de acceso a una cuenta comprometida o a privilegios podría permitir a un atacante alterar ó capturar detalles de los servicios ó de la configuración	Establecer políticas de seguridad que definan la configuración de los controles de acceso al programa de control. Proteger su manipulación
Inserción de una máquina virtual maliciosa	La inserción de una máquina virtual maliciosa en un host a través del uso de credenciales de autenticación	Una máquina virtual maliciosa puede pasar por una máquina virtual tradicional, si el personal de tecnología no es capaz de detectarla. Un atacante tendría un servidor completo a su disposición que reside en la red de área local interna (LAN)	La proliferación de máquinas virtuales es un asunto de gestión que debe ser manejado a través de la capacitación, seguimiento y cumplimiento de políticas de seguridad
Clonación de una máquina virtual para obtener datos confidenciales	El acceso a un programa de control también presenta la oportunidad de clonar máquinas virtuales existentes como medio para duplicar y acceder a datos corporativos confidenciales	Una máquina virtual clonada podría fácilmente copiada a medios extraíbles, como un dispositivo USB.	Aplicar las políticas de seguridad que definen la configuración de los controles de acceso al programa de control, con el fin de protegerlo contra su manipulación y monitoreo

Tabla 6.1: Ataques al programa de control

Los riesgos asociados con el programa de control requieren que los mecanismos de seguridad en cada plataforma virtual sean revisados cuidadosamente durante el proceso de diseño y evaluación de la misma [47]. Adicionalmente, se deben crear y hacer cumplir políticas de seguridad y gestión que consideren el acceso y administración del programa de control.

Los vendedores de plataformas de virtualización trabajan para eliminar código innecesario en sus programas de control y/o consolas de gestión, de manera de limitar la exposición de sus productos a vulnerabilidades de seguridad. Además, las herramientas de gestión permiten centralizar la gestión de actualizaciones, de manera de automatizar dicho proceso cuando sea necesario.

En definitiva, se requiere de toda una metodología que se base en el análisis y administración de los riesgos de seguridad de este componente para poder asegurar la plataforma virtual. Se pueden contar con políticas y procedimientos de seguridad para máquinas virtuales, pero no se deben descuidar los riesgos asociados al programa de control.

6.4.1. Autenticación

Con respecto a la autenticación, si bien todos los medios tradicionales para la misma se siguen aplicando en un entorno virtual, los controles de la virtualización relacionados con la autenticación de administradores para el control de máquinas virtuales y gestión de la plataforma entera, es un elemento clave.

La gestión de autenticación de administradores puede hacerse compleja rápidamente, dependiendo de la asignación de credenciales, considerando controles en máquinas virtuales en la cual, el acceso pueda ser otorgado directamente a través de la línea de comando, una línea de comando remota, una conexión segura SSH, vía una interfaz web ó a través de una herramienta en particular.

La organización debe ser capaz de rastrear la autenticación de usuarios y controlar el acceso, llevando a cabo las actividades de auditoría en aplicaciones y registros correspondientes [48].

6.4.2. Estado de la información

La información con respecto a la configuración de arranque, migraciones de máquinas virtuales, información de estado e información relacionada con las políticas de seguridad, debe ser asegurada de manera recurrente. Dado que las máquinas virtuales son sistemas dinámicos y móviles, la gestión adecuada de la integridad en la configuración de cada una de ellas, así como el manejo de la información de estado, ayuda a reducir los casos en los que puedan ser vulnerables a ataques de suplantación, intercepción ó reescritura de información crítica.

6.4.3. Seguridad en la red virtual

La seguridad en la red virtual es otro de los aspectos que juega un papel crítico en el entorno virtual, por lo que deben ejecutarse planes de seguridad que eviten comprometer la integridad y confiabilidad de las comunicaciones entre máquinas virtuales y dispositivos de red.

Cada entorno virtual debe esperar que las siguientes funciones de seguridad de red sean incluidas en la plataforma, de manera de aprovecharlos de manera más adecuada:

- Habilitar uno o varios puertos para monitoreo en cada conmutador virtual, con el fin de integrar un sistema de detección de intrusos virtuales
- Capacidad de conectar una subred de manera segura, a través de múltiples hosts
- Gestión de conmutadores virtuales

6.5. Mejores prácticas para virtualizar

Finalmente, la estabilidad y buen funcionamiento de los componentes de la virtualización dependerán de los mecanismos de seguridad ejecutados durante el proceso de instalación y configuración de las soluciones utilizadas, así como el uso de las herramientas de gestión. A continuación se recopilan una serie de lineamientos que deben seguirse en una infraestructura virtual, de acuerdo a los procedimientos ejecutados durante el desarrollo de este proyecto.

6.5.1. Consideraciones en hardware

Las consideraciones del hardware están orientadas a la implementación y configuración de la plataforma que sostiene la virtualización. Las mismas pueden ser usadas para estudiar la compatibilidad de los componentes y asegurar su correcto funcionamiento.

- **Procesador**

Se pueden aprovechar las funcionalidades adicionales que ofrezca la tecnología de procesadores adoptados. Por ejemplo, los procesadores más recientes incluyen funciones para asistir en la virtualización, conocida como asistencia de hardware en la virtualización de MMU (*hardware-assisted MMU virtualization*, en inglés), una característica que aumenta el rendimiento de los sistemas virtualizados [49].

Casos particulares son las funciones VT-x de procesadores Intel ó AMD-V de procesadores AMD [50], que forman parte de una de las tecnologías que asisten en la virtualización de hardware, las cuales permiten "capturar" instrucciones y eventos que pueden inducir a la sobrecarga de los sistemas. Estas funciones pueden ser habilitadas para reducir el consumo de memoria y acelerar el procesamiento de cargas de trabajo de los sistemas operativos invitados.

- **Almacenamiento**

La buena gestión en la configuración del espacio puede afectar satisfactoriamente el rendimiento de los sistemas, particularmente en el rendimiento del almacenamiento, un concepto que depende de factores como la carga de trabajo, hardware, vendedores, niveles RAID, tamaño de cache, entre otros.

Muchas cargas de trabajo son muy sensibles a la latencia en operaciones de entrada y salida, por lo que es importante configurar adecuadamente los dispositivos de almacenamiento, sobre todo si se trabaja sobre una red de almacenamiento SAN ó bajo dispositivos NAS.

El planteamiento de un mejor rendimiento en una red de almacenamiento debe tomar en cuenta los componentes físicos de la red y no las locaciones lógicas [51]. Por ejemplo, el uso de redes virtuales (VPNs ó VLANs) no representa una solución adecuada al problema de compartición de recursos. Aunque permiten configurar lógicamente una red, no se toman en cuenta al considerar las capacidades físicas de enlaces y troncales entre conmutadores. Sin embargo, permiten la incorporación de calidad de servicio (QoS), una función que permite disponer de ancho de banda preferencial o proporcional a cierto tipo de tráfico.

Con respecto al uso de canales de fibra, se debe asegurar el uso de una velocidad de transmisión punto a punto consistente a fin de evitar inconvenientes en el rendimiento, configurando niveles máximos de encolamiento en las tarjetas HBA.

Las aplicaciones ó sistemas que requieran grandes cantidades de datos en el almacenamiento usando enlaces Ethernet con dispositivos de almacenamiento, tal y como la adquisición de datos o transacciones de registro entre sistemas, no deben compartir sus enlaces con otras aplicaciones o sistemas. Este tipo de aplicaciones adquieren un mejor rendimiento usando conexiones dedicadas con los dispositivos de almacenamiento.

Para iSCSI y NFS, se debe asegurar una topología de red Ethernet que no contenga cuellos de botella que provoque el descarte de paquetes. La recuperación del descarte de paquetes de red resulta en una notable degradación en el rendimiento. En adición al tiempo invertido en determinar los datos desechados, la retransmisión de los mismos usa un ancho de banda de red que puede ser usado en otro tipo de transacciones.

El rendimiento del almacenamiento local puede mejorarse con una cache de escritura hacia atrás (*write-back cache*, en ingles). Si se encuentra instalada, la misma debe habilitarse.

Se debe asegurar que los adaptadores de almacenamiento estén instalados en ranuras con suficiente ancho de banda, tomando en cuenta la arquitectura de buses (en muchos casos, ciertas arquitecturas son similares pero incompatibles entre sí). Los adaptadores de alto rendimiento generalmente funcionan adecuadamente en ranuras diseñadas para PCI tradicionales, pero su máximo rendimiento puede limitarse, siendo un caso particular de atención cuando se trate de soportar cargas de trabajo que requieran de altos rendimiento en operaciones de entrada y salida, por ejemplo.

- **Red**

Se debe considerar el uso de tarjetas de interfaz de red (NICs) diseñadas para servidores para mejores rendimientos. Asegurándose de que la infraestructura de red entre las tarjetas origen y destino no introduzca cuellos de botella. Por ejemplo, si ambas NICs son de 10 Gbps, se debe asegurar que todos los cables y conmutadores tengan las mismas capacidades en velocidad de transmisión ó que no estén configurados con velocidades diferentes.

En algunos adaptadores de red Ethernet de 10 Gbps y dependiendo de la tecnología de virtualización usada, se puede soportar NetQueue, una tecnología que mejora significativamente su rendimiento en ambientes virtualizados. Asegurándose de que las tarjetas de red estén instaladas en ranuras con suficiente ancho de banda que soporte su máximo rendimiento.

El uso de múltiples adaptadores de red entre un único conmutador virtual y una red física constituye un conjunto NIC. Un conjunto NIC puede facilitar una recuperación sencilla ante una falla de hardware o un corte de red. Dependiendo de su configuración, puede aumentar el rendimiento distribuyendo el tráfico a través de los adaptadores físicos de red.

- **BIOS**

Se debe asegurar que se esté ejecutando la versión más reciente del BIOS disponible para el sistema físico usado. Luego de actualizar el BIOS, se deben revisar sus opciones en caso de que nuevas funciones se encuentren disponibles o la disposición de opciones anteriores cambie.

Asegurarse de que la concurrencia en hilos de ejecución esté habilitada en el BIOS para procesadores que lo soporten. Además de habilitar las funciones de virtualización de hardware asistida, tales como: VT-x, AMD-V, EPT, RVI, entre otras.

Deshabilitar aquellos dispositivos que no se usen. Como por ejemplo, aquellos puertos seriales, puertos USB ó puertos de red sin usar.

Algunos software para virtualizar tales como VMware ESXi, incluyen capacidades para la gestión de energía permite ahorrar energía en un sistema que no esté en uso en su totalidad. Se recomienda configurar el BIOS para permitir que el software para virtualizar controle todo lo relacionado a la gestión de energía de los sistemas.

6.5.2. Consideraciones en el programa de control

El programa de control es la base que sostiene todos los ambientes virtuales ya que gestiona los cuatro recursos principales de los sistemas, como lo son procesadores, memoria, almacenamiento y red. Por ello requiere de una especial atención en su implementación y configuración, con el fin de garantizar un entorno operativo funcional con el menor riesgo posible.

- **Generales**

El proceso de instalación de un programa de control inicialmente puede hacerse bajo la metodología del ensayo y error, sobre todo en caso de que no se cuente con la suficiente experticia al respecto. Es por ello que se sugiere documentar cada paso llevado a cabo, de manera de poder perfeccionar el proceso en futuras implementaciones.

Antes de instalar, deben conocerse las etapas fundamentales del proceso a fin de prepararse en la elección de diferentes opciones de configuración. Se sugiere identificar por adelantado, la unidad de almacenamiento en donde será dispuesto el hypervisor, identificándolo a través de su LUN y capacidad. Dicha unidad debe ser local al host, de manera de no comprometer el almacenamiento compartido.

La configuración de parámetros de red, tales como direcciones IP y nombres de identificación deben hacerse de manera inmediata, al momento de culminar el proceso de instalación. Se sugiere el uso de direcciones IP estáticas, así como la integración en un dominio de red (Por ejemplo, los sistemas ESXi cuentan con servicios de sincronización con Active Directory), aislándolos de políticas de grupos especificas, en caso de que estas influyan en el funcionamiento de los mismos.

Las credenciales administrativas locales deben ser configuradas por el administrador encargado de la seguridad de activos de información ó afines, el cual es el encargado de su resguardo y modificación en un periodo de 45 a 90 días. De ser incluido en un dominio de red, el acceso de los administradores debe hacerse con sus respectivas credenciales de dominio, habilitando funciones de auditoría constantes para registrar los cambios realizados. Por lo que la cuenta administrativa local sólo debe usarse para tareas críticas.

Por otra parte, se pueden considerar mecanismos adicionales para restringir el acceso a las interfaces de gestión de los programas de control. La creación e instalación de certificados de seguridad es una de ellas, en caso de contar con una herramienta de administración web, muy común en los últimos años.

El proceso de actualización y de aplicación de parches de seguridad es una tarea constante que debe tomarse en consideración. Se puede hacer uso de funcionalidades que automaticen este proceso, aunque se recomienda conocer los mecanismos manuales para su aplicación en caso de una contingencia. Su aplicación puede incurrir en cambios drásticos en las configuraciones iniciales, por lo que se recomienda realizar respaldos antes de cualquier aplicación de parches o actualizaciones.

- **Hardware**

Planear la implementación con suficientes recursos para todas las máquinas virtuales a ejecutar, así como aquellos necesitados por el programa de control como tal. Asignar a cada máquina virtual de tanto hardware virtual como sea requerido, previéndolas con más recursos de lo solicitado.

Desconectar o deshabilitar cualquier dispositivo físico que no se use. Esto puede incluir dispositivos como: puertos COM y LTP, controladores USB y de CD / DVD, Interfaces de red y controladores de almacenamiento. Deshabilitar dispositivos de hardware (generalmente realizado en el BIOS) puede evitar la interrupción de recursos. Adicionalmente, algunos dispositivos como controladores USB operan bajo un esquema de encuesta que consumen recursos de CPU adicionales. Por otra parte, algunos dispositivos PCI reservan bloques de memoria, los cuales no estarán disponibles para el programa de control.

Los dispositivos de hardware virtuales sin usar o innecesarios pueden comprometer el rendimiento y deben ser deshabilitados. Por ejemplo, un sistema operativo invitado Windows consulta frecuentemente sobre la presencia de unidades de CD ó DVD. Cuando las máquinas

virtuales se configuran para usar una unidad física y múltiples sistemas invitados intentan acceder simultáneamente a esa unidad, el rendimiento puede sufrir. Este impacto puede reducirse configurando las máquinas virtuales para que usen imágenes ISO en lugar de usar unidades físicas, deshabilitando las mismas cuando no sean requeridas.

- **Procesamiento**

La virtualización de CPU incluye una cantidad de sobrecarga que depende del porcentaje de carga de trabajo de las máquinas virtuales que pueden ejecutarse en el conjunto de procesadores físicos. Para muchas cargas de trabajo, la virtualización de CPU adiciona solo una cantidad mínima de sobrecarga, lo que da como resultado un rendimiento casi nativo.

Muchas cargas de trabajo a las que la virtualización de CPU adiciona sobrecarga no están limitadas por CPU, dado que pasan la mayor parte del tiempo esperando por eventos externos tales como interacción del usuario, entrada de dispositivos ó recuperación de datos. Debido a que otros ciclos de CPU estarán disponibles para "absorber" la sobrecarga de virtualización, estas cargas de trabajo tendrán un rendimiento similar a si fuesen nativas, pero potencialmente con un ligero incremento de latencia. Para un pequeño porcentaje de carga de trabajo para el cual la virtualización de CPU adiciona sobrecarga y que están limitados por CPU, tendrán una degradación notable tanto en rendimiento como en latencia.

Dependiendo del programa de control, se pueden permitir la ejecución de más CPU virtuales en un host, independientemente del número de procesadores físicos presentes en dicho host, sin alterar el rendimiento de las máquinas virtuales. Si un host se satura a nivel de CPU (es decir, las máquinas virtuales y demás cargas en el host demandan todos los recursos de CPU disponibles), las cargas de trabajo sensibles a latencia no podrán ejecutarse correctamente. En este caso, se puede reducir la carga de CPU, por ejemplo, apagando algunas máquinas virtuales ó migrarlas a diferentes hosts. Por lo que se recomienda monitorear periódicamente el uso de CPU en el host.

Configurar una máquina virtual con más procesador virtual que sus cargas de trabajo puedan usar puede causar un incremento ligero en el uso de recursos, potencialmente impactando el rendimiento de los sistemas más cargados. Un ejemplo común es la inclusión de una carga de trabajo de un único hilo de ejecución en una máquina virtual con múltiples procesadores virtuales ó una carga de trabajo con múltiples hilos de ejecución en una máquina virtual con más procesadores virtuales de los que la carga de trabajo pueda usar.

Incluso si el sistema operativo invitado no utiliza algunos de sus procesadores virtuales, configurar máquinas virtuales con dichos procesadores sigue imponiendo ciertos requerimientos de recursos en el programa de control para traducir el consumo real de CPU en el host. Por ejemplo:

- Los procesadores virtuales sin usar consumen interrupciones del temporizador en algunos sistemas operativos invitados.

- Mantener una vista consistente de memoria entre múltiples procesadores virtuales puede consumir recursos adicionales tanto en el programa de control como en los sistemas operativos invitados, aunque la virtualización de MMU asistida por hardware reduce significativamente reduce este costo.

- Los planificadores en los sistema operativos invitados deben migrar a cargas de trabajo con un único hilo de ejecución entre múltiples procesadores virtuales, perdiendo así la localidad de la cache.

La capacidad de sostener múltiples hilos de ejecución permite que un único procesador físico pueda comportarse como dos procesadores lógicos, específicamente, permite la ejecución simultánea de dos hilos concurrentes. A diferencia de tener dos procesadores, que pueden doblar

el rendimiento, múltiples hilos de ejecución pueden proveer un incremento significante del rendimiento del sistema sin alterar el funcionamiento del procesador. Para un mejor rendimiento, se recomienda habilitar la ejecución de múltiples hilos, asegurándose de que el sistema soporte esta tecnología. Si no es suficiente con el procesador, se puede habilitar en el BIOS.

La mayoría de los programas de control gestionan el tiempo de procesamiento de manera inteligente para garantizar que la carga es distribuida sin inconvenientes a través de todos los núcleos físicos en el sistema. Si no hay carga para un determinado procesador lógico, este es detenido para liberar recursos en ejecución, permitiendo que máquinas virtuales que se ejecuten en otro procesador lógico del mismo núcleo pueda utilizar dichos recursos.

- **Memoria**

La virtualización causa un incremento entre la memoria física requerida y la cantidad de memoria extra requerida por el programa de control para su propio código y estructuras de dato. En el caso de VMware ESXi, este requerimiento adicional de memoria puede separarse en dos formas:

- Espacio de memoria amplio para el VMkernel y demás agentes
- Espacio adicional de memoria para cada máquina virtual

El espacio de memoria dedicado a cada máquina virtual puede ser dividido de la siguiente manera:

- Memoria reservada para el proceso de ejecución de máquina virtual.
- Memoria reservada para el monitor de máquinas virtuales.
- Memoria reservada para varios dispositivos virtuales.
- Memoria reservada por otros subsistemas, como el kernel, agentes de gestión, entre otros.

La cantidad de memoria reservada para estos propósitos depende de una variedad de factores, incluyendo el número de procesadores virtuales, la memoria configurada en los sistemas operativos invitados y si estos son de 32 ó 64 bits, además de las funciones habilitadas en cada máquina virtual.

Se debe alocar suficiente memoria para mantener en funcionamiento en conjunto de aplicaciones a ejecutar en una máquina virtual, minimizando su desperdicio. Evitando la sobre-asignación de memoria. Asignar más memoria de la necesaria no incrementa su sobrecarga en máquinas virtuales necesariamente, pero esta puede ser consumida en lugar de ser usada para soportar una mayor cantidad de máquinas virtuales.

Con el fin de reducir dinámicamente la cantidad de memoria física requerida por cada máquina virtual se pueden usar los siguientes mecanismos de gestión:

- Compartición de páginas, una técnica que permite compartir paginas de memoria entre máquinas virtuales de manera segura y transparente, eliminando copias redundantes de páginas de memoria. En la mayoría de los casos, la compartición de páginas es usada por defecto sin tener en cuenta la demanda de memoria en el host.

- Ballooning. Si el uso de memoria de una máquina virtual es consistente con su objetivo, el programa de control puede usar esta técnica para reducir la demanda de memoria en máquinas virtuales haciendo que los sistemas invitados renuncien a las páginas de memoria consideradas como menos valiosas. La técnica de ballooning provee niveles de rendimiento cercanos a los alcanzados en un sistema nativo bajo limitaciones de memoria similares. Para usarla, el sistema operativo invitado debe estar configurado con suficiente espacio intercambiable.

- Comprensión de memoria. Si el uso de memoria de una máquina virtual aprovecha el nivel requerido en el intercambio de host, el programa de control usa la comprensión de memoria para reducir el número de página de memoria necesario para el intercambio. Debido a que la latencia involucrada en la descomprensión es mucho más pequeña que la latencia en un intercambio, la comprensión tiene un menor impacto significativo en el rendimiento.

- Intercambio a la cache del host. Si la comprensión de memoria no mantiene el uso de memoria por parte de máquinas virtuales en un nivel lo suficientemente bajo, el programa de control reclamará de manera forzosa el uso de memoria destinado al intercambio de host a la cache de dicho host.

- Intercambio tradicional basado en host. Si la cache del host se llena ó si la misma no ha sido configurada, el programa de control reclamará memoria de la máquina virtual intercambiando páginas a un archivo de intercambio tradicional. Como sucede en el intercambio a la cache del host, algunas de las páginas intercambiadas estarán activas. Sin embargo, la diferencia es que este mecanismo puede comprometer el rendimiento de máquinas virtuales, degradando significativamente ya que introduce altos niveles de latencia.

Mientras que el programa de control use la compartición de páginas, la técnica de ballooning, la comprensión de memoria y haga intercambio con la cache del host para permitir un sobre alojamiento de memoria significante con o sin impacto sobre el rendimiento, se debe evitar el sobre alojamiento de memoria al punto de activar las páginas de memoria que son intercambiadas tradicionalmente a través del host.

- **Almacenamiento**

El programa de control por lo general cuenta con un gran alcance respecto a los volúmenes de almacenamiento disponibles, tanto locales como compartidos en una red SAN, por ejemplo. Se sugiere que la gestión de los mismos no dependa solamente del hypervisor, sino que también se incorporen las herramientas de gestión propias de la plataforma de hardware que los aloje.

Por ejemplo, la disposición de dispositivos de almacenamiento debe gestionarse a nivel de host, de manera de poder darles el formato adecuado (por ejemplo, se puede usar un formato RAID-5 para redundancia de información, aportando en los procedimientos de respaldo y recuperación). De esta manera se puede contar con un pool de almacenamiento compartido, que puede dividirse en volúmenes. La creación, expansión, reducción y mapeo de hosts de diferentes volúmenes de almacenamiento puede ser fácilmente responsabilidad de las herramientas de gestión de hosts, la interfaz web del Storage Configuration Manager del IBM BladeCenter es un ejemplo de ello.

Por otra parte, la gestión del almacenamiento local puede correr por cuenta del hypervisor, el cual puede tomar control total sobre el sistema de archivos usado, lo que facilita la gestión de máquinas virtuales, en caso de que estas se alojen de manera local. Desde el punto de vista de un administrador, la gestión del almacenamiento local puede restringirse a recopilar información del mismo en términos de capacidad y contenido, o por otra parte, ejercer control absoluto sobre configuraciones particulares sobre el sistema de archivos, en la medida que la tecnología de virtualización lo permita.

Particularmente, ESXi establece un sistema de archivos propio, conocido como VMFS, el cual puede ser manipulado por un administrador a través de una consola de usuario, accedida vía SSH ó PowerShell. Este sistema está basado en Linux, por lo que su administración a este nivel, puede ser bastante útil en análisis forenses luego de una contingencia.

Adicionalmente, dicho sistema operativo soporta el mapeo de dispositivos de formato RAW (conocido como RDM), los cuales permiten la gestión y acceso a discos SCSI de formato RAW ó

discos LUNs bajo un sistema de archivos VMFS. El mapeo RDM consiste en un archivo especial sobre un volumen VMFS que actúa como un proxy para dispositivos RAW.

El archivo RDM contiene metadatos usados en la gestión y redirige el acceso de discos a los dispositivos físicos. El sistema de archivos VMFS tradicional es recomendado para la mayoría del almacenamiento virtual en disco, pero los discos en formato RAW pueden ser requeridos en ciertos casos.

Se puede usar un mapeo RDM en un modo de compatibilidad virtual ó físico, de acuerdo a lo siguiente:

- Un modo de compatibilidad virtual requiere de una virtualización completa del dispositivo mapeado, permitiendo al sistema operativo invitado tratar el RDM como cualquier otro disco virtual en un volumen VMFS, habilitando el uso del mismo.

- Un modo de compatibilidad físico requiere de una mínima virtualización SCSI en el dispositivo mapeado, permitiendo mayor flexibilidad para aplicaciones de gestión SAN ó demás aplicaciones SCSI ejecutándose en la máquina virtual.

- **Red**

En un ambiente nativo, el uso de CPU juega un rol importante en el rendimiento de la red. Para procesar altos niveles de rendimiento se requiere un número mayor de recursos de procesamiento. El efecto de la disponibilidad de recursos con respecto al rendimiento de una red con aplicaciones virtuales es mucho mayor. Naturalmente, la insuficiencia de recursos de CPU limita el rendimiento, por lo que es importante monitorear el uso de recursos de procesamiento en cargas de trabajo de alto rendimiento en red.

En caso de que una tarjeta NIC física sea compartida para múltiples consumidores (máquinas virtuales y/o el programa de control), el rendimiento de los mismos se verá afectado. Así que, para garantizar un rendimiento adecuado de red, se deben usar diferentes NICs físicas para consumidores con altos requerimientos de entrada y salida, así como aquellos con cargas de trabajo sensibles a latencia. Sin embargo, existen casos particulares a los que esta sugerencia no aplica, tal es el caso de las NICS de 10 Gbps, las cuales soportan múltiples colas de transmisión, hacen posible la alternativa de separar el consumo de red en diferentes colas

Para establecer una conexión de red entre dos máquinas virtuales que residen en un mismo host, las mismas deben conectarse al mismo conmutador virtual. Si las máquinas virtuales se conectan a diferentes conmutadores, el tráfico puede incurrir a una demanda excesiva de procesamiento y red.

6.5.3. Consideraciones en máquinas virtuales

Para efectos de este documento, el término máquina virtual se refiere a sistemas alojados sobre el programa de control y que funcionan como servidores virtuales de la organización, ofreciendo una serie de servicios a través de las aplicaciones instaladas. Del mismo modo, requieren de configuraciones particulares que garanticen su correcto funcionamiento durante el periodo en que sean dispuestas en la infraestructura de la organización.

- **Generales**

En principio debe tomarse en cuenta que la creación de máquinas virtuales puede convertirse en un vicio, por lo que si no se restringe de algún modo, rápidamente el centro de datos virtual puede convertirse en una estructura desorganizada, lejos del cumplimiento de las mejores prácticas.

Es así como la creación, modificación y eliminación es un proceso que debe ser supervisado y aprobado bajo una estructura de control de cambios, que permita registrar las modificaciones realizadas de manera particular y general en referencia al centro de datos virtual.

Por otra parte, se sugiere usar un sistema operativo que sea soportado por el programa de control instalado en el sistema host. Particularmente, en caso de usar ESXi de VMware, los sistemas invitados deben tener instalada la versión más reciente de VMware Tools, un conjunto de herramientas que facilitan la comunicación y gestión de los mismos con respecto al host.

A pesar de que en muchas ocasiones, una organización busca consolidar un conjunto de servidores en base al uso de plantillas reutilizables con sistemas operativos estandarizados, la virtualización permite incursionar en las "pruebas" de nuevos sistemas operativos, siempre y cuando el programa de control lo permita. Lo importante es consolidar estos sistemas en el entorno operativo adecuado y garantizar la seguridad de las demás máquinas virtuales.

La inclusión de máquinas virtuales en el dominio de red debe hacerse durante su fase de pruebas, de manera de poder identificar inconvenientes y la manera de solventarlos con respecto a la aplicación de políticas de dominio, reglas de firewall, mecanismos de autenticación, etc. Sobre todo, si su disposición forma parte de un proyecto con tiempos de culminación estrictos.

Se recomienda deshabilitar protectores de pantalla y animaciones (en el caso de Windows) en máquinas virtuales. En caso de Linux, si no se requiere un X-server, el mismo debe ser deshabilitado. Estas opciones consumen recursos de procesamiento adicionales que potencialmente pueden afectar las proporciones en consolidación y rendimiento de máquinas virtuales.

Planificar respaldos y programas de escaneo de virus en máquinas virtuales que sean ejecutados fuera de las horas pico, evitando que la planificación de los mismos se haga de manera simultánea. En general, es una buena idea distribuir, eventualmente, el uso de CPU, no en función de procesamiento sino en función de tiempo.

Para cargas de trabajo cuyo análisis de virus y respaldo sea de alguna manera predecible, es sencillo planificarlos adecuadamente. Adicionalmente, se puede considerar la configuración de máquinas virtuales para usar NTP, Windows Time Service ó alguna otra opción que permita sincronizar la fecha y hora de los sistemas.

- **Procesamiento**

Particularmente, las máquinas virtuales con multiprocesamiento asimétrico (SMP) pueden migrar procesos de un procesador virtual a otro. Sin embargo, esta migración puede incurrir en una baja sobrecarga de procesamiento. En caso de que las migraciones sean frecuentes, se pueden consultar los hilos de ejecución ó procesos en un procesador en específico (Siendo esta situación, otra razón por la cual no se recomienda configurar una máquina virtual con más procesadores virtuales de los que realmente necesita).

Al crear máquinas virtuales, se cuenta con la opción de especificar el número de sockets virtuales y el número de núcleos por socket virtual. En general, se recomienda usar las opciones por defecto a un núcleo por socket, asumiendo que el número de sockets virtuales es igual al número de procesadores virtuales.

- **Almacenamiento**

Se recomienda almacenar los archivos propios de sistema operativo en el almacenamiento local del host, mientras que los datos e información usados por la aplicación y los servicios alojados se mantengan el almacenamiento compartido, bajo constantes procedimientos de respaldo.

Las implementaciones de máquinas virtuales pueden ser sometidas a constantes control de versiones (*snapshots*, de acuerdo a la terminología de VMware), lo que asegura una recuperación ante una contingencia.

Los adaptadores de almacenamiento por defecto pueden variar entre BusLogic Parallel, LSI Logic Parallel ó LSI Logic SAS, dependiendo del sistema operativo invitado y la versión del hardware virtualizado. Particularmente, ESXi incluye un adaptador de almacenamiento SCSI paravirtualizado: PVSCSI (también llamado VMware Paravirtual). Este adaptador reduce significativamente el uso de CPU así como incrementa el rendimiento comparado con demás adaptadores virtuales, por lo que puede ser la mejor opción en ambientes con altas demandas de entrada y salida.

La manera en como los controladores SCSI de un sistema operativo invitado gestionan el encolamiento de peticiones puede impactar de manera significativa el rendimiento de los discos. La profundidad de una cola es muy pequeña, por lo que puede limitar el ancho de banda de un disco dispuesto en una máquina virtual.

En algunos casos, las peticiones largas de entrada y salida de aplicaciones en máquina virtuales pueden separarse por el controlador de almacenamiento. Sin embargo, cambiar las configuraciones de registro en los sistemas invitados con el fin de reducir el tamaño de bloques de peticiones puede ser una alternativa ante la separación de las mismas, mejorando así el rendimiento.

Finalmente, se debe asegurar que las particiones de discos de invitados se encuentren alineadas. Para mayor información, se puede consultar la documentación asociada al sistema operativo invitado usado con el fin de usar las herramientas adecuadas en la gestión de particiones.

- **Funcionalidades**

La consolidación de máquinas virtuales como servidores puede traer consigo un conjunto de procedimientos automatizados dedicados a explotar las funcionalidades propias de la virtualización. Un ejemplo de ello es la recuperación ante desastres, una de las ventajas inmediatas de mantener máquinas virtuales en ejecución. Para garantizar una adecuada recuperación, se sugiere realizar respaldos constantes de la configuración y datos de las mismas, de manera de poder contar con los recursos necesarios para la disposición de un centro de datos virtual alterno ante una contingencia.

Otra de las ventajas en la migración en caliente, una característica muy común en términos de máquinas virtuales, la cual es soportada principalmente por el programa de control y que sostiene el concepto de portabilidad. La migración de un entorno a otro puede hacerse durante horas laborales, ya que no altera el funcionamiento de las aplicaciones y servicios ofrecidos a los usuarios de una organización que los use. Sin embargo, se recomienda llevar a cabo este proceso durante horas no laborales, de manera de considerar el caso en que una falla pueda ocurrir.

La auditoría es un proceso bastante útil que puede aprovecharse en el establecimiento de políticas de seguridad en ambientes virtuales, fundamentado en las aplicadas en los sistemas físicos. Un proceso de auditoría en los diferentes entornos operativos permitirá recopilar información referente a sesiones iniciadas, tareas ejecutadas y cambios realizados, permitiendo un control con un alcance amplio sobre la gestión de los sistemas. Se recomienda realizar estos procedimientos de manera constante, dependiendo de la categorización de riesgo asociada al servidor y aplicaciones alojadas.

6.5.4. Consideraciones en la infraestructura virtual

Mientras que las máquinas virtuales representan la disposición de recursos en un único sistema, la infraestructura virtual corresponde a la disposición de recursos en todo el entorno de tecnologías de información, agrupando tanto servidores, red y almacenamiento en una unificación de componentes propios de la arquitectura de comunicaciones de la organización. La adecuada gestión de la infraestructura virtual permite una eficiente consolidación de servidores, así como maximizar el ciclo de vida de las aplicaciones y la continuidad de negocio.

Toda infraestructura para virtualizar cuenta con diversos mecanismos para permitir la configuración y asignación de recursos de procesamiento y memoria para las máquinas virtuales que se estén ejecutando en la misma. La gestión y configuración de los recursos puede tener un impacto significativo en el rendimiento de las máquinas virtuales.

Utilizar las funciones y opciones del programa de control para la gestión de recursos sólo cuando sea necesario. Entre estas funciones se encuentran la reservación, compartición y limitación de recursos. Si se esperaran cambios frecuentes en la disponibilidad total de recursos, se sugiere usar la compartición de los mismos y no la reservación, de manera de asignar los recursos lo bastante justa en torno a las máquinas virtuales. Si se usa la compartición de recursos y el hardware es sometido a frecuentes actualizaciones, cada máquina virtual debe contar con un mismo nivel de prioridad relativo (manteniendo el mismo número de recursos compartidos), a pesar de que cada acción represente una gran cantidad de memoria y procesamiento.

La reservación de recursos permite especificar una cantidad mínima aceptable de procesamiento ó memoria, no la cantidad que se quisiera tener disponible. Luego de la consolidación de todas las reservaciones de recursos, el programa de control debe estar capacitado para disponer de los recursos disponibles basado en el número de comparticiones y la limitación de los recursos, previamente configurados en cada máquina virtual.

Como se indico anteriormente, la reservación de recursos puede ser usada para especificar un mínimo de procesamiento ó memoria reservado para cada máquina virtual. En contraste con la compartición, la cantidad de recursos reservados no cambia al migrar de ambiente (agregar o remover máquinas virtuales, por ejemplo). No se recomienda configurar altos niveles de reservación, ya que puede limitar el número de máquinas virtuales que pueden hacer uso de un conjunto de recursos, clúster ó host.

Al especificar las reservaciones de máquinas virtuales, es recomendable disponer de un mínimo para controlar los desbordamientos de memoria y migraciones. Si se cuenta con un clúster que albergue diversos hosts, las reservaciones que se consoliden ocupando la capacidad total del mismo ó de cada host albergado, pueden evitar la migración de máquinas virtuales entre hosts. Naturalmente, si se reservan todos los recursos de un sistema, la dificultad de realizar cambios aumenta.

Adicionalmente, se recomienda usar los pools de recursos para delegar la gestión de recursos, agrupando las máquinas virtuales para múltiples niveles de servicio en dichos pools. Esto permite que los recursos sean dispuestos como un todo.

6.6. Recomendaciones finales

A continuación se exponen un conjunto de recomendaciones de seguridad que engloban los planteamientos más destacados y que componen la estrategia desarrollada en este documento:

- Asegúrese de que todos los procedimientos de seguridad establecidos por la organización, incluyan la actualización de los sistemas.

- Implemente seguridad en la red para aislar el tráfico en máquinas virtuales. Un modelo híbrido que combine máquinas virtuales con diferentes niveles de criticidad en un mismo host puede ser una opción, el tráfico puede trasmitirse a través de diferentes tarjetas de red físicas que pasen por un firewall físico.

- Deshabilite los servicios no utilizados en los sistemas operativos y desconecte los dispositivos físicos que no se necesiten.

- Monitoree los sistemas de manera proactiva con el fin de detectar la presencia de máquinas virtuales maliciosas, eliminarlas y determinar cómo fueron instaladas en el sistema.

- Establezca plantillas para reutilizar los sistemas operativos previamente reforzados antes de la instalación de aplicaciones.

- Aísle las redes de las máquinas virtuales. La segmentación de la red reduce el riesgo ante varios tipos de ataques y el establecimiento de una zona desmilitarizada mantiene la separación de máquinas virtuales.

- Establezca controles estrictos de seguridad sobre la capacidad de actualizar las políticas, lo que requiere una autenticación fuerte y uso de firmas digitales, asegurando la integridad y validez de la información.

- Finalmente, restringa la capacidad de los administradores para disponer de software arbitrario con respecto a la seguridad, la gestión y otros componentes críticos.

La estrategia desarrollada se basa en la necesidad de reducir el riesgo asociado a los amenazas de seguridad que se presentan al consolidar un proyecto de virtualización de servidores en una organización. Este documento pretende ser una guía que una organización con una pequeña, mediana ó gran infraestructura tecnológica pueda entender los riesgos asociados a la virtualización de servidores y a la importancia de la seguridad de la información en todas y cada una de las fases de implantación del proyecto.

7. Conclusiones

En este trabajo se desarrolló una estrategia para la virtualización de servidores basada en las mejores prácticas y en el uso de tecnologías presentes en el mercado actual. La consolidación de este proyecto permitió orientar a una empresa en particular en la incorporación de la tecnología de virtualización dentro de un ambiente fundamentado en un esquema de servidores físicos, permitiendo un crecimiento en términos de innovación y mejor aprovechamiento de los recursos tecnológicos.

La culminación de este proyecto permitió alcanzar los objetivos planteados, gran parte de ello se debe a que los procedimientos llevados a cabo durante la fase de instalación y configuración de las tecnologías de virtualización adoptadas fueron documentados, permitiendo generar una base de datos de conocimiento para futuras implementaciones.

De esta manera, el capital invertido por la organización es retribuido en conocimiento por parte del personal de tecnologías de información. Así como la recopilación de información de la infraestructura original permitió desarrollar una documentación que funciona a manera de inventario de servidores, aplicaciones y recursos, mejorando la gestión de los mismos al centralizar toda esta información en un documento propiedad de la respectiva gerencia.

7.1. Logros alcanzados

Los logros alcanzados en este trabajo son:

- Migración de un conjunto de servidores de propósito general de una organización, a partir de un ambiente físico a un ambiente virtual, consolidándolos como máquinas virtuales con recursos compartidos en diferentes entornos operativos.

- Implementación de nuevos servicios en una organización directamente en una plataforma virtual, asegurando el crecimiento de la infraestructura en términos de cantidad de servicios y aplicaciones.

- Análisis de resultados en términos de recursos de procesamiento, memoria, red y almacenamiento de cada servidor virtual. Consolidando las ventajas de los ambientes virtuales con respecto a los servidores físicos.

- Desarrollo de una planificación basada en el establecimiento de objetivos, estudio de tecnologías y delegación de actividades divididas en etapas, siguiendo una metodología organizacional que permite desarrollar e implementar un proyecto de virtualización exitoso.

- Establecimiento de una serie de pautas, consideraciones, afirmaciones y sugerencias que dan origen a un marco estratégico destinado a las empresas y que pretende orientar a las mismas en la adopción de tecnologías de virtualización de la manera más adecuada, segura, confiable y eficiente.

- Definición de un conjunto de mejores prácticas diseñadas para asistir en el proceso de virtualización de servidores de una organización con el fin de asegurar el establecimiento de una plataforma virtual segura, escalable, robusta y funcional.

7.2. Contribuciones

Las contribuciones de este trabajo se resumen en:

- Los procedimientos descritos asisten en el proceso de migración de una plataforma física a una plataforma virtual, en función de soportar un crecimiento en términos de servidores y aplicaciones por cada componente físico adoptado.

- La metodología usada consolida una serie de pautas que permiten la categorización de servidores de acuerdo a niveles de criticidad y una segregación de entornos operativos para la separación de ambientes en una plataforma virtual. Lo que fundamente la toma de decisiones en la elección de servidores candidatos a ser virtualizados.

- Las mejores prácticas para virtualización ofrecen sugerencias para el mejor aprovechamiento de los recursos de procesamiento, memoria y almacenamiento, lo que permite mejorar las prestaciones y rendimiento de los servidores virtuales.

- La estrategia desarrollada reseña diferentes modelos de gestión, resguardo y seguridad de la información, diseñados para ambientes virtuales basados en los modelos actuales y que aún siguen siendo adoptados, incluso en plataformas físicas.

7.3. Trabajo futuro

Como trabajo futuro se plantea la aplicación de los procedimientos, mecanismos y planteamientos definidos en esta estrategia en las demás oficinas de la organización, usando otras tecnologías de virtualización en el mercado, principalmente la solución ofrecida por Microsoft: Hyper-V server, en servidores tradicionales Dell. Esta implementación debe considerar las diferencias en los resultados obtenidos a fin de determinar el alcance de la estrategia, identificando puntos a mejorar y procedimientos específicos de las tecnologías seleccionadas, a fin de complementar los planteamientos presentados en este trabajo.

Tomando en consideración los planteamientos presentados, el desarrollo de una estrategia de virtualización acorde a las necesidades de una organización fundamentada bajo las mejores prácticas en términos de funcionalidad y eficiencia estructurada que tome en cuenta diferentes factores cuantitativos, cualitativos, organizacionales y relativos al comportamiento de una organización en una situación específica fue satisfactorio, la cual permitirá establecer una disciplina que obligue a los administradores de infraestructuras tecnológicas organizacionales a llevar sistemáticamente y cuidadosamente un proyecto de virtualización de servidores hacia delante, exigiendo detalles rigurosos acerca de las metas proyectadas y asignación de deberes.

Por otra parte, la tecnología de computación en la nube está tomando un protagonismo notable dentro de las tecnologías de información debido a la flexibilidad que ofrece. Particularmente, el sistema IBM BladeCenter es catalogada como una plataforma sólida para este tipo de tecnología. De esta manera, se puede plantear incursionar en la planificación de un proyecto de *cloud computing* que permita consolidar una plataforma de nube privada dedicada al acceso de información de manera rápida y eficiente, tanto para clientes externos e internos de la organización en particular.

Referencias

[1] C. Scheffy. Virtualization for dummies. Wiley publishing. 2007.

[2] G. Popek y R. Goldberg. Formal requirements for virtualizable third-generation architectures. Communications of the ACM. Julio, 1974.

[3] VMware. Server Consolidation: Reduce IT costs while maintaining control and offering choice. [En línea]. Disponible en: http://www.vmware.com/solutions/consolidation/

[4] SearchServerVirtualization. Definition: Hypevisor. [En línea]. Octubre, 2006. Disponible en: http://searchservervirtualization.techtarget.com/definition/hypervisor

[5] R.Vanover. Type 1 and type 2 hypervisors explained. [En línea]. Virtualization review. Junio, 2009. Disponible en: http://virtualizationreview.com/blogs/everyday-virtualization/2009/06/type-1-and-type-2-hypervisors-explained.aspx

[6] D.Robb. Server virtualization guide for small business. [En línea]. Small business computing. Octubre, 2011. Disponible en: http://www.smallbusinesscomputing.com/3939556/Server-Virtualization-Guide-for-Small-Business.htm

[7] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, I. Pratt, A. Warfield y R. Neugebauer. Xen and the art of virtualization: In proceedings of the ACM symposium on operating systems principles. Octubre, 2003.

[8] Microsoft. Windows server 2012: server virtualization white paper. 2012.

[9] VMware. Migrating to VMware ESXi. 2011.

[10] J. Bozman y G. Chen. Optimizing hardware for x86 server virtualization. Intel. Agosto, 2009.

[11] VMware. Performance best practices for VMware vSphere 5.1. 2012.

[12] G. Neiger, A. Santoni, F. Leung, D. Rodgers y R. Uhlig. Intel virtualization technology: hardware support for efficient processor virtualization. Intel technology journal. Agosto, 2006.

[13] Dell. Dell PowerEdge 12th generation servers. [En línea]. Disponible en: http://www.dell.com/poweredge

[14] G. Chrysos. Intel Xeon Phi coprocessor: The architecture. [En línea]. Intel Software. 2012. Disponible en: http://software.intel.com/en-us/articles/intel-xeon-phi-coprocessor-codename-knights-corner

[15] J. Loffink. Dell PowerEdge modular enclosure architecture. Dell enterprise white paper. Enero, 2008.

[16] Dell. Embedded server management: unified server Configurator. [En línea]. 2010. Disponible en: http://www.dell.com/Learn/us/en/19/solutions/unified-server-configurator

[17] HP. HP ProLiant servers. [En línea]. Disponible en: http://www.hp.com/products/servers/platforms/index.html

[18] HP. Configuring and tuning HP ProLiant servers for low-latency applications white paper. Abril, 2009.

[19] IBM. IBM BladeCenter S type 7779/8886 planning guide. Octubre, 2007.

[20] IBM. BladeCenter information center. [En línea]. Disponible en: http://publib.boulder.ibm.com/infocenter/bladectr/documentation/index.jsp

[21] VMware. Virtualization in the enterprise: how are you adapting to the current business climate? [En línea]. Disponible en: http://www.vmware.com/solutions/company-size/enterprise/

[22] VMware. VMware data recovery 2.0 evaluation guide. Junio, 2011.

[23] A. Luthra. Virtualization: Where is the ROI? [En línea]. DynamicCIO. Disponible en: http://www.dynamiccio.com/2011/11/virtualization-a-game-changer-but-where-is-the-roi.html

[24] TechNet. Virtualización: ROI y beneficios para su compañía. [En línea]. Disponible en: http://blogs.technet.com/themes/blogs/generic/virtualizacion-roi-y-beneficios-para-su-compania/

[25] M. Branscombe. HP puts 1000 cores in a single rack. [En línea]. Tom's Hardware. Junio, 2008. Disponible en: http://www.tomshardware.com/reviews/hp-server-web,1943.html

[26] D. Watts, M. Hurman y L. Braz. Implementing the IBM BladeCenter S chassis. IBM Redbooks. Enero, 2009.

[27] IBM. IBM Storage Configuration Manager: Planning, installation and configuration guide. Febrero, 2010.

[28] J B. Layton. Intro to nested-RAID: RAID-01 and RAID-10. [En línea]. Linux magazine. Enero, 2011. Disponible en: http://www.linux-mag.com/id/7928/

[29] JetStor. RAID.EDU: Understand RAID technology with our award winning RAID tutorial. [En línea]. Disponible en: http://www.acnc.com/raid

[30] VMware. VMware technical support welcome guide. Abril, 2012.

[31] VMware. The architecture of VMware ESXi. 2007.

[32] VMware. VMware vSphere: Virtual machine file system (VMFS). [En línea]. Disponible en: http://www.vmware.com/ve/products/datacenter-virtualization/vsphere/vmfs.html

[33] VMware knowledge base. Minimum system requirements for installing ESX/ESXI (1003661). [En línea]. VMware. Disponible en: http://kb.vmware.com/kb/1003661

[34] K. Gleed. What is in a VIB? [En línea]. VMware vSphere blog. Septiembre, 2011. Disponible en: http://blogs.vmware.com/vsphere/2011/09/whats-in-a-vib.html

[35] VMware knowledge base. Minimum system requirements for installing vCenter Server (1003882). [En línea]. Disponible en: http://kb.vmware.com/kb/1003882

[36] VMware knowledge base. Upgrading to vCenter 5.1 best practices (2021193). [En línea]. Disponible en: http://kb.vmware.com/kb/2021193

[37] Microsoft IT showcase. Identifying server candidates for virtualization: technical case study. Junio, 2008.

[38] VMware. VMware vSphere 5.0 evaluation guide. Abril, 2011.

[39] VMware. VMware vSphere 5.0 competitive reviewer's guide. 2011.

[40] VMware. VMware vSphere command-line interface installation and reference guide. 2009.

[41] VMware. Virtual machine disk format (VMDK). [En línea]. Disponible en: http://www.vmware.com/technical-resources/interfaces/vmdk.html

[42] VMware. VMware vCenter converter. [En línea]. Disponible en: http://www.vmware.com/products/converter/

[43] B. Mitchell. SAN. [En línea]. Disponible en: http://compnetworking.about.com/od/networkstorage/g/storage_san.htm

[44] L. Silva. Product standard: virtual server. PricewaterhouseCoopers Network Technology Group. Marzo, 2011.

[45] VMware. VMware vSphere 5.1 vMotion architecture performance and best practices. 2012.

[46] PricewaterhouseCoopers Information Technology Security. Virtual machine server. 2013.

[47] HyTrust. Virtualization security checklist. ISACA. 2010.

[48] M. Butler y R. Vandenbrink. IT audit for the virtual environment. SANS. Septiembre, 2009.

[49] J. Fisher-Ogden. Hardware support for efficient virtualization. University of San Diego, USA. 2008.

[50] AMD. AMD64 virtualization codenamed "pacifica" technology: secure virtual machine architecture reference manual. Mayo, 2005.

[51] VMware. Network segmentation in virtualized environment. Mayo, 2009.

[52] Acronis. Virtualización: Como planificar una infraestructura virtual. 2008.