UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

Estudio y Análisis de seguridades en servidores virtualizados

AUTOR:

Albán Ortiz, Erick Fabián

Trabajo de Titulación previo a la Obtención del Título de:

INGENIERO EN TELECOMUNICACIONES

TUTOR:

M. Sc. Romero Paz, Manuel de Jesús

Guayaquil, Ecuador

15 de Septiembre del 2021

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Sr. **Alban Ortiz, Erick Fabian** como requerimiento para la obtención del título de **INGENIERO EN TELECOMUNICACIONES**.

TUTOR

Ing. Romero Paz, Manuel de Jesús

DIRECTOR DE CARRERA

M. Sc. Heras Sánchez, Miguel Armando

Guayaquil, a los 15 días del mes de septiembre del año 2021

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Alban Ortiz, Erick Fabian**

DECLARÓ QUE:

El trabajo de titulación **"Estudio y Análisis de seguridades en servidores virtualizados"** previo a la obtención del Título de **Ingeniero en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 15 días del mes de septiembre del año 2021

EL AUTOR

ALBAN ORTIZ, ERICK FABIAN

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Alban Ortiz, Erick Fabian**

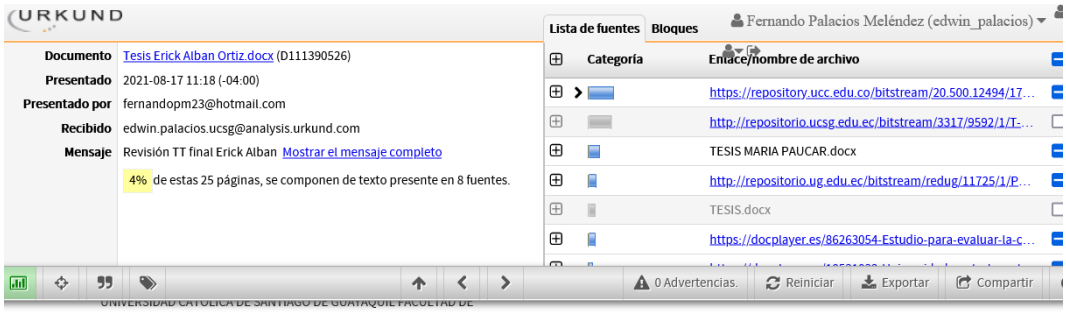
Autorizó a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Trabajo de Titulación: **"Estudio y Análisis de seguridades en servidores virtualizados"**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 15 días del mes de septiembre del año 2021

EL AUTOR

ALBAN ORTIZ, ERICK FABIAN

REPORTE DE URKUND



UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TÍTULO: Estudio y Análisis de seguridades en servidores virtualizados

AUTOR: Albán Ortiz Erick Fabián

Trabajo de Titulación previo a la Obtención del Título de: INGENIERO EN TELECOMUNICACIONES

TUTOR: Ing. Romero Paz, Manuel de Jesús MSC.

Guayaquil, a los 28 días del mes de agosto del año 2021

UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO CARRERA DE INGENIERÍA EN

TELECOMUNICACIONES

CERTIFICACIÓN

DEDICATORIA

Quisiera dedicarle mi trabajo de titulación a Dios, a mis padres y a mi hermana que me han dado la oportunidad de permitirme estudiar para así lograr ser un buen profesional, y también le dedico todos mis esfuerzos a mi abuelita y a mi prima que siempre las he llevado presente.

EL AUTOR

ALBAN ORTIZ, ERICK FABIAN

AGRADECIMIENTO

Primeramente, quisiera agradecerle a Dios y a mis padres que han estado siempre conmigo para guiarme y brindarme su apoyo durante toda mi carrera universitaria, también agradecerle a mi tutor y profesor el Ingeniero Manuel Romero una excelente persona y un excelente tutor, que gracias a su tiempo y paciencia he podido desarrollar mi trabajo de titulación, de igual manera agradecerles a todos mis profesores que me han ayudado a mejorar para así poder ser un mejor profesional, y por ultimo agradecerle a mi tío y tía que me han aportado con buenos consejos para seguir adelante y cumplir mis metas.

EL AUTOR

ALBAN ORTIZ, ERICK FABIAN

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

M. Sc. ROMERO PAZ, MANUEL DE JESÚS

DECANO

f. _____

M. Sc. HERAS SÁNCHEZ, MIGUEL ARMANDO

DIRECTOR DE CARRERA

f. _____

M. Sc. PALACIOS MELÉNDEZ, EDWIN FERNANDO

OPONENTE

ÍNDICE GENERAL

Índice de figuras

Capítulo 1

Capítulo 2

Capítulo 3

Índice de tablas

Capítulo 3

Resumen

La virtualización es un tema frecuentemente aplicado por la tecnología de información y comunicación, y cada vez va evolucionando y provocando un avance muy productivo para usuarios y empresas, en la cual consiste en permitir que varias máquinas virtuales con sistemas operativos puedan ejecutarse individualmente, operando en la misma máquina física, por tal razón se debe considerar los problemas a los que se puede llegar a tener a un futuro, ya que como todo va evolucionando de igual manera lo harán los problemas de la fiabilidad de la información. Al momento de virtualizar los sistemas de información, se llega a obtener un mayor de ahorro de energía, un favorable espacio físico y un ahorro considerable recursos económicos, aunque lo que conlleva a establecer un sistema de seguridad para los servidores virtualizados que permitan identificar las amenazas que lleguen a existir en la red. En el proyecto propuesto, consiste en proporcionar seguridad a servidores en los entornos virtuales, con el fin de combatir las vulnerabilidades a los que está expuesto dicho servidor, debe garantizar que la información debe estar disponible, integra y confiable. La virtualización tiene como beneficio tener distintos servicios en diferentes equipos, evitando que colapse en la transmisión de sus datos, su administración es más sencilla de controlar, en la actualidad muchas empresas prefieren alquilar VPS, cloud computing, hosts u otros, todo espacio en la nube es mucho más económico que tenerlo en el cuarto de comunicaciones.

Palabras claves: VIRTUALIZACIÓN – SISTEMAS OPERATIVOS – SERVIDORES – MAQUINAS VITUALES – NUBE – SERVIDOR VIRTUAL PRIVADO – TRANSMISION – RED – SEGURIDAD – CLOUD COMPUTING – HOST

Abstract

Virtualization is a topic frequently applied by information and communication technology, and every time it is evolving and causing a very productive advance for users and companies, in which consists of allowing several virtual machines with operating systems can run individually, operating on the same physical machine, for this reason you should consider the problems that you may have in the future, because as everything is evolving in the same way the problems of reliability of information will do. When information systems are virtualized, it is possible to obtain a greater energy saving, more space-saving, and significant economic resource savings, but this means establishing a security system for virtualized servers that allows to identify the threats that may exist on the network. The proposed project consists of providing security to servers in virtual environments, in order to combat the vulnerabilities that the server is exposed, it must ensure that the information must be available, integrated and reliable. Virtualization has the benefit of having different services on different computers, avoiding collapse in the transmission of data, its administration is easier to control, and today many companies prefer to rent VPS, cloud computing, hosts, or others, using the cloud is cheaper than having the information in communications room.

Keywords: VIRTUALIZATION - OPERATING SYSTEMS - SERVERS - VITAL MACHINES - CLOUD - PRIVATE VIRTUAL SERVER - TRANSMISSION - NETWORK - SECURITY - CLOUD COMPUTING - HOST

CAPÍTULO 1: FUNDAMENTOS DEL PROYECTO DE INVESTIGACIÓN

En este capítulo se analizará acerca de los conceptos que se encuentran en relación a la seguridad de los servidores virtuales, fundamento principal, su estructura, definiciones acerca de los virus que se llegue ha encontrar, sistema de protección a los servidores en caso de que exista algún tipo de amenaza.

1.1 Introducción

La virtualización es una herramienta que permite crear una representación basada en la optimización lo cual conlleva una gran cantidad de información con respecto a los procesos de un centro de datos, con el fin de escoger el que tenga mayor beneficio. Este tipo de herramienta tiene una función la cual es optimizar dichos recursos para así obtener un considerable ahorro de recursos tales como, menor consumo de equipos, menor cantidad de personas, con el fin de ahorrar gastos a la empresa.

Con referencia a este nuevo método innovador, muchas empresas hacen uso de esta herramienta, ya que ofrece una gran posibilidad de trabajar en cualquier lugar, estableciendo una conexión con un computador con internet, para así tener acceso a la plataforma de la empresa, y así contar con la base de datos.

Aunque se debe conocer todo referente a esta herramienta, se debe conocer sus ventajas y desventajas, que tan seguro podría ser al momento de ejecutar diversas actividades, ya que existen varios peligros al nivel de red, los más conocidos hackers tratan de forzar la seguridad de la red.

Para extender los servicios a clientes, proveedores y aliados por medio de una conexión segura en las nubes. ¿Qué hacer para cumplir con las garantías de la información y conservar la confidencialidad, Integridad y disponibilidad de la información?, serán muchas las preguntas que se analizará en este estudio.

Mencionar los distintos sitios web que ofrecen equipos virtualizados en la nube, que brinda una plataforma para distintos servicios dentro de una organización, comparar las distintas características que ofrecen los distintos servicios, y que tipo de seguridad ofrece para considerar su alquiler.

En este estudio no sólo se muestran las vulnerabilidades que se tienen al usar la virtualización en la nube, también se plantea una gestión para crear políticas de seguridad en base a norma internacionales y buenas prácticas para contrarrestar y mantener la seguridad de la información.

Se plantea un prototipo de servicios en la nube, donde se define recursos, servicios y costos, esta propuesta ayudará a emprender con ideas para atender necesidades operativas y administrativas dentro de una organización.

1.2 Antecedentes

Actualmente existe una demanda considerable con el uso de internet por parte de personas y empresas que ofrecen diversos productos, lo que trae como consecuencia una necesidad de aumentar los servidores web con el único propósito de que proporcionen un mayor espacio en la nube.

Desde hace mucho las empresas se dedican a realizar ventas de equipos tecnológicos y también ofrecen servicio con soporte, con el fin de garantizar un funcionamiento correcto de sus productos a cada uno de sus clientes.

Para garantizar un funcionamiento correcto en los equipos tecnológicos que proporcionan la virtualización del centro de datos, se realiza una serie pruebas para que no exista error alguno al momento de hacer uso de dicho equipo, y en caso que exista problema alguno poder detectar el error y darle solución de inmediato.

1.3 Planteamiento del problema

Los servicios que la organización va a ofrecer a sus clientes demandan mejorar la parte tecnológica correspondiente y la inversión para realizarlos, actualmente no se cuenta con plataformas en nubes para dar servicios a clientes y proveedores.

Los servicios son: aplicaciones web financieras, hosting de páginas web, plataformas educativas y otras.

No tienen recursos humanos para dar seguimiento a las sesiones recurrentes de accesos en los sistemas, por eso es importante el análisis de la propuesta antes de la entrega, considerando la conveniencia de contar los recursos para las operaciones o la prestación de servicios de terceros.

Inprosec es una empresa que ofrece trabajo de ingeniería y publicidad, la cual está abriendo un abanico de servicios, y requiere tomar decisiones para lograr ofertar nuevos productos, se toma sus necesidades para elaborar un estudio en la realización de esta tesis. El detalle de los servicios que pretenden ofrecer es:

Sistemas informáticos para sus clientes y proveedores.

Control de cámaras a clientes, usando una aplicación receptora de videos y almacenamiento en la nube.

Control de alarmas, que será monitoreada por el mismo cliente.

Servicio de página web a pequeños y medianos clientes, usando el motor WordPress.

Gestor de contenidos para la parte académica y centro de investigación, usando herramientas tecnológicas.

Tomando en consideración la información anterior, debe mencionarse los posibles problemas en el camino de la implementación para plantear posibles soluciones y mostrarlo como parte del estudio. La situación se muestra gráficamente de esta manera:

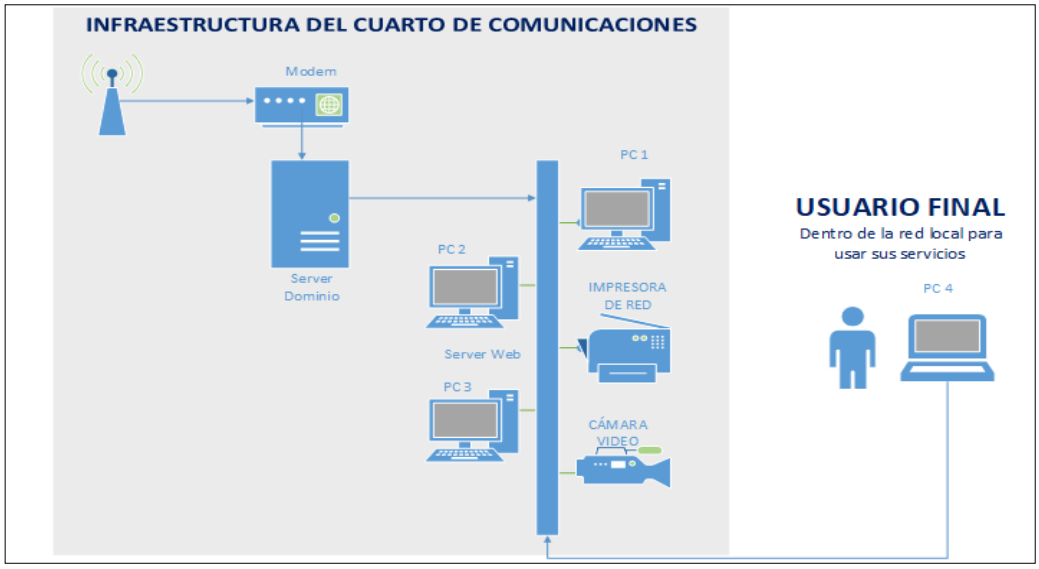


Figura 1. 1: Análisis de la situación actual de la organización
Fuente: Elaboración propia

1.4 Definición del problema

Antes de todo hay que entender todo referente a los servidores, las vulnerabilidades que llegan a tener al momento de estar disponibles en la red y buscar soluciones en caso sufrir algún tipo de atraco informático para así solucionar de manera eficaz sin tener que se filtre la información, por lo que el problema de investigación se define así:

La necesidad de muchas empresas ante la situación que enfrentan que buscan proteger sus servidores en contra de los peligros que hay en la red, por ese motivo deben mejorar su sistema de seguridad, pero teniendo en cuenta que deben optar por compañías que sean fiables, ya que es información delicada.

1.5 Justificación de la investigación

El presente proyecto de investigación tiene como fin identificar cualquier tipo de error a futuro y también proporcionar seguridad a los servidores para que de esa manera no haya ningún tipo de ataque informático.

En la actualidad muchas empresas hacen uso de la virtualización, para así poder desenvolverse y relacionarse con sus clientes de manera organizada y concreta, la cual indica que la inversión de hardware se llega a

reducir considerablemente porque la tecnología permite establecer diversos equipos y servidores virtuales en tan solo un servidor físico.

La seguridad es lo primordial para esta nueva generación tecnológica, ya que se encuentran vulnerables ante el medio en el que se encuentra, siendo necesario protegerlo ante posibles amenazas internas y externas, por eso razón las empresas necesitan que dicha información que se almacenará en la nube se encuentre disponible y sin ninguna alteración en sus datos.

A lo que se quiere llegar según la visión y misión de la organización se lo puede visualizar en el siguiente gráfico.

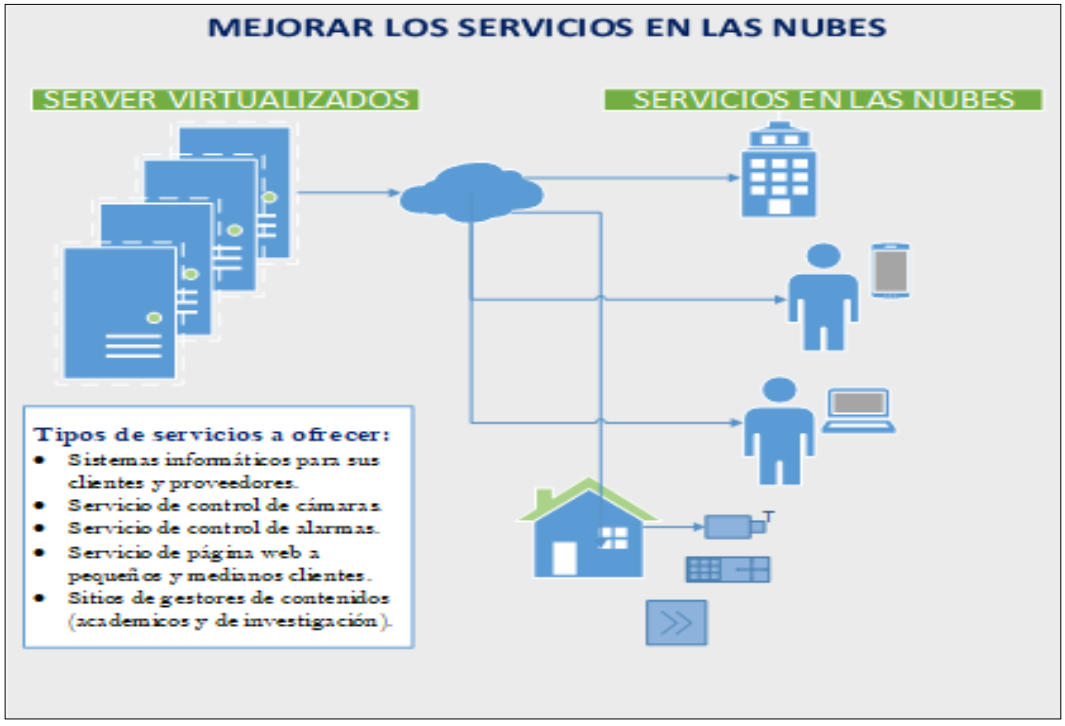


Figura 1. 2: Virtualización de servidores
Fuente: Elaboración propia

1.6 Objetivo General

Plantear una propuesta de estudio de los equipos virtualizados en la nube, mediante un ámbito teórico, pero con una propuesta básica para mostrar los pasos y funcionamiento de una virtualización, con el fin de brindar servicios con sus respectivas seguridades para la información, creando un

entorno seguro con las políticas claves para contrarrestar los ataques a los datos.

1.7 Objetivos Específicos

Crear una gestión de políticas y controles para aplicar en un entorno virtualizado, basada en normas y buenas prácticas internacionales, que serán normalizadas para proteger los datos en los servicios en la nube.

Aprender lo referente al planteamiento general de VPS (Virtual Private Server), Cloud Computing y Servidor dedicado, ver la diferencia entre los servicios y seguridades aplicables en su entorno.

Analizar los tipos de servicios para clientes al momento de implementar una virtualización y llevarlo a la nube, aplicando controles y políticas de seguridades.

Conocer los beneficios de mantener un equipo virtualizado en el cuarto de comunicaciones o tener un proveedor que ofrezca equipos virtualizados en la nube.

1.8 Hipótesis

Cuanto mayor sea la seguridad en los servidores virtuales, menor será la probabilidad de que el equipo se vea afectado ante una amenaza informática, por lo cual es recomendable adquirir un servicio de seguridad que sea confiable.

La efectividad de los equipos puede ser evaluada a través de simulaciones para así detectar algún tipo de error y dar solución respecto al daño, con el fin de que no existan problemas a futuro.

A partir de los análisis de capacidad que se realizan, con el fin de poder verificar si existen recursos adecuados y totalmente disponibles para los servidores.

Aunque se deberá tomar en cuenta que no todos los componentes virtuales llegan a tener el mismo nivel de control de acceso, lo cual traería como consecuencia un incremento alto de riesgo.

1.9 Metodología de la investigación

El objetivo que llega tener este capítulo es proporcionar seguridad a los servidores virtuales que se encuentran vulnerables, con la finalidad de mitigar o realizar una reducción de riegos que haya en los sistemas de la regularización, y para esto se debe establecer un régimen de normas para el proceso.

Se establece un método exploratorio para determinar la información existente necesaria para llevar a cabo este trabajo. Luego se aplica el método descriptivo para desarrollar la explicación de la investigación.

Con el método de Análisis-Síntesis se estudia cada una de las partes involucradas en esta investigación y luego los resultados de este análisis se sintetiza para presentar los resultados y conclusiones del trabajo.

CAPÍTULO 2: FUNDAMENTACIÓN TEÓRICA

En este capítulo se lleva a cabo la estructura de la seguridad en los servidores virtualizados para empresas públicas y privadas, tomando en cuenta la fundamentación teórica de este trabajo de investigación.

2.1. Historia de la virtualización

La era de la virtualización apenas comienza a medida que se crean nuevos servicios, en la cual se necesitan equipos físicos, para ejecutar ese proceso y se necesitan más de ellos (Chahin, 2015).

La virtualización comenzó a desarrollarse en la década de 1960 y se utilizó para dividir mainframes para facilitar su uso. Las computadoras basadas en la arquitectura x86 (32 bits) de hoy enfrentan los mismos problemas de rigidez y poca usabilidad que plagaron los mainframes de su década (Chahin, 2015).

“VMware inventó la virtualización para la plataforma x86 en la década de 1990 para abordar los problemas de infrautilización y de otra índole, a lo largo de un proceso que obligó a superar gran cantidad de desafíos. En la actualidad, VMware es líder mundial en virtualización para x86, con más de 400,000 clientes, incluido el 100 % de las empresas de la lista Fortune 100” (Chahin, 2015).

Desde 2005 se habla de la primera fase de virtualización, en la que se implementan muchas máquinas virtuales en servidores físicos. En 2008 hay una segunda fase en la que se unen diferentes aplicaciones de producción para seguir desarrollando el concepto de oficinas virtuales. Esta fase se llama Virtualización 2.0. Hoy, se ve el aumento de la virtualización 3.0 más allá de los servidores virtuales y las plataformas de virtualización. Presentada como una serie de servicios, esta virtualización es la evolución futura de este concepto, conocido como computación en la nube (Chahin, 2015).

2.2 Virtualización

La virtualización es una técnica que oculta las características físicas de

los recursos informáticos de cómo el sistema operativo (SO), la aplicación u otro usuario final interactúa con esos recursos. La virtualización a nivel de sistema operativo es la tecnología de virtualización de servidores a través de los canales del sistema operativo (kernel), la simulación de dividir un servidor físico en muchas piezas pequeñas (Congo, 2014).

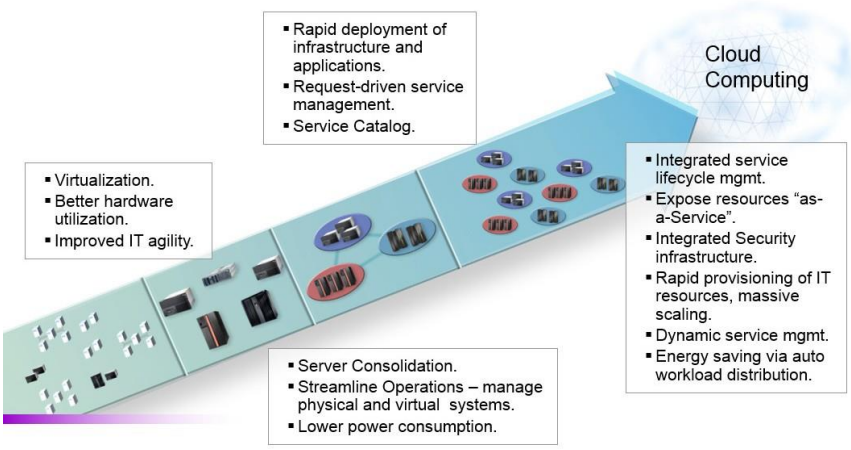


Figura 2. 1: Fases del desarrollo de la virtualización
Fuente: (Chahin, 2015)

Un servidor virtual es una máquina que crea un entorno virtualizado en su computadora para que los usuarios finales puedan utilizar el software en un entorno controlado: Paquete de virtualización de servidor de hardware, sistema operativo, aplicaciones (HW SO APP) en un paquete de servidor virtual portátil (Congo, 2014).

Al adoptar la tecnología de virtualización se aprovecha los servidores existentes, tiene hardware de alto rendimiento y mejora la preparación para emergencias de hardware y software. Es decir, no hay tiempo de inactividad de virtualización para ejecutarse en un entorno virtual mientras se ejecuta en el mismo servidor físico, software adjunto al hardware (Congo, 2014).

Si bien los sistemas operativos y las aplicaciones utilizan la virtualización independiente del hardware, cada servidor virtual puede proporcionar un sistema operativo en el que la administración y las aplicaciones se administran como una sola unidad (Congo, 2014).

Figura 2. 2: Representación de virtualización
Fuente: (Congo, 2014)

2.3 Máquina Virtual

Una máquina virtual es un contenedor de software completamente independiente que le permite ejecutar sistemas operativos y aplicaciones como si fuera un servidor físico (Cabrera, 2017).

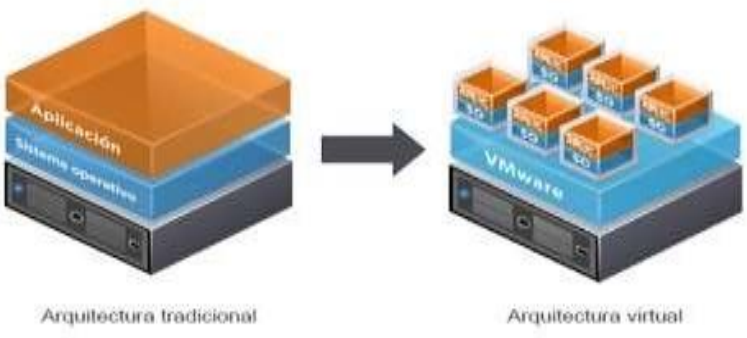


Figura 2. 3: Arquitectura de Máquina Virtual
Fuente: (Robles, 2017)

Las máquinas virtuales funcionan como servidores físicos, con sus propios procesadores virtuales, RAM, discos duros y tarjetas de interfaz de red de software (NIC). El sistema operativo no puede distinguir entre una máquina virtual y una máquina física. Esto también lo hace indistinguible de otras aplicaciones y servidores de la red (Cabrera, 2017).

Incluso la propia máquina virtual lo ve como un servidor real. Sin embargo, la máquina virtual consta solo de software y no contiene ningún componente de hardware. Por lo tanto, las máquinas virtuales ofrecen muchas ventajas sobre el hardware físico (Cabrera, 2017).

2.3.1 Ventajas de las máquinas virtuales

En general, las máquinas virtuales de VMware tienen cuatro características clave que benefician a los usuarios: compatibilidad, aislamiento, encapsulación e independencia del hardware (Cabrera, 2017).

2.3.1.1 Compatibilidad

Al igual que los servidores físicos, las máquinas virtuales alojan su propio sistema operativo y aplicaciones cliente y tienen los mismos componentes (placa base, tarjeta VGA, controlador de tarjeta de red) (Cabrera, 2017).

Como resultado, las máquinas virtuales son totalmente compatibles con todos los sistemas operativos, aplicaciones y controladores de dispositivos estándar, por lo que pueden usarse para ejecutar el mismo software que puede ejecutar en el servidor (Cabrera, 2017).

2.3.1.2 Aislamiento

Las máquinas virtuales pueden compartir recursos físicos en un solo host, pero permanecen completamente separadas entre sí como si fueran máquinas independientes. Por ejemplo, si tiene cuatro máquinas virtuales en un servidor físico y una de ellas falla, las otras tres todavía están disponibles (Cabrera, 2017).

Este es un factor importante para explicar por qué las aplicaciones que se ejecutan en entornos virtualizados están mucho más disponibles y protegidas que las aplicaciones que se ejecutan en sistemas tradicionales no virtualizados.

2.3.1.3 Encapsulamiento

Una máquina virtual, junto con el sistema operativo y todas sus aplicaciones, es un contenedor de software que agrega o "agrupa" un conjunto completo de recursos de hardware virtual en un solo paquete de software. La

encapsulación hace que las máquinas virtuales sean portátiles y fáciles de administrar (Cabrera, 2017).

Como por ejemplo, se puede mover y copiar una máquina virtual desde un lugar a otro como lo haría con cualquier otro archivo de software, o guardar una máquina virtual en un diferente medio de almacenamiento de datos estándar, desde una memoria USB de bolsillo hasta las redes de área de almacenamiento (SAN) de una empresa (Cabrera, 2017).

2.3.1.4 Independencia de hardware

Las máquinas virtuales son completamente independientes del hardware físico subyacente. Por ejemplo, una máquina virtual puede constar de componentes virtuales (CPU, tarjeta de red, controlador SCSI) que son completamente diferentes de los componentes físicos contenidos en el hardware subyacente. Las máquinas virtuales en el mismo servidor físico también pueden ejecutar diferentes tipos de sistemas operativos (Windows, Linux, etc.) (Cabrera, 2017).

Combinado con funciones de encapsulación y compatibilidad, es independiente del hardware y permite que las máquinas virtuales se muevan libremente de un tipo de servidor a otro sin tener ninguna necesidad de ejecutar algún tipo de cambio en los controladores de dispositivos, en el sistema operativo o en las aplicaciones (Cabrera, 2017).

La independencia del hardware también significa que se pueden ejecutar diferentes combinaciones de sistemas operativos y aplicaciones en un solo servidor físico (Cabrera, 2017).

2.3.2 Desventajas de las máquinas virtuales

Según (Cabrera, 2017), si bien la virtualización tiene ventajas significativas, debe tenerse en cuenta que también tiene algunos inconvenientes que deben considerarse antes de comenzar a implementar

este enfoque: los inconvenientes que siempre trae la virtualización son (Cabrera, 2017):

Daño físico. Este no es siempre el caso, pero los discos duros pueden fallar y todas las máquinas virtuales pueden perderse (Cabrera, 2017).

La desventaja es que está principalmente relacionado con el hardware y los eventos que ocurren en este afectan a todas las máquinas virtuales y a toda la infraestructura virtualizada, incluidos los discos y redes (Cabrera, 2017).

2.4 Tipos de virtualización

Según (Chahin, 2015) existen diferentes tipos de virtualización, entre los cuales se tiene:

2.4.1 Virtualización de Hardware

Esta virtualización se considera la más completa de lograr. Esto llega a ser posible gracias a una tecnología de virtualización como por ejemplo las diseñadas por Intel (Intel-VT) o por AMD (AMD-V) conocidas como *Hardware-Assisted Virtualization* (Chahin, 2015).

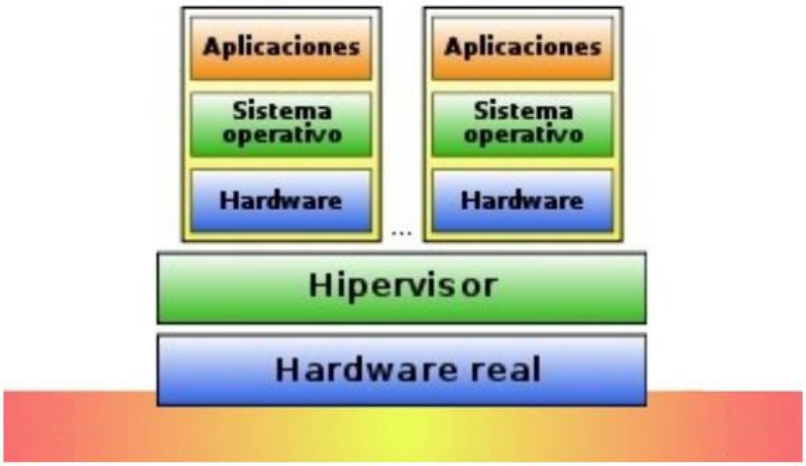


Figura 2. 4: Virtualización por hardware
Fuente: (Sistem@t, 2012)

Las máquinas virtuales emulan componentes de hardware. La máquina física que realiza la virtualización se llama servidor y la máquina virtual se llama cliente. Finalmente, el servidor está a bordo y se inicia para encontrar el nivel generado por el hipervisor (Chahin, 2015).

La virtualización de hardware puede ser una virtualización completa o full virtualización. Cada máquina virtual puede emular su propio dispositivo como si fuera nativo, lo que ralentiza el rendimiento de la máquina virtual. En este tipo de sistema, el anfitrión no sufre ninguna modificación nuclear (Chahin, 2015).

El otro tipo de Virtualización por hardware es el conocido como para virtualización. El sistema operativo se comporta como si no estuviera en un entorno virtual. En el caso mencionado llega a existir una modificación del núcleo, los controladores del hardware están integrados en el Hipervisor y su rendimiento es similar al de una maquina no virtual (Chahin, 2015).

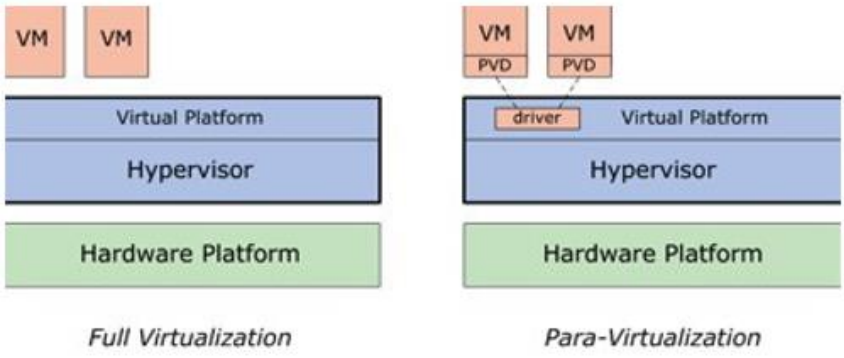


Figura 2. 5: Diferencia entre Full Virtualization y Para-Virtualization
Fuente: (Valentim, Pereira, & Couto)

2.4.2 Virtualización a nivel del sistema Operativo

En este caso, el entorno virtual se ejecuta en el nivel del sistema operativo base. El hipervisor ha sido reemplazado por este sistema operativo básico. Las máquinas virtuales funcionan con sistemas operativos invitados, los procesos se ejecutan de forma independiente y están aislados entre sí (Chahin, 2015).

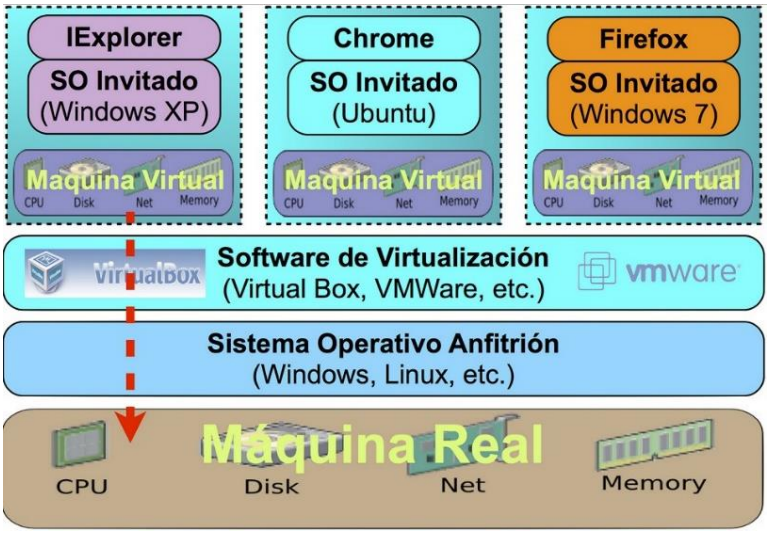


Figura 2. 6: Virtualización a nivel de sistema operativo
Fuente: (Ramírez J. , 2011)

Para que el sistema funcione, el dispositivo físico debe tener tecnología de virtualización compatible con hardware como por ejemplo Intel-VT o AMD-V (Chahin, 2015).

Este tipo de virtualización implementa la virtualización completa a nivel del sistema operativo y crea múltiples instancias del mismo. Cada instancia o entorno virtual creado tiene su propio entorno con recursos asignados previamente.

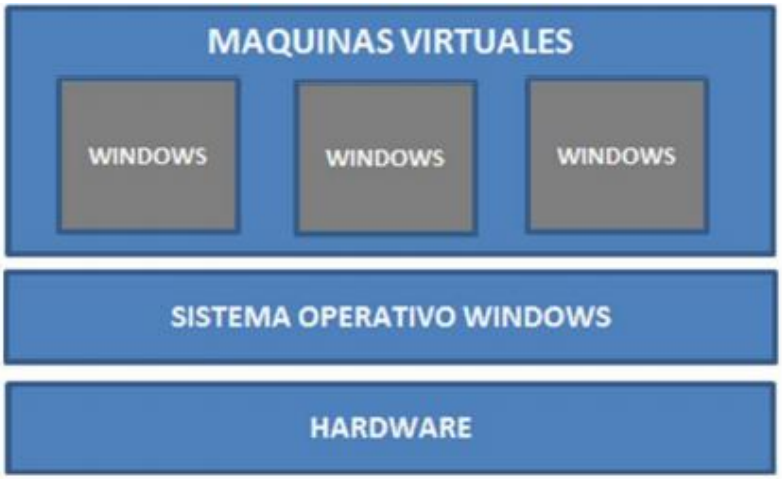


Figura 2. 7: Virtualización a nivel de sistema operativo Windows
Fuente: (Mero & Gallegos, 2015)

2.4.3 Virtualización de Almacenamiento

La virtualización del almacenamiento es el proceso de consolidación de varios dispositivos físicos de diferentes fabricantes moviéndolos a grupos virtuales, no solo a dispositivos lógicos o unidades de almacenamiento. La virtualización del almacenamiento se puede dividir en tres grupos, según la ubicación de la implementación: virtualización basada en dispositivos y en red (Niño, 2020).

2.4.3.1 Virtualización basada en dispositivo

Con este tipo, la virtualización se realiza en una amplia gama de dispositivos de almacenamiento. Cada host tiene un dispositivo virtual asociado con una ubicación física en la matriz de dispositivos, como un disco duro (Niño, 2020).

2.4.3.2 Virtualización basada en red

En este modelo, la virtualización se implementa dentro de la misma red y utiliza conmutadores inteligentes u otros dispositivos virtualizados; en redes como SAN (red de área de almacenamiento), NAS (almacenamiento conectado a red), y DAS (almacenamiento de conexión directa) (Niño, 2020).

2.4.4 Virtualización de Redes

La virtualización de la red es la segmentación lógica o la partición de una sola red física para utilizar los recursos de la red. Esto se logra instalando software, así como servicios de alojamiento compartido, ciclos de cómputo y administración de aplicaciones (Niño, 2020).

La virtualización de red trata a todos los servidores y servicios de la red como un único grupo de recursos al que se puede acceder, independientemente de los componentes físicos. Existen varios tipos de virtualización de redes, de los cuales principalmente son: Virtual LAN, Virtual IP y Virtual Private Network (Niño, 2020).

2.4.4.1 Virtual LAN (VLAN)

La operación consiste en crear una red lógicamente independiente compartiendo la red a nivel físico. Su uso le permite segmentar su dominio de transmisión de manera lógica y controlar la interacción entre dispositivos en diferentes segmentos de red (Niño, 2020).

2.4.4.2 Virtual IP

La dirección IP no está conectada a la tarjeta de red de una computadora o dispositivo en particular. VIP se asigna a los dispositivos de red en la ruta del tráfico de la red. Todos los paquetes entrantes se envían a la dirección IP virtual, pero se redirigen a la interfaz de red del dispositivo receptor (Niño, 2020).

2.4.4.3 Red privada virtual (Virtual Private Network, VPN)

Una VPN configura una red de comunicación privada que se utilizará para enviar datos a través de la red pública de una manera muy sensible, completa y segura. El tráfico se enruta a través de medios de red altamente inseguros, como Internet, creando un canal seguro para enviar información confidencial de un sitio a otro (Niño, 2020).

2.4.4.4 Virtualización de Estaciones de Trabajo

La virtualización de estaciones de trabajo o de escritorio está diseñada para permitirle separar el procesamiento y almacenamiento local del escritorio del usuario con la máquina personal, en la cual hace uso. Con este tipo de virtualización, el soporte se ejecuta en el servidor de virtualización de escritorio central (Niño, 2020).

A través de esta técnica, el usuario hace uso de un lugar de su computador de escritorio un thinclient, el cual hace referencia a un dispositivo que necesita principalmente del servidor central para las tareas de procesamiento, en la cual se enfoca únicamente en transportar tanto la entrada como la salida entre el usuario y el servidor remoto. El thinclient está

constituido de monitor, teclado y mouse para su interacción con el servidor (Niño, 2020).

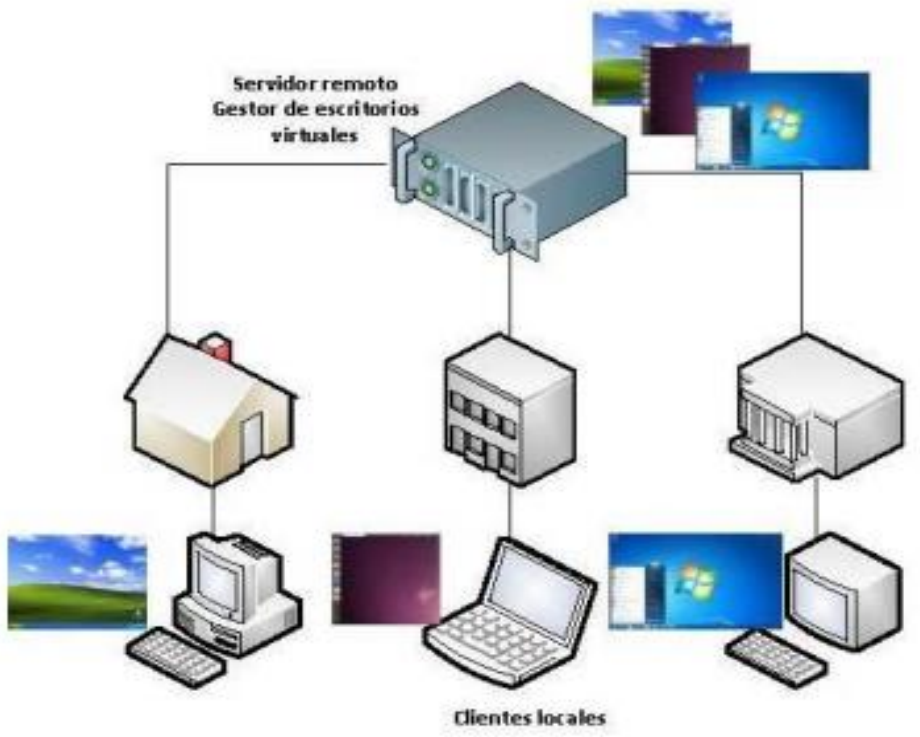


Figura 2. 8: Ejemplo simple de escritorio virtual
Fuente: (Cerrada, 2012)

2.4.5 Virtualización de servidores

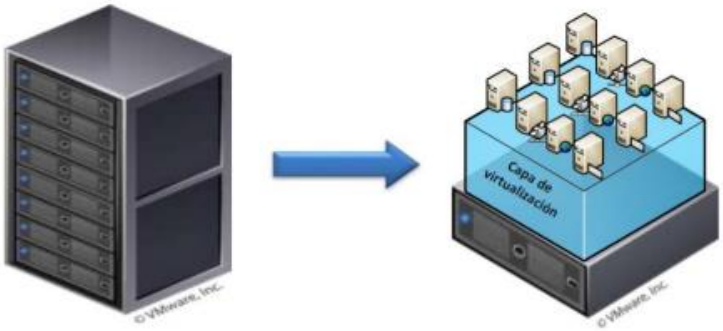


Figura 2. 9: Capa de virtualización
Fuente: (Cerrada, 2012)

Esta es una técnica de virtualización que implica el uso de software de virtualización para dividir un servidor físico en varios servidores virtuales más pequeños. Con la virtualización de servidores, cada servidor virtual ejecuta

varias instancias del sistema operativo al mismo tiempo. Es una ofuscación de los recursos del servidor, incluido el número y la identidad de los servidores físicos, procesadores y sistemas operativos de los usuarios del servidor (Niño, 2020).

2.4.6 Virtualización de aplicaciones

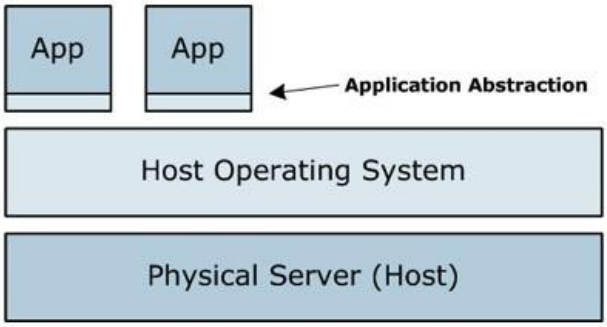


Figura 2. 10: Virtualización de aplicaciones
Fuente: (Chahin, 2015)

La aplicación se ejecuta en un sistema operativo independiente. Esta solución es ideal si tiene aplicaciones incompatibles. La virtualización de aplicaciones convierte una aplicación en un servicio de virtualización centralizado y nunca instalado. Por tanto, no existe ningún conflicto con otras aplicaciones (Chahin, 2015).

2.5 Modos de Virtualización

Según (Ramírez & Robalino, 2014), cuando se describe los hipervisores, se pueden diferenciar entre la virtualización completa y los paravirtualizadores que dispone de funcionalidades y características distintas, (Ramírez & Robalino, 2014):

2.5.1 Virtualización completa

Proporciona una capa intermedia que interviene en el acceso a los recursos hardware y posibilita la coexistencia de múltiples sistemas operativos en un exclusivo servidor (Ramírez & Robalino, 2014).

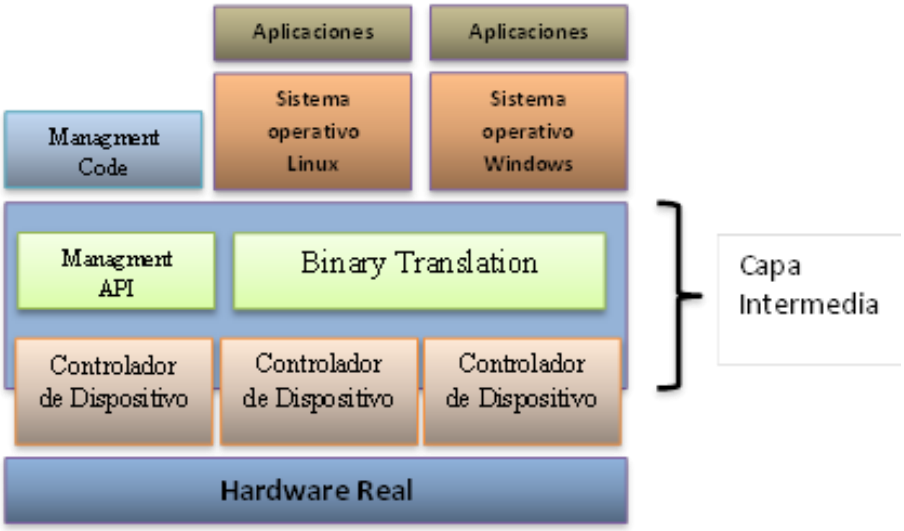


Figura 2. 11: Esquema de Virtualización Completa micro-kernelizada
Fuente: (Raya, 2009)

La máquina virtual debe adquirir y emular todas las instrucciones privilegiadas en este nivel intermedio, lo que tiene un impacto negativo en el rendimiento. Se puede considerar que las máquinas virtuales que se ejecutan en este modo no saben que esta capa de virtualización está separada del hardware (Ramírez & Robalino, 2014).

Los recursos no se pueden compartir si dos o más máquinas virtuales se ejecutan en la misma máquina física. Ejemplos de este enfoque incluyen: Virtual Server, Virtual PC, VMware GSX Server, VMware Plawer, VMware Workstation, VirtualBox, etc. (Ramírez & Robalino, 2014).

2.5.2 Paravirtualización

Un sistema operativo virtualizado reconoce que se está ejecutando en un entorno virtualizado y debe aprovechar ese entorno. De esta manera, algunas llamadas privilegiadas no pasan por la capa de virtualización, lo que resulta en una menor carga y una menor degradación del rendimiento. Sin embargo, esto causa problemas de compatibilidad y portabilidad. A continuación, se muestran algunos ejemplos de este modo: VMware ESX

Server, Hyper-V, Xen, los LDOM, KVM y Virtual Iron (Ramírez & Robalino, 2014).

Según (Ramírez & Robalino, 2014), los procesadores actuales tienen tecnología incorporada para que el hipervisor realice una virtualización completa. Entonces, si necesita implementar un sistema de virtualización de primera clase, por ejemplo, no necesita cambiar el sistema operativo (Ramírez & Robalino, 2014):

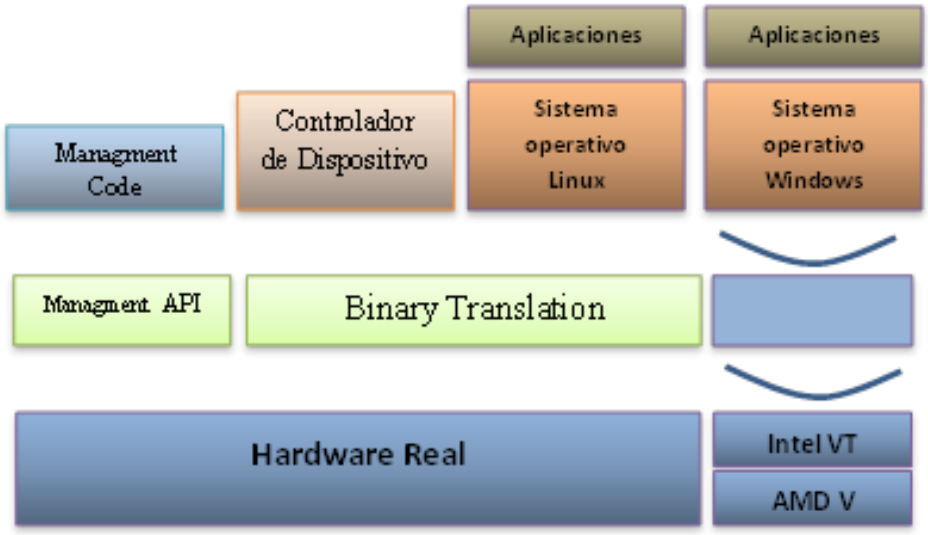


Figura 2. 12: Esquema de Paravirtualización
Fuente: (Raya, 2009)

Intel VT: Intel Virtualization Technology (Tecnología de Virtualización de Intel), esta es la tecnología de Intel para la virtualización de la arquitectura de 32 y 64 bits, también denominada como “Vanderpool” antes conocida como“Silvervale” (Ramírez & Robalino, 2014).

AMD-V: La tecnología de virtualización AMD para la arquitectura de 32 y 64 bits se denomina AMD Virtualization, A menudo referido por nombres en clave "Pacífica" (Ramírez & Robalino, 2014).

2.6 Arquitectura de virtualización

Según (Ramírez & Robalino, 2014) los componentes de la virtualización se organizan de tres formas, como se describe a continuación

(Ramírez & Robalino, 2014):

2.6.1 Virtualización de tipo 1

También conocida como nativa, unhosted, bare-metal, o virtualización sin un sistemaoperativo anfitrión (Hipervisor). Es una capa de software ubicada directamente encima del hardware físico y por debajo de uno o más sistemas operativos (Ramírez & Robalino, 2014).

Su objetivo principal es proporcionar un entorno de ejecución o una partición independiente en la que se pueda ejecutar las máquinas virtuales con sistemas operativos “invitados” (Ramírez & Robalino, 2014).

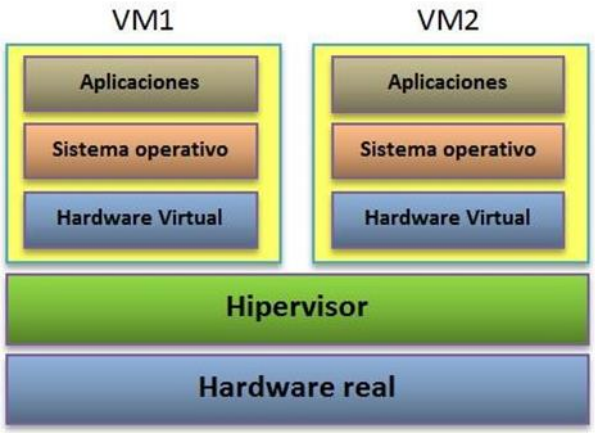


Figura 2. 13: Esquema de virtualización Tipo 1
Fuente: (Raya, 2009)

Los recursos de hardware se asignan a cada partición, como el espacio en disco, el uso de la memoria, el ciclo del procesador y el uso del dispositivo I / S1. El hipervisor es responsable de controlar el acceso al hardware y las aplicaciones cliente que son sistemas operativos o elementos de software de tipo firmware (Ramírez & Robalino, 2014).

Por otro lado, (Ramírez & Robalino, 2014), afirmó que en la virtualización de tipo 1 se pueden distinguir a su vez dos subtipos:

- Arquitectura monolítica
- Arquitectura micro-kernelizada.

2.6.1.1 Arquitectura monolítica

Según (Ramírez & Robalino, 2014), el desarrollo que procede una llamada a hardware en un sistema virtualizado usando un hipervisor de tipo monolítico es (Ramírez & Robalino, 2014):

1. El hardware emulado debe bloquear la llamada.
2. El Monitor de Máquinas Virtuales (VMM) redirige estas llamadas hacia los drivers de dispositivo que se ejecutan en el hipervisor, esto requiere de numerosas alteraciones de contexto en el código de llamada.
3. Los drivers del hipervisor enrutan la llamada al dispositivo físico.

Esto requiere el desarrollo de drivers específicos para el hipervisor para cada componente hardware (Ramírez & Robalino, 2014).

2.6.1.2 Arquitectura micro-kernelizada

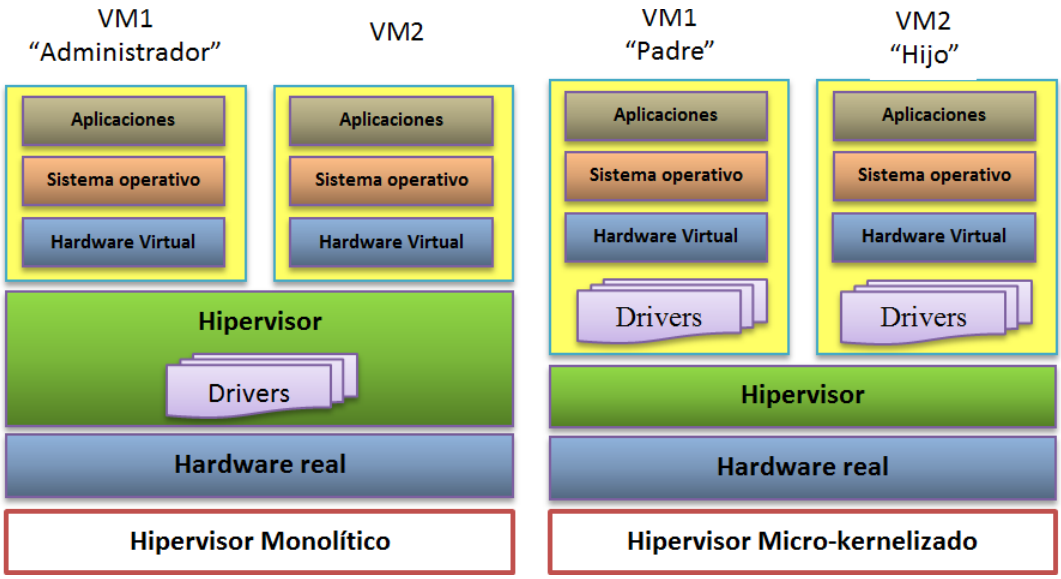


Figura 2. 14: Clases de Virtualización Tipo 1
Fuente: (Raya, 2009)

Esta arquitectura es más simpe, ya que por esa razón las máquinas virtuales no requieren de drivers específicos al acceder al hardware directamente a través de los controladores utilizados por el hipervisor. Así, el hipervisor se convierte en una capa transparente dedicada al aislamiento y la gestión de las distintas máquinas virtuales (Ramírez & Robalino, 2014).

De esta manera, no solo se puede mejorar el rendimiento al reducir el número de cambios de contexto y código intermedio, sino que también es posible mejorar la estabilidad del sistema y reducir el espacio de trabajo del hipervisor al reducir el número de componentes (Ramírez & Robalino, 2014).

2.6.2 Virtualización de tipo 2

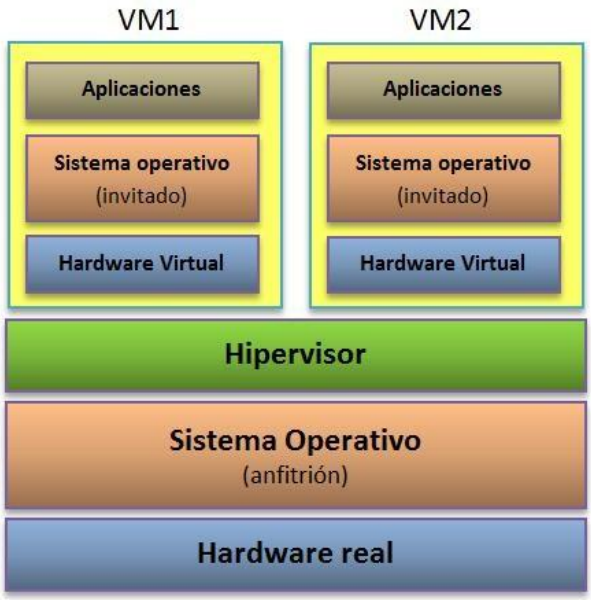


Figura 2. 15: Esquema de Virtualización Tipo 2
Fuente: (Raya, 2009)

Según (Ramírez & Robalino, 2014), es también denominado hosted o virtualización, tomándose en cuenta el sistema operativo anfitrión, en lo que se refiere a una máquina física para así instalar un sistema operativo, partiendo del mismo se establece una capa de virtualización (VMM) debido a la instalación de un software de virtualización adicional o a través del uso de alguna funcionalidad propia del sistema operativo, por ese motivo existe (Ramírez & Robalino, 2014):

- Una capa de virtualización.
- El sistema operativo
- Máquinas virtuales

Este tipo de virtualización, con un sistema operativo instalado, brinda la

capacidad de ejecutar aplicaciones sin un entorno virtualizado mientras se ejecuta una máquina virtual (VM). Por el contrario, esta arquitectura tiene un costo de máquina física más alto y un rendimiento más bajo que otras soluciones.

2.6.3 Virtualización hibrida

El sistema híbrido fue un precursor de los programas anteriores destinados a mejorar el rendimiento de la máquina virtual porque el sistema operativo host y VMM se ejecutaban directamente en el hardware (Chahin, 2015).

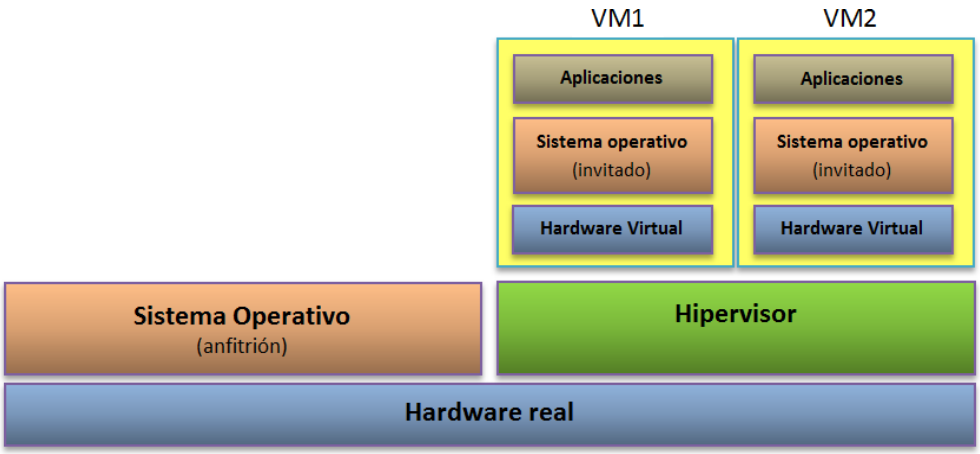


Figura 2. 16: Esquema de Virtualización Híbrida
Fuente: (Raya, 2009)

2.7 El Hipervisor

La mayoría de los sistemas virtualizados se basan en imágenes de hipervisor. Gracias a eso, muchos sistemas operativos pueden ejecutarse en servidores reales. Los sistemas operativos invitados comparten el mismo hardware y tienen el mismo procesador, memoria y recursos de hardware (Chahin, 2015).

El Hipervisor, es en pocas palabras el monitor de máquina virtual (VMM), constituye el núcleo central de las tecnologías de virtualización de hardware más populares y eficaces. Los hipervisores son aplicaciones que presentan a los sistemas operativos virtualizados una plataforma operativa virtual (hardware virtual), a la vez que ocultan a dicho sistema operativo

virtualizado, las características físicas reales del equipo sobre el que operan (Chahin, 2015).

Los hipervisores también son los encargados de monitorizar las tareas y los recursos que emplean los sistemas operativos invitados. Al utilizar hipervisores es posible conseguir que múltiples sistemas operativos compitan por el acceso simultáneo a los recursos hardware de una máquina virtual de manera completa y sin conflictos (Chahin, 2015).

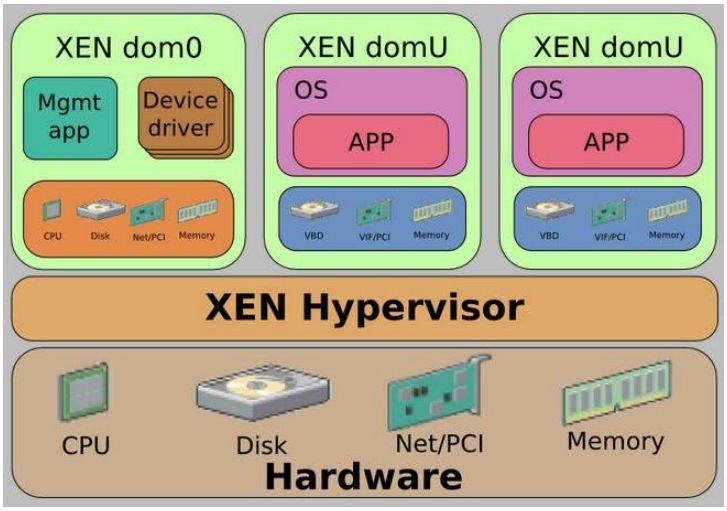


Figura 2. 17: Papel del Hipervisor XEN en un ambiente Virtual
Fuente: (linuxprience, 2012)

2.7.1 Hipervisor tipo 1: Bare-metal

También llamado nativo, unhosted o bare metal (sobre el metal desnudo), es un programa que se ejecuta directamente sobre el hardware, para desarrollar una funcionalidad especifica. Entre los hipervisores del tipo 1 se tiene los siguientes: VMware ESX, Xen (Libre) y Microsoft Hyper-V (Chahin, 2015).

Para conseguir instalar este Hipervisor del tipo 1 es necesario que el procesador lo soporte. Existe una tecnología que permite subdividir las tareas que realiza el procesador de manera que sea capaz de gestionar diferentes sistemas operativos o aplicaciones en particiones independientes del propio chip (Chahin, 2015).

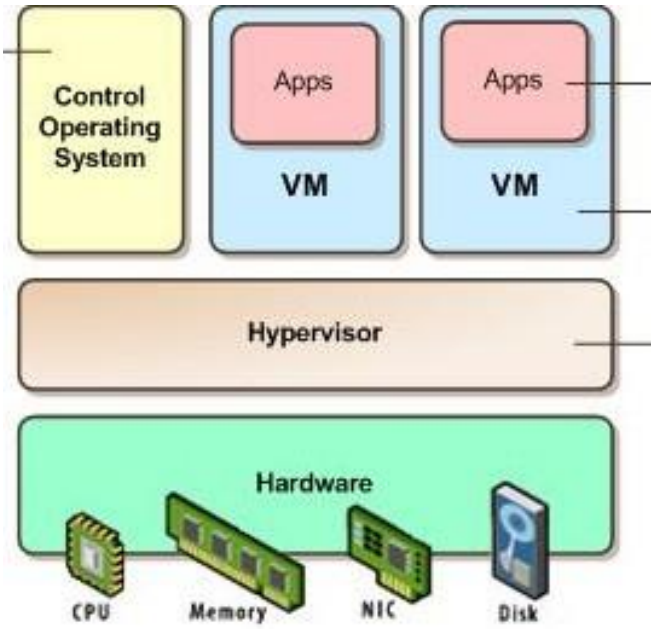


Figura 2. 18: Hipervisor Tipo 1: Bare metal
Fuente: (Art4Software, 2012)

2.7.2 Hipervisor tipo 2: Hosted

También denominado “Hosted”. Es software que se ejecuta sobre un sistema operativo para ofrecer la funcionalidad descrita. Algunos de los hipervisores tipo 2 más conocidos son: VMware WorkStation, Microsoft Virtual Server y Oracle Virtual Box (Chahin, 2015).

Figura 2. 19: Hipervisor Tipo 2: Hosted
Fuente: Elaborado por el autor

2.7.3 Virtualización híbrida

Un sistema híbrido es una opción ante el esquema anterior, en el cual el sistema operativo anfitrión tanto como VMM se ejecutan directamente sobre el hardware y así mejora el rendimiento de las máquinas virtuales.

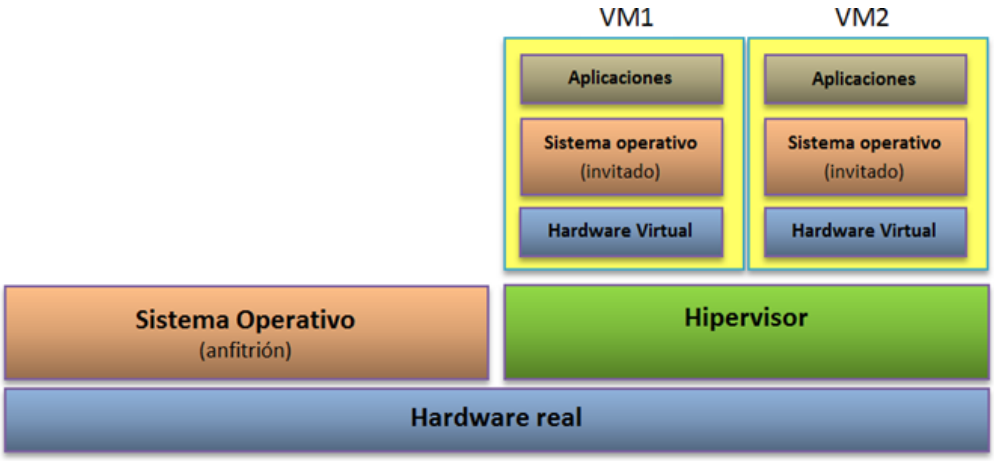


Figura 2. 20: Esquema de Virtualización Híbrida
Fuente: (Raya, 2009)

Según (Chahin, 2015), la seguridad en los servidores virtuales está dada en un sistema de anillos o dominios de protección jerárquica. Cada uno de los anillos delimita un sector donde se establecen determinados privilegios y son empleados como se explica a continuación (Chahin, 2015):

Anillo (0): Conocido también como nivel *Kernel*. En este anillo funciona el sistema operativo. En él es donde existen más privilegios y se ejecutan las instrucciones más relevantes. Cualquier suceso que ocurra en el anillo cero repercute en el modo de usuario (Anillo 3). Por seguridad este anillo (0) en cada VM debe ser desplazado del anillo (0) nativo para que los problemas de este sector no tengan repercusiones en todas las máquinas virtuales (Chahin, 2015).

Los anillos (1) y (2) conocidos como de servicios del sistema y extensiones al sistema operativo, son usado precisamente para proveer servicios al usuario (Chahin, 2015).

El Anillo (3) corresponde a las aplicaciones que son ejecutadas por los usuarios (Chahin, 2015).

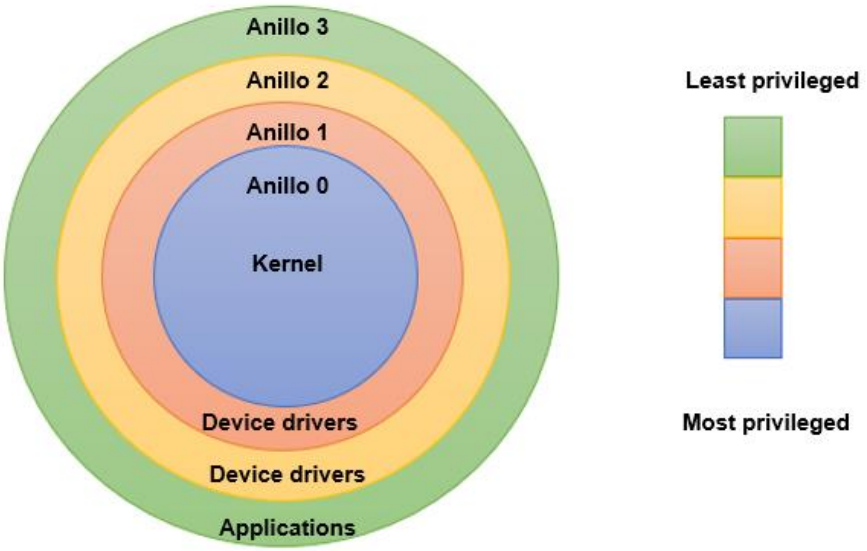


Figura 2. 21: Anillos de privilegio para la arquitectura x86.
Fuente: Elaborado por el autor

La virtualización de escritorios es un concepto que está tomando fuerza en el entorno empresarial, los usuarios pueden tener con una VM (*Virtual Machine*) la experiencia de utilizar un computador real para realizar su trabajo (Chahin, 2015).

Este tipo de virtualización conocida como de plataforma permite tener instalado en un mismo recurso físico diversos sistemas operativos, aplicaciones o emulación de programas (Chahin, 2015).

2.8 La importancia de la virtualización

Una de las razones más relevantes de la virtualización, es la consolidación de servidores, debido a que al virtualizar varios de ellos dentro de uno solo, se ahorra energía, espacio, capacidad de refrigeración y administración y dinero. Sin embargo, la virtualización permite la migración en directo, lo que significa que se puede mover un sistema operativo y sus aplicaciones a un nuevo servidor con el objeto de balancear las cargas (Congo, 2014).

Otro aspecto importante de la virtualización, al permitir ejecutar varios sistemas operativos, si uno falla este no afecta a los demás, pues el núcleo Linux ocupa un solo espacio de direcciones, lo que significa que un fallo en el

núcleo o en cualquier driver provoca la caída del sistema operativo completo, lo que sería una gran desventaja si se tiene un server físico, esto derivaría en la afectación para todos los hospedados (Congo, 2014).

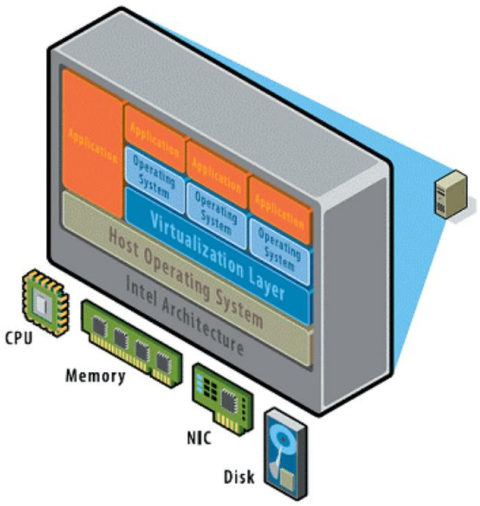


Figura 2. 22: Representación de un modelo de Máquina Virtual
Fuente: (Doña, García, López, Pascual, & Pascual, 2012)

2.9 Propiedades de la virtualización

Las propiedades de la virtualización se componen de los siguientes:

2.9.1 División

Se pueden ejecutar múltiples aplicaciones y sistemas operativos en un mismo sistema físico. Los servidores se pueden consolidar en servidores virtuales con una arquitectura de escalabilidad vertical (scale-up) u horizontal (scale-out) (Congo, 2014).

2.9.2 Aislamiento

Los servidores virtuales están completamente aislados entre sí y del servidor host. Si existen fallas en un servidor virtual, las demás no se ven afectados. Los datos no se filtran a través de los servidores virtuales y las aplicaciones sólo se pueden comunicar a través de conexiones de red configuradas (Congo, 2014).

2.9.3 Encapsulación

El entorno completo del servidor virtual se guarda en un solo archivo, fácil de mover, copiar y resguardar. La aplicación reconoce el hardware virtual estandarizado de manera que se garantiza su compatibilidad (Congo, 2014).

2.10 Hosting

El término host es usado en informática para referirse a las computadoras conectadas a una red, que proveen y utilizan servicios de ella. Los usuarios deben utilizar anfitriones para tener acceso a la red. En general, los anfitriones son computadores monousuario o multiusuario que ofrecen servicios de transferencia de archivos, conexión remota, servidores de base de datos, servidores web, etc. Los usuarios que hacen uso de los anfitriones pueden a su vez pedir los mismos servicios a otras máquinas conectadas a la red (Congo, 2014).

De forma general un anfitrión es todo equipo informático que posee una dirección IP y que se encuentra interconectado con uno o más equipos. Un host o anfitrión es un servidor que funciona como el punto de inicio y final de las transferencias de datos. Comúnmente descrito como el lugar donde reside un sitio web. Un anfitrión de Internet tiene una dirección de Internet única (dirección IP) y un nombre de dominio único o nombre de anfitrión (Congo, 2014). Por otro lado, (Chahin, 2015) indica que los servicios Cloud que pertenecen a esta tercera fase de la virtualización, abundan en internet, dentro de lo que ofrecen se puede encontrar equipos virtuales como *Cloud Servers* entre sus características más relevantes se tiene:

- ✓ Sistemas de *Raid* con dos o más discos duros.
- ✓ Servidores virtuales que pueden tener un hardware optimizado (procesadores con más de 10 núcleos, RAM hasta de 128 Gb y conexiones de red de 10 Gbps) se pueden configurar para suplir las labores de procesamiento más exigentes.
- ✓ Las Máquinas Virtuales pueden ser configuradas con un hardware acorde a las necesidades de trabajo.

- ✓ Escalabilidad en la potencia del hardware, permitiendo tener un crecimiento variable a las necesidades de procesamiento, ya sean fijas o temporales.
- ✓ Asistencia técnica las 24 horas, administración de la infraestructura y capacitación para que los usuarios aprendan a utilizar los recursos, todo esto a muy bajos costos.

Este término se viene usando desde hace 60 años, y ha sido aplicado a diferentes aspectos y ámbitos de la informática, desde sistemas computacionales completos, hasta capacidades o componentes individuales. Fueron creadas por IBM como una forma para compartir diferentes sistemas, y se conoce como virtualización de plataforma o sistema. De esta forma, la plataforma de hardware subyacente es virtualizada para ser compartida con cierto número de sistemas operativos y usuarios diferentes (Niño, 2020).

2.11 Beneficios de la virtualización y la externalización de infraestructura

Los equipos de cómputos que se convierten en servidores de tipo de servicios de correos, aplicaciones web, base de datos, de respaldo u otros, demanda costos en tecnología, recursos físicos y recursos humanos, para mantenerlo dentro del cuarto de comunicaciones, muchos prefieren alquilar proveedores que den servicios en las nubes.

La era de transformación digital nos exigen migrar por un sistema más modular, lo tradicional de tener equipos con tecnología de cliente servidor, aplicaciones locales o algún servicio local, la pandemia han obligado a trabajar en forma virtual.

Aparece "Cloud computing es un nuevo modelo de prestación de servicios de negocio y tecnología, que permite al usuario acceder a un catálogo de servicios estandarizados y responder a las necesidades de su negocio, de forma flexible y adaptativa, en caso de demandas no previsibles o de picos de trabajo, pagando únicamente por el consumo efectuado.“(Ernesto Rengifo García, 2013).

Algunos problemas que trae un sistema tradicional son:

- Mucho tiempo para implementar distintos servicios para la entrega.
- Lugar físico reducido.
- Consumo de planilla de luz muy alto
- En momento de operación o mantenimiento es un gran problema.
- La obsolescencia en equipos.

Hay proveedores que ofrecen servicios de infraestructura virtual de equipo en las nubes y con distintos servicios, según sus necesidades pueden alquilarlo.

A nivel de costo y tiempo es mucho más factible irse con proveedores que nos den recursos en las nubes.

2.11.1 Servidores Cloud

Son servicios tipo Iaas, donde podemos definir como ejemplos: AbiCloud, Amazon, Web Services EC2, GoGrid, entre otros.

Estos planes hay que agregar Licencias de aplicaciones, sistema operativo, manejo de seguridades, todo para administrarlo.

Figura 2. 23: Servidores Cloud en Sudamérica
Fuente: (Ecuahosting, 2019)

2.11.2 Servidores VPS

Figura 2. 24: Servidores VPS en Sudamérica
Fuente: (Ecuahosting, 2019)

Tiene un aislamiento completo, tiene características y funciones del servidor dedicado, es independiente y puede instalar aplicaciones, programa o servicios únicos que corre en ese equipo.

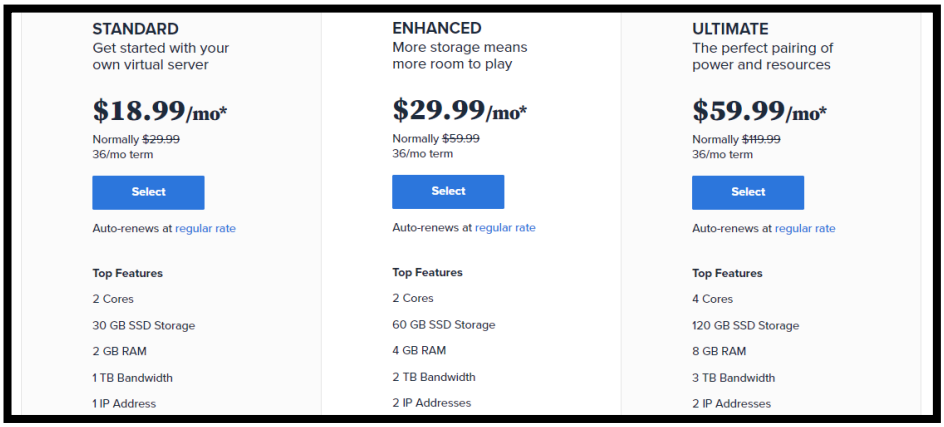


Figura 2. 25: Servidores VPS U.S.A.
Fuente: (Bluehost, 2002)

CAPÍTULO 3: SEGURIDAD DE LA INFORMACIÓN EN AMBIENTE VIRTUALIZADO

La información se considera el activo más importante de toda organización, todo data center debe manejar las gestiones de seguridad (Enriquez & Hidalgo, 2015), la demanda de los servicios exige mayor control, ahora, el ambiente virtualizado va a exigir lo mismo, en los siguientes puntos se muestra temas como los ataques más frecuentes y como proteger las máquinas virtuales.

3.1 Estudio de incidentes de ataques en las empresas en Latinoamérica.

Se considera dentro de esta investigación los reportes de estudio más reciente de la seguridad de la información en América Latina, edición 2021 y se ha tomado la información de 17 países de Latinoamérica (Eset, 2021), cada tabla muestra información que demuestra la situación en el último trimestre del año 2020, tiempo de la pandemia mundial, pero que para muchas empresas en Latinoamérica se convirtió en el foco para cometer ataques.

3.1.1Incidencia de ataques

Se crea un resumen de información del estudio de empresas de control de seguridad de la información (Enriquez & Hidalgo, 2015), los países que muestran mayor incidencia de distintos ataques a la seguridad de la información se detallan en las siguientes tablas.

Tabla 3. 1 Incidencia de ataques en empresas en Latinoamérica.

Ítem	Ataques	Lugar	Incidencia (%)	Observación
1	Códigos maliciosos	Latinoamérica	34,0%	Principal preocupación entre los ataques.
2	Malware	Brasil	19,0%	
3	Malware	México	17,5%	
4	Malware	Argentina	13,3%	
5	Ransomware	Latinoamérica	35,0%	Características como doxing, print bombing, cold call y ataques de DDoS.

6	Minería de criptomonedas	Perú	10,1%	Tailandia (17,9%) fue el país con mayor porcentaje de detecciones.
7	Minería de criptomonedas	Ecuador	5,1%	Concordancia con el aumento en el valor de las criptodivisas.
8	Phishing	Brasil	26,4%	
9	Phishing	Perú	22,8%	
10	Phishing	México	12,0%	

Fuente: Elaboración propia con información de estudio realizado por (Eset, 2021)
Elaborado por: Autor

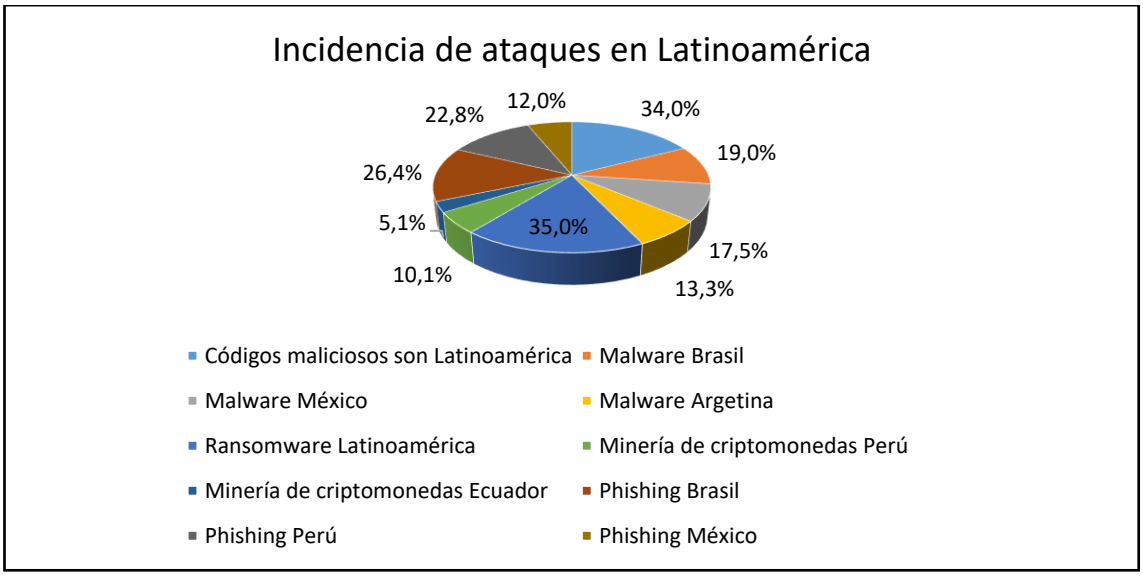


Figura 3. 1: Cuadro de incidencia de ataques
Fuente: Elaboración propia con información de estudio realizado por (Eset, 2021)

Los encargados de la seguridad de la información son responsables para plantear a los dueños o directivos principales de la institución la búsqueda de alternativas de solución para proteger la información, se plantea la siguiente pregunta ¿Aplica invertir en la seguridad de la información en su organización?, revise la tabla 3.2.

Tabla 3. 2: Encuesta de seguridades tecnológicas aplicadas en su empresa

Presupuesto para la seguridad de la información dentro de la institución			
	La Seguridad se mantuvo o se redujo con respecto a años anteriores	76%	
	Recurso insuficiente	81%	

Fuente: Elaboración propia con información de estudio realizado por (Eset, 2021)
Elaborado por: Autor

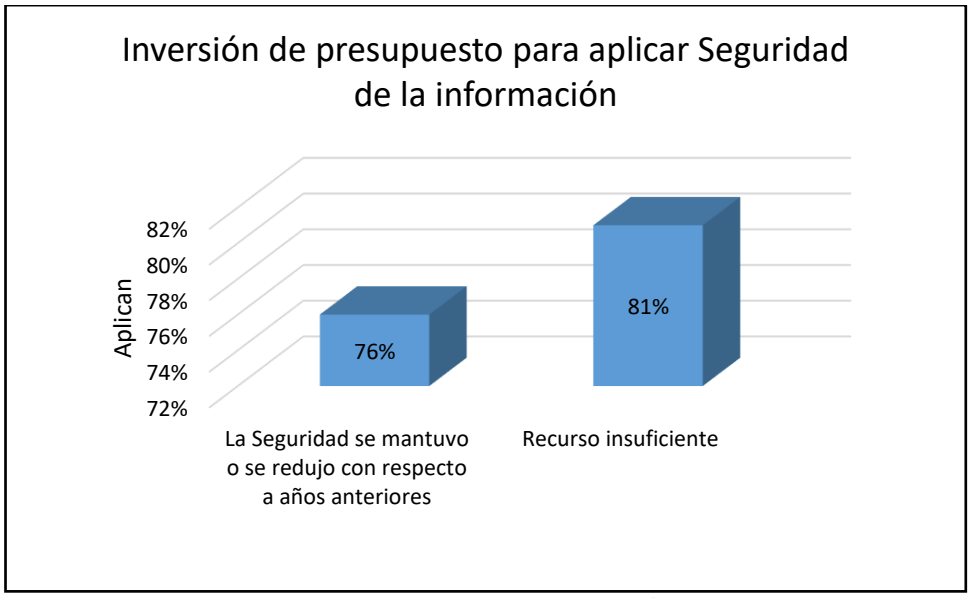


Figura 3. 2: Cuadro de encuesta para conocer si la inversión es aplicable en su institución
Fuente: Elaboración propia con información de estudio realizado por (Eset, 2021)

Se muestra datos muy puntuales acerca de la aplicación de seguridad en medios de acceso a la información y la forma de comunicar del peligro por falta de conocimientos con temas de seguridad de la información y de la organización.

Tabla 3. 3: Parte de la encuesta de conocer la aplicación de seguridades y de lo que conoce de ella

Actores directo para contrarrestar la inseguridad en la red del internet		
Equipos	**Solución**	**Uso (%)**
Dispositivos móviles	Antimalware	15%
La concientización y educación en ciberseguridad		
Actividades de manera ocasional		78%

Fuente: Elaboración propia con información de estudio realizado por (Eset, 2021)

Hay soluciones tecnológicas en el mercado para aplicar seguridades en entornos físico y lógicos, las más usadas son para aquellas que contrarrestan ataques que tienen mayor incidencia, en la tabla 3.4 nos muestra soluciones de aplicados en empresas.

Tabla 3. 4: Soluciones de seguridad tecnológicas aplicadas en empresas en Latinoamérica

Soluciones	**Aplicado**
Antivirus	86%

Firewall	75%
Respaldo de información	68%
Doble autenticación	22%
Tecnología de cifrado	18%
EDR (Endpoint Detection and Response)	16%
Data loss prevention (DLP)	16%
Seguridad para móviles	15%
Otro	1%
Ningún control de seguridad	3%

Fuente: Elaboración propia con información de estudio realizado por (Eset, 2021)

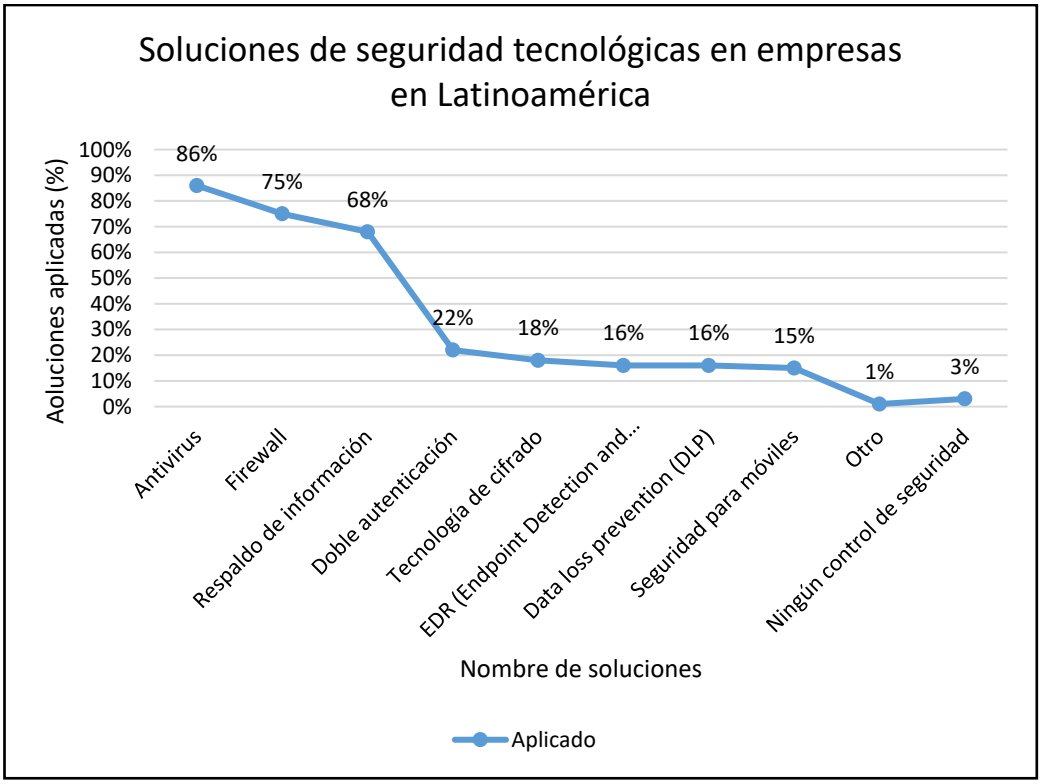


Figura 3. 3: Soluciones tecnológicas aplicada en empresa Latinoamérica
Fuente: Elaboración propia con información de estudio realizado por (Eset, 2021)

3.2 Gestión de Riesgo

Permite identificar y valorar los distintos riesgos de seguridad, el estándar ISO/IEC 27005 es una guía, se usa para determinar o identificar un riesgo, también mitigar los riesgos a un nivel aceptado (Enriquez & Hidalgo, 2015).

Un estudio del 2020 de la empresa de seguridad ESET da a conocer los ataques a la seguridad de la información en Latinoamérica, donde menciona en una encuesta que el 81% que los recursos con los que cuentan para seguridad resultan insuficientes (Eset, 2021).

Los servicios tales como hosting, housing y cloud computing han surgido con gran demanda, y los centros de datos han tenido que implementar las seguridades tanto físicas y lógicas para cumplir con la garantía de la información que es confidencialidad, integridad y disponibilidad. Para tener una alta disponibilidad hay que identificar y contrarrestar las vulnerabilidades que existan en la organización.

3.2.1 Riesgos de seguridad en ambientes virtualizados

Sistemas virtualizados o físicos requieren atención de seguridad, en la figura 3.1 se muestra que existe más ataques de malware en Latinoamérica, en ambientes virtualizados se emplea un agente de seguridad que pueda verificar que no sea infectado por cada máquina virtual, sin requerir agente SVA (Security Virtual Appliance) en cada máquina virtual, donde se ejecuta en el hipervisor (Mendoza, 2016). La figura 3.4 se muestra dentro del hipervisor donde mantiene el motor de análisis e identificación de malware, dando seguridad a las máquinas virtuales.

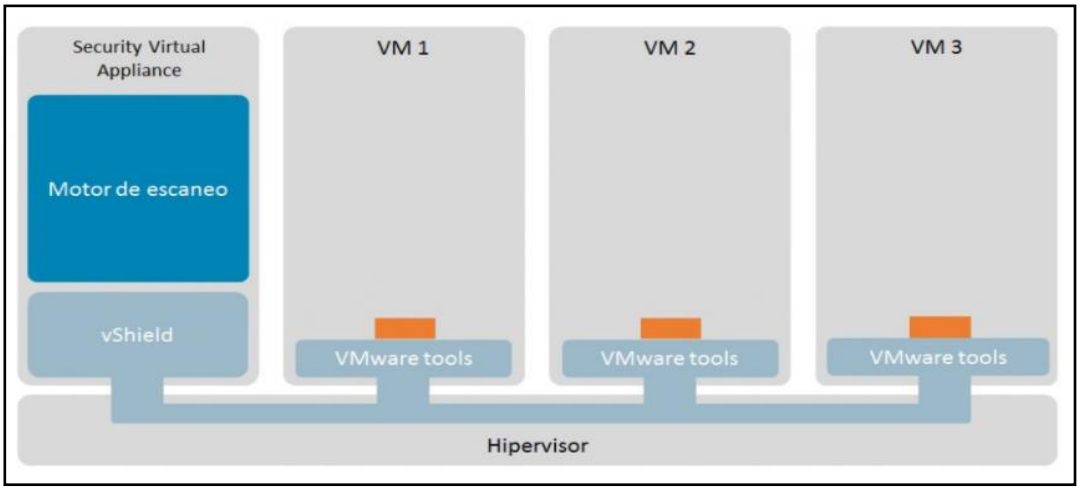


Figura 3. 4: Estructura de VSA (Security Virtual Appliance) en entrorno virtual
Fuente: (Mendoza, 2016)

3.2.2 Análisis de riesgo

Para conocer los posibles riegos, se ha creado una matriz donde se puede ver las vulnerabilidades para medir el impacto que puede producir tanto en los equipos como en los servicios.

La estructura de red virtual, las vulnerabilidades en software de virtualización y nuevos tipos de ataques (HyperJacking, Hypervisor Escape, Ataques a VM) (Descalzo, 2016). La figura 3.5 muestra la formación de una red virtual, donde se muestra la estructura interna de la máquina virtual.

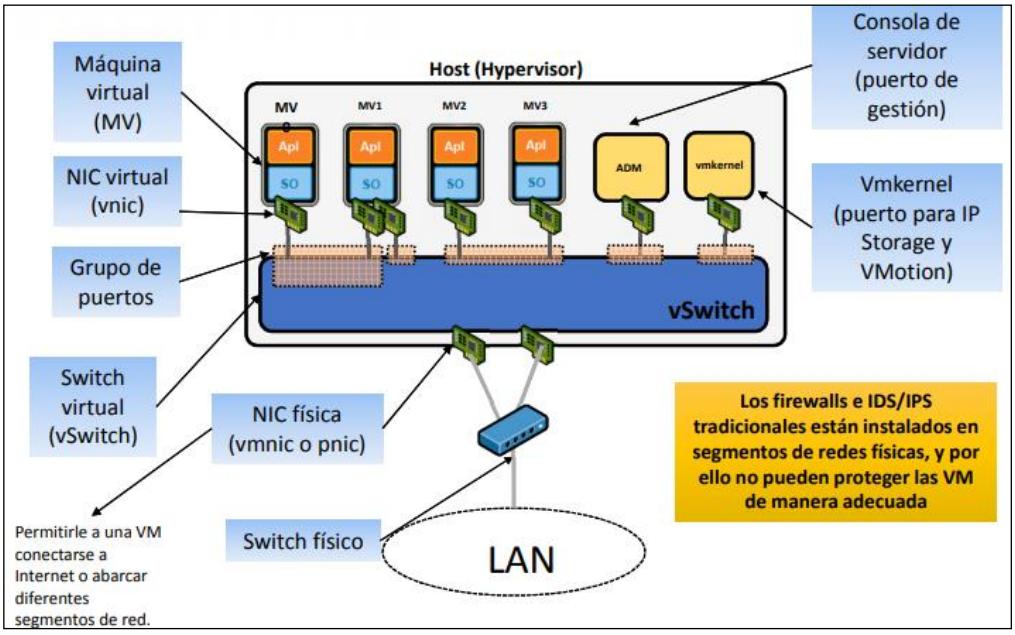


Figura 3. 5: Estructura interna de ambiente de la máquina virtual
Fuente: (Descalzo, 2016)

3.2.2.1 Identificación de Activos

Hace referencia a cuál elemento de la organización que contenga datos e información, se clasifican de acuerdo en la sensibilidad y criticidad de la información (Arévalo, Cedillo, & Moscoso, 2017).

Activos identificados:

Servidor físico

Software de virtualización

Equipos de comunicación

Equipos de seguridad

Personal TI capacitado

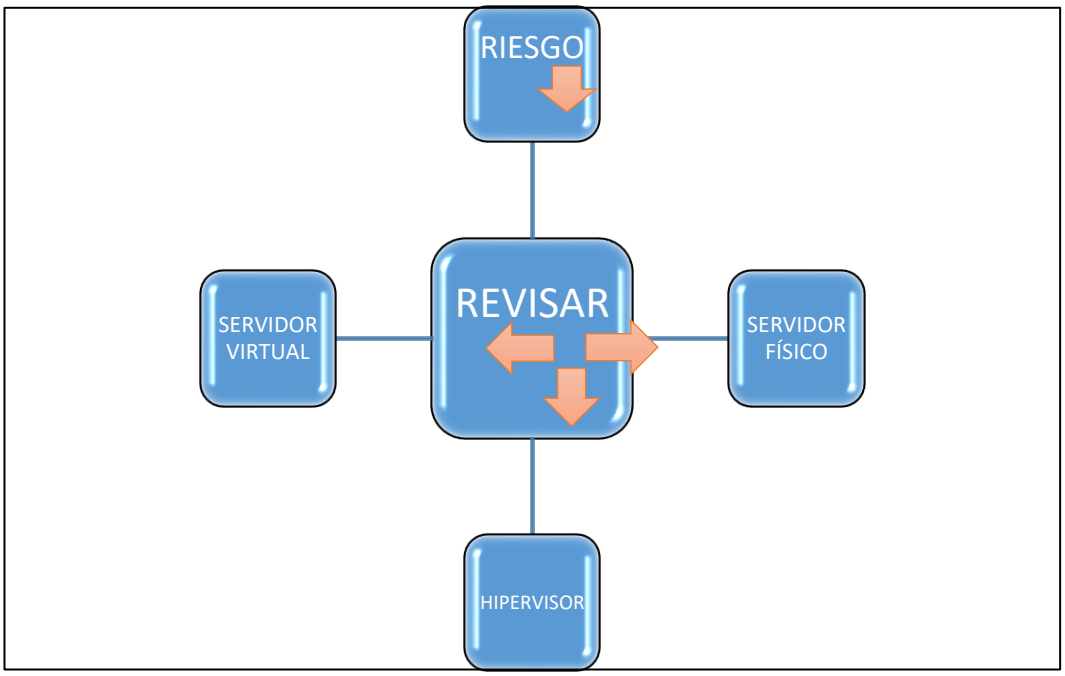


Figura 3. 6: Activos de información identificados en la organización
Fuente: Elaboración propia

3.2.3 Evaluación de riesgo

Se considera los activos mencionados en la figura 3.6, donde soportan los procesos y servicios para virtualizar. Cada riesgo debe considerarse como las amenazas que pueden aparecer en el ambiente virtual, tarjeta de red, software de virtualización, memoria interna, procesadores, el personal que configura y demás involucrados para poner en producción, estos riesgos pueden dañar lo mencionado.

Se resumen datos resultantes que debe considerarse al momento de hacer el tratamiento, la acción a tomar depende del nivel impacto. Los encontrados son: Riesgos técnicos y Riesgos de gestión.

3.2.3.1 Elementos de Riesgo

Se define en lo siguiente: Activos de información, Amenazas, Vulnerabilidades e Impacto.

Formulas:

$$Vulnerabilidad = \frac{\text{Frecuencia estimada}}{\text{Días de año}}$$

Impacto= Valor x Degradación del activo

El riesgo puede estimarse:

Riesgo = Probabilidad × Impacto

3.3 Metodología propuesta para el proceso de Análisis de riesgo y gestión de riesgo

Para mejorar y recomendar hay guías y metodologías basadas en normas internaciones como la ISO/IEC, ITIL, MAGERIT y otros.

3.3.1 Usando la metodología Magerit

Creada para minimizar el riesgo en el uso de tecnología de la información, trabaja de la mano con las normas ISO/IEC. Se plantea de la siguiente manera: Identificar los activos, como muestra la figura 3.7:

	A	B	C	D
1	COD	TIPO DE ACTIVO	ACTIVOS	DESCRIPCIÓN
2	HW100	[HW] Hardware / Equipos informáticos	Los dispositivos informáticos y medios de comunicación	Equipos informáticos y medios de comunicación que son parte de seguridad de ambientes virtualizados.
3	HW200	[HW] Hardware / Equipos informáticos	Servidor de aplicaciones y BD	Equipos de alta disponibilidad interconectados al que acceden los usuarios para ingresar a los sistemas.
4	P100	[P] Personal	Personal de TI	Empleados del área de tecnología
5	D100	[D] Datos	Datos almacenados en BD	Base, tablas donde se deposita la información
6	SW100	[SW] Software	Sistema de Control de Acceso	Sistema que permite que crea perfiles de acceso
7				

Figura 3. 7: Activos de información
Fuente: Elaboración propia

Se identifican las amenazas y la probabilidad que ocurra, cuál será el impacto que provoca en la organización, se detalla en la figura 3.8:

						Impacto						
Activo		Id Riesgo	Amenaza	Probabilidad		[C]	[i]	[D]	Total Cualitativo	Total Cuantitativo	Riesgo	
[HW] Hardware	HW100	R1	Daños por agua	Bajo (1)	1	2	2	3	2	Medio (2)	2	
		R3	Acceso no autorizado	Alto (3)	3	3	3	3	3	Alto (3)	9	
	HW200	R1	Daños por agua	Bajo (1)	1	2	2	2	2	Medio (2)	2	
		R3	Acceso no autorizado	Alto (3)	3	3	3	3	3	Alto (3)	9	
[P] Personal	P100	R5	Indisponibilidad del personal	Bajo (1)	1	1	1	3	2	Medio (2)	2	
[D] Datos	D100	R2	Errores de los usuarios	Alta (3)	3	1	3	2	2	Medio (2)	6	
[SW] Software	SW100	R2	Errores de los usuarios	Media (2)	2	3	3	3	3	Alto (3)	6	
		R4	Manipulación de programas	Bajo (1)	1	3	3	3	3	Alto (3)	3	

Figura 3. 8: Estimación del riesgo
Fuente: Elaboración propia

La manera de reducir los riesgos depende de cómo aplicar controles o buenas prácticas, como se muestra en el cuadro de análisis de riesgo de la figura 3.9.

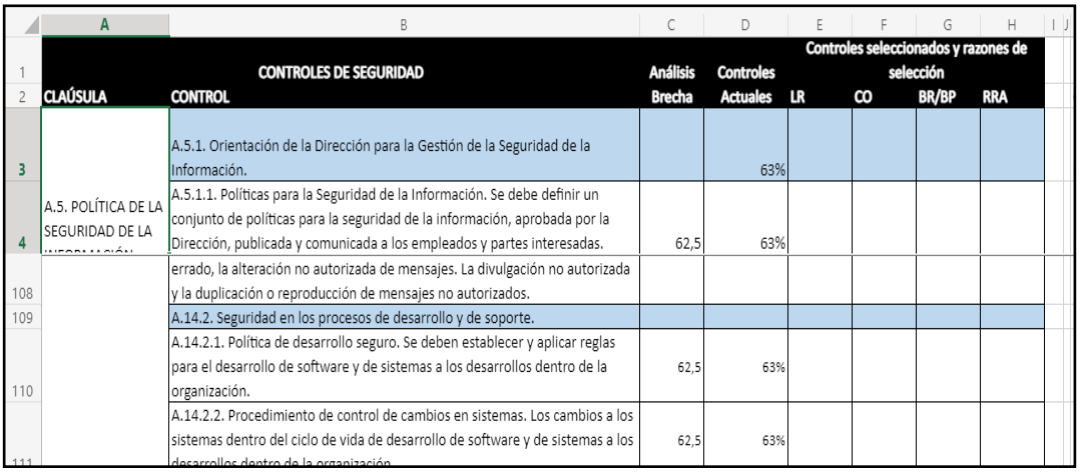
Activo		Id Riesgo	Amenaza	Riesgo	Controles	Reducir Riesgo
					A.8.2.3. Manejo de Activos. Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	13%
					A.8.3.3. Transferencia de medios de soporte físicos. Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	75%
	HW100	R3	Acceso no autorizado	9	A.9.1.1. Política de Control de Acceso. Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	63%
					A.11.1.3. Seguridad de oficinas, salones e instalaciones. Se debe diseñar y aplicar seguridad física a oficinas, salones e instalaciones.	63%
Hardware					A.11.2.9. Política de escritorio limpio y pantalla limpia. Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una	

Figura 3. 9: Análisis de riesgo
Fuente: Elaboración propia y uso de la norma Iso/IEC 27000

3.3.2 Controles

Para mitigar los riesgos y poder reducir las probabilidades que ocurran o disminuir su impacto se plantea controles. Es necesario el uso de un Sistema de Gestión de Seguridad de la Información (SGSI) (ISO, 2021).

Se plantea una declaración documentada que define o detalla los objetivos de seguridad, así como las medidas adecuadas y aplicables para el SGSI de una empresa. Esto ayudará a asegurar la información de la organización y la disponibilidad de la información con la integridad de los datos. Tal como se muestra en la figura 3.10.



	A	B	C	D	E	F	G	H	I	J
1	CONTROLES DE SEGURIDAD		Análisis	Controles	Controles seleccionados y razones de selección					
2	CLAÚSULA	CONTROL	Brecha	Actuales	LR	CO	BR/BP	RRA		
3		A.5.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información.		63%						
4	A.5. POLÍTICA DE LA SEGURIDAD DE LA	A.5.1.1. Políticas para la Seguridad de la Información. Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.	62,5	63%						
108		errado, la alteración no autorizada de mensajes. La divulgación no autorizada y la duplicación o reproducción de mensajes no autorizados.								
109		A.14.2. Seguridad en los procesos de desarrollo y de soporte.								
110		A.14.2.1. Política de desarrollo seguro. Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas a los desarrollos dentro de la organización.	62,5	63%						
111		A.14.2.2. Procedimiento de control de cambios en sistemas. Los cambios a los sistemas dentro del ciclo de vida de desarrollo de software y de sistemas a los desarrollos dentro de la organización.	62,5	63%						

Figura 3. 10: Declaración Aplicativa del sistema de gestión.
Fuente: Elaboración propia y uso de la norma Iso/IEC 27000

Conclusiones

La Empresa que escoja en trabajar con entornos virtualizados debe contemplar y asegurarse que sus aplicaciones o herramientas pueden no funcionar de igual manera en este tipo de entorno virtualizado. Cabe recalcar que debe realizar un análisis de todo su desarrollo lógico.

Al pensar en un entorno virtual, no debe separar la parte física, ya que es contenedor de la parte virtualizada, el trato de proteger la información debe ser el mismo. La seguridad de los equipos físicos debe considerarse también una prioridad ante los distintos ataques.

Aplicar estándares internaciones de organismos especializados en la seguridad informática y de la información a nivel mundial, seguir fuentes de información actualizada de las posibles vulnerabilidades que puede causar impactos fuertes en el entorno virtualizado.

La instalación de los equipos virtualizados debe tener todos los manuales que es entregado por proveedores, para evitar una mala configuración de los equipos físicos y lógicos, tomando en cuenta que los sistemas operativos deben ser actualizados periódicamente.

Recomendaciones

Crear políticas de seguridad contra las amenazas externas, es decir impactos ambientales, perdida de energía, el clima, cables de comunicación, backup de UPS y todo que permita que la parte física funciones para que las máquinas virtuales ofrezcan los servicios de la empresa.

El manejo de entornos virtuales debe ser configurado y monitoreado por personal técnico altamente capacitados, tener dentro de su plan de trabajo capacitaciones continúas a sus técnicos. Uno de los errores frecuentes es la mala configuración de equipos físicos y virtuales.

Tener actualizados los parámetros descritos en la NORMA ISO/IEC 27005 para el análisis de riesgo y la gestión de riesgos, aplicando criterios claros de controles para evitar las amenazas y que este provoque impactos muy altos a la organización. Además de tratar los riesgos, verificar la incidencia de ataques, para ser controlados con las políticas creadas.

Bibliografía

Arévalo, F., Cedillo, I., & Moscoso, S. (2017). *Metodología Ágil para la Gestión de Riesgos Informáticos.* Obtenido de Revista Killkana Técnica Vol. 1 Num. 2 (2017). Universidad Católica de Cuenca: https://killkana.ucacue.edu.ec/index.php/killkana_tecnico/article/view/81

Art4Software. (2012). *Virtualización (I) – Introducción & Hypervisor.* Obtenido de http://www.art4software.com/2012/05/virtualizacion-i-introduccion-hypervisor/

Cabrera, A. (2017). *Diseño e implementación de virtualización con Vsphere sobre servidores blade, dentro de una zona desmilitarizada linux para ambientes de pruebas de software web en el departamento de desarrollo de la empresa Transoceánica C. Ltda.* Obtenido de Repositorio Institucional de la Universidad Politécnica Salesiana: https://dspace.ups.edu.ec/handle/123456789/15005

Cerrada, J. (2012). *Evolución de la estrategia IT apoyada por la virtualización.* Obtenido de Repositorio Universidad Politecnica de Catalunya: https://upcommons.upc.edu/handle/2099.1/15054

Chahin, J. (2015). *Metodologia ACRD para la gestion de seguridad en entornos virtuales.* Obtenido de Repositorio de la UNIR: https://reunir.unir.net/bitstream/handle/123456789/3510/CHAHIN%20NORE%C3%91A%2C%20JUAN%20ANTONIO.pdf?sequence=1&isAllowed=y

Congo, M. (2014). *Implementar un servidor Hosting Linux compartido y servidores dedicados utilizando virtualización para la empresa Undermedia S.A.* Obtenido de Repositorio de la Escuela Politecnica Nacional: https://bibdigital.epn.edu.ec/bitstream/15000/8099/4/CD-5703.pdf

Descalzo, F. (2016). *Riesgos actuales en entornos virtualizados.* Obtenido de Cybsec: http://www.cybsec.com/upload/Descalzo_Riesgos_Virtualizacion_v1.pdf

Doña, J., García, J., López, J., Pascual, F., & Pascual, R. (2012). *Virtualización de Servidores. Una Solución de Futuro.* Obtenido de redtauros: http://www.redtauros.com/Clases/Gestion_SO/Sistemas_paravirtuales.pdf

Enriquez, V., & Hidalgo, P. (2015). *Metodología de Valuación de Riesgos Como Parte del Sistema de Gestión de Seguridad de la Información (SGSI) Aplicado a un Data Center de Alta Gama.* Obtenido de Revista Politécnica Vol. 36, No. 1: https://revistapolitecnica.epn.edu.ec/ojs2/index.php/revista_politecnica2/article/view/494/pdf

Eset. (2021). *Security Report Latinoamérica 2021.* Obtenido de welivesecurity.com: www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf

ISO. (2021). *ISO standards are internationally agreed by experts.* Obtenido de ISO Standards: https://www.iso.org/standards.html

linuxprience. (2012). *Easy configuration 4 Linux Debian's services.* Obtenido de http://linuxprience.blogspot.com/2012/08/1-virtualizacion-con-xen.html

Mendoza, M. (2016). *Gestión de la seguridad en ambientes virtualizados: ¿con o sin agente?* Obtenido de Eset: https://www.welivesecurity.com/la-es/2016/01/20/seguridad-en-ambientes-virtualizados-agente/

Mero, J., & Gallegos, H. (2015). *Análisis de factibilidad de migración de los servidores físicos a servidores virtuales Citrix Xenserver en la empresa Ecuavía S.A.* Obtenido de Repositorio Universidad Politécnica

Salesiana : https://docplayer.es/amp/2713382-Universidad-politecnica-salesiana-sede-guayaquil.html

Niño, D. (2020). *Diseño de un modelo de virtualización para la implementación de un sistema de servidores en alta disponibilidad.* Obtenido de Repositorio Institucional UCC: https://repository.ucc.edu.co/handle/20.500.12494/17050

Ramírez, G., & Robalino, A. (2014). *Diseño e implementación de servicios de virtualización de los servidores que operan en el centro de operación de la red (NOC) de la Facultad de Ingeniería de Sistemas.* Obtenido de Repositorio Digital Institucional de la Escuela Politécnica Nacional: https://bibdigital.epn.edu.ec/handle/15000/9002?locale=de

Ramírez, J. (2011). *Virtualización de Sistemas Operativos.* Obtenido de MasQteclas: https://www.masqueteclas.com/articulo/virtualizacion-de-sistemas-operativos/

Raya, J. (2009). *Guía de campo máuinas virtuales.* Ra Ma.

Robles, M. (2017). *Virtualización de servidores con VMWARE.* Obtenido de Universidad San Martín de Porres: https://www.usmp.edu.pe/vision2017/pdf/materiales/VIRTUALIZACION_DE_SERVIDORES_CON_VMWARE.pdf

Sistem@t. (2012). *Virtualización.* Obtenido de http://mat1258.blogspot.com/2012/07/virtualizacion.html

Valentim, H., Pereira, N., & Couto, R. (s.f.). *Virtualization Technologies.* Obtenido de SlidePlayer: https://slideplayer.com/slide/5725906/

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Albán Ortiz Erick Fabián** con C.C: # 1106038258 autor del Trabajo de Titulación: **Estudio y Análisis de seguridades en servidores virtualizados,** previo a la obtención del título de **INGENIERO EN TELECOMUNICACIONES** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 15 de septiembre del 2021

f. _____

Nombre: Albán Ortiz Erick Fabián
C.C: 1106038258

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Estudio y Análisis de seguridades en servidores virtualizados		
AUTOR(ES)	ALBÁN ORTIZ ERICK FABIÁN		
REVISOR(ES)/TUTOR(ES)	MSc. Romero Paz, Manuel De Jesús		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Educación Técnica para el Desarrollo		
CARRERA:	Ingeniería en Telecomunicaciones		
TITULO OBTENIDO:	Ingeniero en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	15 de septiembre del 2021	**No. DE PÁGINAS:**	65
ÁREAS TEMÁTICAS:	Sistemas Operativos, Máquinas Virtuales, Servidor Virtual Privado, Cloud Computing, Host		
PALABRAS CLAVES/ KEYWORDS:	Virtualización, Servidores, Nube, Transmisión, Red, Seguridad		

RESUMEN/ABSTRACT: La virtualización es un tema frecuentemente aplicado por la tecnología de información y comunicación, y cada vez va evolucionando y provocando un avance muy productivo para usuarios y empresas, en la cual consiste en permitir que varias máquinas virtuales con sistemas operativos puedan ejecutarse individualmente, operando en la misma máquina física, por tal razón se debe considerar los problemas a los que se puede llegar a tener a un futuro, ya que como todo va evolucionando de igual manera lo harán los problemas de la fiabilidad de la información. Al momento de virtualizar los sistemas de información, se llega a obtener un mayor de ahorro de energía, un favorable espacio físico y un ahorro considerable recursos económicos, aunque lo que conlleva a establecer un sistema de seguridad para los servidores virtualizados que permitan identificar las amenazas que lleguen a existir en la red. En el proyecto propuesto, consiste en proporcionar seguridad a servidores en los entornos virtuales, con el fin de combatir las vulnerabilidades a los que está expuesto dicho servidor, debe garantizar que la información debe estar disponible, integra y confiable. La virtualización tiene como beneficio tener distintos servicios en diferentes equipos, evitando que colapse en la transmisión de sus datos, su administración es más sencilla de controlar, en la actualidad muchas empresas prefieren alquilar VPS, cloud computing, hosts u otros, todo espacio en la nube es mucho más económico que tenerlo en el cuarto de comunicaciones.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593968526600	E-mail: erick.alban01@cu.ucsg.edu.ec
CONTACTO CON LA INSTITUCIÓN: COORDINADOR DEL PROCESO DE UTE	**Nombre:** Palacios Meléndez, Edwin Fernando	
	Teléfono: 593-967608298	
	E-mail: edwin.palacios@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	