Universitat Oberta de Catalunya

TRABAJO DE FIN DE MÁSTER

Gestión de Seguridad en Virtualización de Servidores

Sistemas de autenticación y autorización

Autor: Felipe Emiliano Arévalo Cordovilla

Tutor: Pau del Canto Rodrigo

Diciembre, 2018

Agradezco a Dios por todas las bendiciones que me ha dado. A mi familia, por estar siempre pendiente de mí y apoyarme durante mi carrera estudiantil; ellos que son mi motor, que han proporcionado toda la energía para llevar a cabo y tratar de cumplir cada uno de mis propósitos.

Resumen

Este proyecto trata el tema de seguridad en Servidores Virtuales en el Cloud, específicamente en la parte relacionada al Infrastructure as a Service (IaaS).

Se toma el caso específico de la minimización del riesgo relacionado a la seguridad al instalar maquinas virtuales en servidores físicos. Se analiza y describe como una maquina virtual vulnerable, puede comprometer a las otras máquinas virtuales vecinas e inclusive al servidor físico.

En este estudio se propone un nuevo método de cuantificación del riesgo de seguridad para las máquinas virtuales. Los resultados arrojados por este método son tomados en cuenta para decidir la ubicación de un nuevo servidor virtual en un servidor físico y por ende minimizar el riesgo relacionado a la seguridad.

Como resultado de este estudio, se provee un manual de buenas practicas y medidas mínimas a tomar para maximizar la seguridad de los servidores virtuales.

Palabras clave: Virtualización, IaaS, seguridad Informática, Cloud

Abstract

This project focuses on the field of Security in Virtual Servers in the Cloud environments. Specifically, the security at the IaaS is studied.

The specific case related to minimization of risks when allocating new virtual machines into physical machines is studied. The case of how a vulnerable virtual machine that is allocated in a physical server can compromise the neighboring virtual machines and even the physical server is explained.

In this study a new method for quantifying the security risk of virtual machines is proposed. This parameter helps in the decision making task for choosing the phisical server to install the new virtual server in order to maximize the security.

A security good practice guide focusing on Virtual Server Security is provided in this document.

Keywords: Virtualization, information security, security threats, IaaS, Cloud

Índice general

Índice de figuras

Siglas

AMD Advanced Micro Devices. 26, 27

AWS Amazon Web Services. 35

CERT Computer Emergency Response Team. 37, 45

CPU Central Processing Unit. 26, 27, 32

CSIRT Computer Security Incident Response Team. 37, 45

CTSS Compatible Time Sharing System. 25

CVE Common Vulnerabilities and Exposures. 37, 38

CVSS Common Vulnerability Scoring System. 37, 38

DHCP Dynamic Host Configuration Protocol. 30

DNS Domain Name Service. 30

FIRST Forum of Incident Response and Security Teams. 37, 45

FTP File Transfer Protocol. 39

HTTP Hypertext Transfer Protocol. 39

IaaS Infrastructure as a Service. 4, 12, 15, 16, 18, 35, 36, 45

IDS Intrusion Detection System. 14

IP Internet Protocol. 40

IPS Intrusion Prevention System. 14

MV Máquina Virtual. 13, 14

NVD National Vulnerability Database. 37–39, 45

PaaS Platform as a Service. 12, 35

RAM Random Access Memory. 31

ROI Return of Investment. 29

SaaS Software as a Service. 12, 35

TCO total Cost of Ownership. 29

TIC Tecnologías de la Información y Comunicación. 11, 12, 28

VLAN Virtual Local Access Network. 31

VMM Virtual Machine Monitor. 25–27, 31, 34

1 Introducción

1.1. Contexto y justificación

El mundo actual se caracteriza por la creciente tendencia al uso de las Tecnologías de la Información y Comunicacións (TICs), de los paquetes ofimáticos, de programas administrativos y contables, de programas educativos, entre otros, en todos los ámbitos de la sociedad. Estos recursos son utilizados tanto por organizaciones públicas, privadas, en el sector educativo, el sector industrial y empresarial, llegando a convertirse para todas estas instituciones en un factor importante de eficiencia, de competitividad y de asegurar la prestación de un mejor servicio o producto.

Es el mejor aprovechamiento de estos recursos lo que le permite a las organizaciones ir añadiendo calidad y valor a los servicios o productos que ofrecen. Uno de los problemas de mayor envergadura a los que las empresas u organizaciones deben enfrentarse para alcanzar estos objetivos, y principalmente las pequeñas y medianas, es el que se relacionan con la capacidad del crecimiento, del uso del hardware y software para cubrir sus necesidades operativas y les obliga a tener que abordar de forma continua aquellos temas que se relacionan con los costos, versatilidad, escalabilidad y funcionabilidad de estos componentes.

Entre las opciones que existen para hacer frente la problemática descrita se encuentra la virtualización, es decir, crear máquinas virtuales que dupliquen el funcionamiento integro de la máquina real, "engañándola" para que funcione con toda su potencialidad como si se ejecutara una máquina normal cuando se está ejecutando es sobre una máquina virtual.

La virtualización de los sistemas y herramientas se ha convertido en una de las soluciones más económica, provechosa y eficiente para dar respuesta a los problemas que se relacionan con el mejor aprovechamiento de estos recursos en la medida que les permite a las organizaciones darle un mejor uso y manejo de los recursos computacionales al mismo tiempo que logran disminuir el costo total asociado a los mismos. La proliferación de nuevas tecnologías en las distintas áreas que conforman las soluciones actuales de TICs ha traído como consecuencia tener que afrontar nuevos retos, y aunque la virtualización no es un proceso nuevo, el auge que ha logrado en los últimos lustros se debe a que los beneficios que ofrecen superan estos nuevos retos.

La posibilidad que ofrece la virtualización de poder implementar ambientes virtuales que les permiten a las instituciones realizar muchas de sus funciones si necesitar de poseer los costosos hardware tradicionales se ha utilizado hasta la actualidad. Por otro lado, las tecnologías móviles virtualizados y las redes virtuales permiten que hoy día, las organizaciones realicen sus procesos vitales a través de puestos de trabajos que no se encuentran en las sedes físicas de la organización permitiéndole prescindir de la presencia física de los usuarios y trabajadores. La virtualización es una opción de las mejores opciones ya que sus beneficios; una mayor eficiencia, mo-

vilidad, portabilidad y descentralización a costos más económicos en comparación a la de los sistemas físicos le han permitido abrirse camino para que muchas organizaciones acepten la idea de la implementación de sistemas híbridos con servidores virtualizados a nivel local, pero la virtualización ha traspasado la frontera organizacional, en la actualidad la Cloud Computing se presenta como una nueva tendencia en TICs que se hace cada vez más popular, que representan cambios importante en la forma en la que se almacenan y ejecutan aplicaciones de escritorio, aplicaciones y servicios Web, por medio de un a autoservicio bajo costos, moviendo la computación a la nube.

El cloud computing como una nueva forma de operar proporciona una infraestructura eventualmente ilimitada para almacenar y ejecutar datos y programas de clientes en donde los clientes no necesitan tener su propia infraestructura, sino sólo acceso vía Web, entre los principales modelos de servicio que ofrece el cloud computing se encuentra:

1. La Nube Software as a Service (SaaS), en donde el consumidor utiliza las aplicaciones del proveedor que se ejecutan en la infraestructura de nube y son accesibles desde diversos dispositivos cliente (PCs-notebooks, teléfonos móviles, iPhones, etc.) utilizando una interfaz cliente ligero como un navegador Web.

2. La Nube Platform as a Service (PaaS), que le proporciona al cliente un conjunto de aplicaciones creadas por el propio cliente que pueden ser virtualizadas y hospedadas en la nube.

3. La Nube IaaS, en donde la capacidad proporcionada al cliente es la capacidad de procesamiento, almacenamiento, redes y otros recursos de computación fundamentales donde el consumidor puede desplegar y ejecutar software arbitrario que puede incluir sistemas operativos y aplicaciones virtualizados.

Pero estas nuevas tecnologías y sus ventajas no se encuentran exenta de problemas o riesgos, vale señalar que la principales desventajas que presentan es la que se relaciona con la seguridad de estos entornos, esta desventaja de seguridad se materializa en un aumento “casi exponencial” de la superficie de ataque del entorno virtualizado y en los cloud computing se manifiesta en la protección de la seguridad y privacidad de datos y programas y de la falta de un control directo por parte del usuario.

Por un lado, los eventos que ocurren fuera del entorno virtualizado, en casi su totalidad no están bajo el control de las personas encargadas de la administración, control y resguardo del sistema, este factor aumenta el riesgo de ataques evidenciando la necesidad de tener que utilizar metodologías de seguridad basadas en políticas de seguridad claras que normen el uso, el acceso, la disponibilidad y manejo de los recursos ofrecidos por el entorno. Por otro lado, a nivel de cloud computing el consumidor no gestiona, ni controla la infraestructura de nube subyacente, aunque puede tener control sobre los elementos y herramientas que se encuentran alojadas en cualquier de los modelos de servicio.

El argumento anterior, explica porque muchas organizaciones aún sopesan la idea de la implementación de esta tecnología, porque aún no se han decidido dar este paso y para no darlo se basan en la creencia, que existe en un segmento significativo

de los administradores de sistemas informáticos, de que no se puede administrar de forma segura aquello que no se puede ver, y como los entornos virtualizados, sean a nivel organizacional o en la nube, no existen en realidad sino que son un "engaño" al sistema para que crea que corre en una maquina real, ésta percepción va en detrimento de la implementación y el uso de los entornos virtualizados, lo que podría agravarse si a los entornos virtualizados a nivel local se le suma que debido a su fácil movilidad acarrearían problemas de separación y fragmentación de las zonas que habitualmente se consideran seguras.

Mientras que a nivel de la nube, además de los nombrados aparecen otros problemas como pueden ser; vulnerabilidades en el proveedor de cloud computing, ataques a nivel de Máquina Virtual (MV) aprovechándose de vulnerabilidades en el hipervisor o tecnología MV utilizada por los proveedores de nubes lo que es muy común en arquitecturas de multi-arrendamiento, Phishing/Scams en proveedores de cloud computing, dificultad para realizar análisis forense en la nube, dificultad para la autenticación y autorización, expansión de la superficie de ataque de red, entre otros.

La aparición de estas fisuras de seguridad en los entornos virtualizados a nivel organizacional se deben a que el flujo de información entre máquinas virtuales no atraviesa ningún dispositivo de seguridad perimetral de los existentes, originando los denominados "Puntos Ciegos"para la seguridad. Estos puntos caracterizan por la inexistencia de los registros del tráfico de información que ocurren entre máquinas virtuales por no generarse las trazas que normalmente son generadas en los dispositivos físicos que permiten realizar un seguimiento de control del flujo de la información.

La imposibilidad de visualizar el tráfico entre máquinas virtuales genera un riesgo que se podría considerar inaceptable debido a la existencia de posibles amenazas desconocidas circulando por el hipervisor. Es la aparición de estas fisuras en la seguridad en los sistemas virtuales que se hace de suma importancia implementar políticas de seguridad efectivas para lograr el adecuado manejo y gestión de forma segura de los sistemas virtualizados y así proteger la inversión realizada, al mismo tiempo que se protegen los recursos informacionales e informáticos de la organización contra los riesgos existentes. A nivel de Cloud Computing son los proveedores los principales encargados de darle solución a los problemas de seguridad son los proveedores del servicio.

En este sentido, cabe señalar que la implementación de nuevas tecnologías arrastra consigo el tener que afrontar nuevos riesgos que deben ser identificados y tratados de forma oportuna con el objetivo de mitigarlos y de esta forma disminuir el nivel de inseguridad y de vulnerabilidades al que pueden verse sometidos los sistemas y la información por la aplicación de estas nuevas tecnologías.

En la actualidad, la inseguridad de los sistemas informáticos y de las redes sean éstas normales o virtualizados, en este mundo interconectado por la súper autopista del internet, se encuentra más allá de los ataques tan comunes de los virus informáticos existentes, hoy se hace necesario darle prioridad a la implementación de mecanismos de protección de naturaleza administrativa contra los posibles ataques de los agentes externos a la organización con el objetivo de atacar la información institucional con la finalidad de copiarla, transmitirla a terceros, modificarla o en el peor de los casos de destruirla.

En relación con lo anterior, en [1] el autor manifiesta que las herramientas que en

la actualidad existen para brindar seguridad a los sistemas clásicos de naturaleza física cuando se implementan en sistemas virtualizados presentan

> "limitaciones que restringen su eficacia en entornos virtuales. Estas limitaciones pueden también reducir o eliminar muchos de los beneficios de la virtualización cuando las herramientas de seguridad diseñadas para sistemas físicos se implementan o asignan a los entornos virtuales"(p. 13)

, afectando de forma negativa a estos entornos virtuales y por consiguiente su seguridad.

El efecto anterior ocurre ya que este programa no cuenta con los mecanismos que les permitan detectar que se encuentran ubicados en un entorno que está virtualizado en donde debe compartir los recursos del servidor con las otras máquinas virtuales que se encuentran en misma máquina virtual física.

Si bien es cierto que en [1], el autor señala que las plataformas de infraestructura virtual son entornos que presentan los mismos inconvenientes de seguridad que las que presentan los entornos físicos, también sostiene que estos entornos presentan problemas adicionales que son muy propios y característicos de los sistemas virtualizados.

Para Ilustrar lo anterior, el autor explica.

> "El hipervisor de un entorno virtual es, de alguna manera, análogo al router de red de un entorno físico. Cada máquina virtual y aplicación hacen pasar su tráfico de red a través del hipervisor de camino a otros sistemas virtuales o físicos o a dispositivos del cliente. Dado que el hipervisor es parte de un sistema cerrado dentro de la infraestructura virtual, muchos productos de seguridad (por ejemplo, los cortafuegos y los sistemas de detección de intrusiones/sistemas de prevención de intrusiones Intrusion Detection System (IDS) e Intrusion Prevention System (IPS) en la red) no pueden ver el tráfico del hipervisor y crean, por tanto, una importante zona de exposición y un vector de ataques muy atrayente, especialmente debido a la variada mezcla de aplicaciones que pueden instalarse a modo de MV en una máquina anfitriona física ".(p. 13-14)

De la anterior, se debe entender que las máquinas virtuales en realidad son simplemente un agregado de procesos que se comunican entre ellos por medio del hipervisor y del uso de redes virtuales que se adecuan a las necesidades intercomunicacionales que se originan entre estos procesos y no constituyen representaciones similares a las físicas, nada es real por lo que resulta muy difícil realizar una aproximación acertada de seguridad si se trata a los entornos virtualizados como representaciones físicas, lo anterior hace necesario tener que abordar nuevas perspectivas de seguridad para los entornos virtualizados.

Para minimizar la aparición de esta zona de exposición y de los posibles vectores de ataques es necesario tratar estas problemáticas de seguridad forma novedosa y eficiente cuya visión vaya más allá de la simple utilización de los programas de seguridad, una visión que se centre en la implementación de procesos administrativos de gestión de la seguridad con un enfoque integral de los riesgos que permita lograr un

adecuado balance entre control y usabilidad, que mitiguen las continuas amenazas sin perder la facilidad de uso de estos sistemas y la incorporación de nuevas tecnologías.

Es en este sentido, la meta que persigue este trabajo es el de presentar una propuesta de un Manual de Gestión de seguridad para entornos virtualizados con la finalidad de brindar un conjunto de orientaciones y políticas de seguridad informática que le sirvan de guía procedimental a los usuarios de esta tecnología para realizar una mejor gestión frente a los riesgos a que se encuentra expuestos estos tipos de entornos a fin de lograr un adecuado trabajo y ejecución de los procesos habituales sin verse afectados por estos riesgos o amenazas.

Esta propuesta se fundamenta en la inexistencia de medidas de seguridad concretas y homogéneas que sirvan de forma general para todos los entornos virtualizados, si bien se pueden decir que algunas compañías dadas a desarrollar programas para virtualizar se han preocupado por diseñar algunos manuales de cómo lograr una mayor seguridad de los entorno virtualizados que ellas desarrollan, estos manuales en la gran mayoría de los casos sólo cubren las necesidades específicas de sus tecnologías no siendo aplicables a entornos virtualizados creados con el uso de otras tecnologías de virtualización.

La propuesta busca ser un aporte para mejorar la gestión de los sistemas virtualizados sin importar bajo que tecnología de virtualización hayan nacido. Esta propuesta tiene su iniciativa en el hecho de que los sistemas virtualizados, sin importar cuál sea su tamaño u orientación de virtualización crecen cada día pero a la par de este crecimiento cada día es también mayor el número de atacantes más organizados y tecnificados que quieren aprovecharse de las debilidades presentes en los entornos virtualizados, y si a este hecho se suma las fallas de seguridad provenientes del interior mismo de la organización hacen necesario enfrentar y subsanar estas debilidades.

Aunque la propuesta de un Manual de Gestión de seguridad para entornos virtualizados está dirigida principalmente hacia estos entornos también abordan las amenazas informáticas que afectan por igual tanto a los sistemas basados en hardware como a los entornos virtuales, y aunque cada entorno posee una serie de condiciones que le son propias e inherentes, pero al momentos de implementar políticas y medidas de seguridad no son excluyentes entre ellas, sino más bien complementarias.

La implementación de nuevas tecnologías de virtualización, el manejo de las máquinas virtuales, la utilización de aplicativos a distancia, de los escritorios virtuales, y el desarrollo de redes virtuales exigen un mayor nivel en las políticas de seguridad que se deben implementar para permitir el acceso y la utilización de forma segura de estas herramientas por los diferentes usuarios. Frente a esta realidad se hace necesaria la implementación de controles administrativos que posibiliten la utilización de los diferentes recursos de forma segura disminuyendo o anulando los riesgos a los que se encuentran expuestos.

1.2. Objetivos del trabajo

1.2.1. Objetivo General

Maximizar el nivel de seguridad en el los entornos de servidores virtuales de IaaS, tanto a nivel de máquina virtual como de máquina física.

1.2.2. Objetivos Específicos

1. Proponer un mecanismo de ubicación de una maquina virtual en un servidor físico que permita minimizar el riesgo de incidentes de seguridad en el entorno IaaS.

2. Recolectar información sobre la protección de entornos físicos y entornos virtualizados.

3. Conocer las organizaciones mundiales que estandarizan y publican los nuevos hallazgos relacionados a la seguridad en el Cloud.

4. Diseñar el Manual de Gestión de seguridad para entornos virtualizados.

1.3. Enfoque y método seguido

El presente estudio se fundamentará en el paradigma positivista, el cual según Meza (citado por Hurtado y Toro, 2007), "... concibe la realidad como única y, la misma, puede ser fragmentada para su análisis y las partes pueden ser manipuladas independientemente" (p.58), lo que permite abordar un problema que en realidades solamente de un todo mucho mayor. El mismo está enmarcado en una investigación de campo de carácter descriptivo, definido por Hernández Sampieri, R, y otros en [2] como:

> "... aquellos estudios que buscan especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Es decir, únicamente pretenden medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables a las que se refieren, esto es, su objetivo no es indicar cómo se relacionan éstas."(p.92)

Las características de las investigaciones de campo es que se van a caracterizar porque los problemas que se estudian por medio de este tipo de investigación es un problema que se evidencia en la realidad. Es por ello que el presente estudio se enmarca dentro de este tipo de investigación debido a que, aunque la tecnología de la virtualización avanza a pasos agigantados no lo ha hecho de igual forma la tecnología, la normativa y los procedimientos administrativos y de gestión colaterales necesario para ofrecerle la adecuada seguridad al producto de esta tecnología.

En este sentido lo que se busca es la de lograr una unificación de los diferentes criterios que existen en el ámbito informático sobre la protección de los servidores, a los escritorios, a las redes o a los centros de información que han sido virtualizados para de esta forma realizar una selección de los más pertinentes a ser reunidos en un manual que sirva como un paso en pro de la búsqueda de solución de problemas dentro de ese contexto.

En función a los anterior es que la presente investigación se circunscribe en esa modalidad, debido a que el propósito fundamental es el de Presenta una propuesta de un Manual de Gestión de seguridad para entornos virtualizados que reduzca los riesgos y amenazas por medio de la aplicación de un conjunto de políticas de seguridad informática y administrativas que ayuden a una gestión de estos entornos.

Para la realización de este trabajo se ha seguido la estrategia de realizar la búsqueda, recopilación, análisis, selección del material informacional disponible en la internet u otro medio disponible para posteriormente utilizarlo en la preparación del Manual como una forma de presentar una guía de seguridad que sea homogénea a los diferentes entornos virtualizados y de esta forma superar la actual limitante de incompatibilidad que existen entra las diferentes políticas de seguridad aplicables a los entornos virtualizados.

1.4. Planificación del proyecto

El proyecto se dividirá en tres fases:

Primera fase: del 01 de octubre al 08 de octubre.

1. Elección de del tema a tratar en el proyecto.
2. Justificación y objetivos del proyecto.
3. Elaboración del plan de trabajo

Segunda fase: del 09 de octubre al 5 de noviembre. Investigación bibliográfica y digitalizada sobre:

1. Virtualización: definición, características, tipos de Virtualización, ventajas y desventajas
2. Programas de virtualización
3. El hipervisor, funciones
4. Seguridad Informática.
   a) Para sistemas físicos. Amenazas, herramientas de seguridad, normativa y protocolos de seguridad, propuestas de seguridad, trabajos sobre seguridad informática.
   b) Para sistemas virtualizados. Amenazas, herramientas de seguridad, normativa y protocolos de seguridad, propuestas de seguridad, trabajos sobre seguridad informática.

Tercera fase: del 05 de noviembre al 30 de noviembre.

1. Recolección del material a utilizar para la propuesta.
2. Análisis del material a utilizar para la propuesta.
3. Selección de del material a utilizar para la propuesta.

Cuarta fase: Del 15 de noviembre al 01 de diciembre

1. Estructuración y diseño de la Propuesta.

1.5. Alcance y limitación del plan

El alcance del presente Plan se suscribe a un proceso de investigación documental tanto a nivel de libros como en documentos digitalizados con el fin de ubicar todo el material posible que por medio del análisis, selección y compilación de la información pertinente a desarrollar el manual de Gestión de seguridad para entornos virtualizados.

La implementación de este plan se realizará con de diseñar un producto final de índole administrativo que contendrá un conjunto de políticas de seguridad para entornos computacionales, así como para virtualizados.

1.6. Principal contribución y producto obtenido

La principal contribución de este documento es la propuesta de un nuevo método para la cuantificación del riesgo al ubicar nuevas máquinas virtuales. Las fórmulas descritas en el capitulo 5 son netamente propuestas por el autor de este trabajo.

El método de reubicación de maquinas virtuales en un servidor físico se basa en un algoritmo pragmático de complejidad baja.

Para reforzar la seguridad en los servidores virtuales se adjunta un Manual de Gestión de seguridad para entornos virtualizados con el objetivo de exponer en el mismo un conjunto de medidas y políticas que sirvan de guía y ayuda para reducir los riesgos y amenazas a las cuales se encuentran sometidos estos ambientes o entornos.

La parte restante de este documento se compone de la siguiente manera:

En el capítulo 2 se presenta un estado del arte conciso sobre la seguridad en IaaS. En el capitulo 3 describe los conceptos más importantes sobre la seguridad informática y la seguridad en Servidores virtuales en el Cloud. A continuación en el capitulo 4 se describe el caso específico de la seguridad en IaaS. En este capítulo se trata sobre la cuantificación del nivel de vulnerabilidad en las maquinas virtuales. El capítulo 5 presenta la solución propuesta al problema expuesto en el capitulo 4. Los manuales de buenas prácticas de seguridad se encuentran detallados en los Anexos 7.1 y 7.2. Finalmente, en el capítulo 6 se presenta las conclusiones y trabajos futuros en este campo.

2 Estado del Arte

Para todo nuevo proyecto de investigación los trabajos que previamente se han realizado en la misma línea de investigación sirven como una guía de acción para el nuevo proyecto.

Los antecedentes que conforman el estudio están centrados en el análisis de algunas investigaciones que se han realizado anteriormente, con el propósito de comparar y comprobar los planteamientos que, de alguna manera, están relacionados con esta investigación.

En [3] el autor concluye que los servicios y productos de almacenamiento de datos en la nube permiten a sus usuarios guardar y compartir cualquier tipo de documento y archivo desde cualquier dispositivo conectado a Internet pero que estos almacenes de información son un objetivo para cualquiera que pretenda hacerse con información confidencial o privada debido a la existencia de amenazas tales como violación y pérdida de datos que ponen en riesgo la seguridad de la información almacenada en la nube y que los usuario debería ser consciente de las garantías de seguridad que los servicios ofrecen para tomar la decisión correcta en relación al servicio que se ajusta a las necesidades de cada usuario.

Los aportes de este trabajo es que permite visualizar que los servicios de Cloud computing aunque suelen ser considerados por los clientes muy seguros, y las compañías que ofrecen el servicios realizan grandes erogaciones de dinero para cada vez hacer que su servicio sean más seguros y confiables, el cliente es el primer interesado a asegurar su recursos e información.

En [4] los autores estudian el comportamiento de filtrado de los cortafuegos que proveen varios proveedores de Cloud. Este estudio afirma que solamente pocos proveedores tienen cortafuegos en sus infraestructuras. Los autores proponen una herramienta de monitoreo de cortafuegos que ayuda a los clientes del cloud a entender el comportamiento de filtrado de los cortafuegos en el Cloud.

En [5] los autores evalúan la sobrecarga de la red causada por la puesta en marcha de mecanismos de seguridad que realizan los clientes del cloud. Los autores proveen recomendaciones para que las organizaciones puedan planificar y optimizar la capacidad de red al implantar mecanismos de seguridad.

En [6] los autores evalúan las políticas de seguridad que provee la Agencia Europea de Seguridad de la Información ENISA [1] . Esta evaluación se centra en los parámetros de seguridad para el IaaS

Algunos autores han propuesto estrategias de ubicación de maquinas virtuales en el IaaS cloud [7], [8], otros se enfocan en la reducción del consumo de energía [9], [10]. Pocos estudios tratan la seguridad en el IaaS cloud como prioridad de investigación.

En [11], los autores proponen un algoritmo para ubicación de máquinas virtuales basado en incompatibilidades entre los usuarios. Cada usuario puede enviar una lista

[1] https://www.enisa.europa.eu

de usuarios adversarios donde detalla con quien no desean compartir una máquina física. Posteriormente la lista de adversarios se une para crear grupos incompatibles que son tomados en cuenta al ubicar o instalar una máquina virtual. Este trabajo aporta con una solución interesante para la mejora de la seguridad en el cloud, esta solución en resumen se basa en la isolación entre usuarios. Este mecanismo no toma en cuenta las preferencias de seguridad del usuario porque no incorpora ninguna métrica de seguridad.

En [12], los autores desarrollan una técnica basada en cadenas de Markov para la migración de máquinas virtuales. El objetivo de este mecanismo es minimizar los riesgos de seguridad considerando las conexiones entre las maquinas virtuales y al mismo tiempo mejorar la supervivencia de todo el cloud. Como desventaja, este mecanismo no considera el problema de ubicación de las nuevas máquinas virtuales.

En [13] los autores proponen un sistema de seguridad basado en métricas específicas para el cloud. Este mecanismos usa dichas métricas para crear algoritmos de ubicación de máquinas virtuales. La desventaja de este método reside en la negligencia de riesgos de seguridad causada por la coexistencia de maquinas virtuales en un mismo servidor físico.

En [14], los autores presentan un mecanismo para la asignación de recursos en el cloud que permite reforzar la seguridad en máquinas virtuales en el cloud. Este mecanismo modela las restricciones del proveedor y los requerimientos del cliente como un problema de satisfacción y restricción. Este problema puede ser solucionado usando un modulo de teorías de satisfacción el cual reduce el riesgo y mejorar la administración en el cloud. Esta solución no es óptima y solamente satisface las restricciones ingresadas.

Si bien existe varios estudios sobre la seguridad en el cloud, muy pocos de ellos se centran en la coexistencia de varias maquinas virtuales en un mismo servidor físico. La los estudios de seguridad no se enfocan en la ubicación de nuevas máquinas virtuales. Esta negligencia puede atraer graves consecuencias de seguridad. Pocos estudios toman en cuenta métricas de seguridad en el cloud. Este es un buen inicio para sustentar la propuesta de este documento.

3 Seguridad Informática y Virtualización

3.1. Conceptos de Seguridad Informática

El termino de seguridad informática se relaciona con el conjunto de herramientas informáticas que permiten ofrecerle la protección a la información y a los equipos que los contienen o los datos (lógicos o impresos); teniendo como objetivos la confidencialidad, disponibilidad e integridad.

En este sentido, Bustamante Sánchez, R. (S .A), en un trabajo realizado para optar al título de Ingeniero en Electrónica y Telecomunicaciones, titulado; Seguridad en Redes, sostiene que las políticas van a ser el entramado de leyes, reglamentaciones y procesos que tienen como finalidad regular, normar y ofrecer protección a los recursos tangibles como no tangibles con los que cuenta una organización.

Entre las razones que existen para brindarles seguridad a los equipos y a la información son:

a) Los equipos de computación y la infraestructura de redes son el principal campo de batalla.

b) La información que es un componente de mucho valor para todas las organizaciones.

Por otro lado problemas de la seguridad surgen por:

a) Crecimiento exponencial de las redes y usuarios interconectados.

b) Profusión de la base de datos on-line.

c) Inmadurez de las nuevas tecnologías.

d) Alta disponibilidad de herramientas automatizadas de ataques.

e) Nuevas técnicas de ataque distribuido.

f) Técnicas de ingeniería social.

En la actualidad, las organizaciones son cada vez más dependientes de sus sistemas y servicios de información lo que las hace más susceptibles a las nuevas amenazas de la era informática como pueden ser:

a) Loa accidentes de los equipos y las redes.

b) Las Intenciones presenciales originadas por los atentados con acceso físico que no son autorizado.

c) Intencionales remotas gracias a internet.

d) La corrupción o destrucción de la información de la organización.

3.1.1. Vulnerabilidad informática

Son las posibilidades del mismo ambiente, en el cual las características propician y se vuelve susceptible a una potencial amenaza, por lo tanto, se puede considerar como la capacidad de reaccionar ante la presencia de una amenaza o un daño.

Se es vulnerable a cualquier evento, sin importar su naturaleza, sea esta interna o externa, pero aplicando los controles adecuados es posible minimizar las posibilidades de que estas se materialicen, por lo tanto, los tipos de vulnerabilidades son:

Vulnerabilidad Física

Se refiere a la vulnerabilidad del entorno físico del sistema de información, equipos de cómputo y servidores, debido a que algún pirata informático ha violentado el acceso a la información de manera persuasiva para robar, modificar o eliminar información confidencial.

Vulnerabilidad Natural

Las vulnerabilidades naturales, son las ocasionadas por los desastres o eventos fortuitos en el medio ambiente, el cual ocasiona daños en los sistemas de cómputo por medio de los picos eléctricos, inundaciones, terremotos, temperatura alta y todos aquellos desastres naturales que son ocasionados por las variaciones atmosféricas y rozamiento de las placas tectónicas.

Vulnerabilidad del hardware y del software

a) Hardware

   Las vulnerabilidades de hardware hace referencia a las probabilidades de que las piezas físicas y/o dispositivos presenten fallas por descuido, mal uso o porque se ha dejado desprotegido los equipos de cómputo sin la seguridad adecuada para su manipulación.

b) Las vulnerabilidades de Software

   Las vulnerabilidades de software son conocidas como bugs del sistema o errores del software, el cual permite acceder a la funcionalidad y aplicación sin mayor esfuerzo por parte del pirata informático, ya que conoce el código fuente, tiene un mal diseño el software, o ha encontrado una puerta trasera para adherirse y conseguir información.

Vulnerabilidad de los medios o dispositivos

Las vulnerabilidades de los dispositivos y medios, son los daños, robos y descuidos humanos que permiten a terceras personas apoderarse de los discos duros, impresoras, equipos de cómputo, memorias USB y demás medios extraíbles que no posean un medio de seguridad adecuado.

Vulnerabilidad de las comunicaciones

Las vulnerabilidades de comunicación se encuentran asociadas a las redes y tipologías de conexión a través de diferentes puntos de red, esto quiere decir que si no se posee un método o herramienta que monitoree el tráfico de paquetes de datos por internet, los datos pueden ser capturados mientras el mensaje viaja por el internet.

Vulnerabilidad Humana

Las vulnerabilidades humanas radican en la falta de conocimiento sobre los métodos para proteger los datos y el acceso completo a las configuraciones del sistema informático, sin tener las restricciones adecuadas para identificar por medio de roles y usuarios el acceso conforme a la auditoría de cambio en el sistema de cómputo.

Vulnerabilidad Económica

Las vulnerabilidades económicas se enmarcan en la falta de recursos económicos, que permitan la adecuada inversión en sistemas, metodologías y demás elementos físicos y lógicos, para garantizar que los activos de información puedan protegerse de la mejor manera posible.

3.1.2. Amenazas informáticas

Es la posibilidad de que algún tipo de evento se pueda presentar en cualquier instante de tiempo, en el cual existe un daño material o inmaterial, sobre los sistemas de información, por lo tanto, se puede clasificar en:

a) Amenaza criminal: son aquellas acciones en las que intervienen seres humanos violando las normas y las leyes.

b) Sucesos de origen físico: son los eventos naturales que se pueden presentar, o aquellos eventos en los que el ser humano propicia las condiciones para determinar un hecho físico.

c) Negligencia: son las omisiones, decisiones o acciones que pueden presentar algunas personas por desconocimiento, falta de capacitación y/o abuso de autoridad porque tienen influencia sobre los sistemas de información, algunos porque no tienen ética para el desarrollo de la profesión.

3.1.3. Clasificación de las amenazas según el efecto causado en el sistema

a) Intercepción

   Es cuando un pirata informático o grupo de personas, logran ingresar a los sistemas de información sin autorización para escuchar, visualizar y copiar archivos confidenciales de las empresas, organizaciones y/o Pymes.

b) Modificación

Es cuando un pirata informático o grupo de personas, han logrado ingresar al sistema de información y además pueden modificar los archivos y/o líneas de código del software para ocasionar perdida de información, mal funcionamiento de los equipos de cómputo o programar cambios en los contenidos de las bases de datos.

c) Interrupción

La interrupción se da cuando los sistemas de información son saturados por medio de inyección SQL, código malicioso, virus, troyanos, gusanos y todas las aplicaciones que pueden ocasionar entorpecimiento en el sistema de información para un mal funcionamiento.

d) Generación

La generación de amenazas se da cuando se añade información en las bases de datos, registros y programas confidenciales, ocasionando daños internos y externos en los equipos de cómputo y prestación del servicio, ya que introduce mensajes no autorizados en cada uno de los comandos, registros y datos requeridos para un buen funcionamiento.

e) Amenazas Intencionadas

Las amenazas intencionadas son aquellas en la cual un grupo de piratas informáticos o una sola persona quiere conocer, modificar, eliminar y/o robar información para sus fines personales.

3.1.4. Principios fundamentales de las políticas de seguridad

En este sentido, Bustamante Sánchez, R. (S.A.), manifiesta que los principios generales de las políticas de seguridad son:

a) Responsabilidad individual: las personas son responsables de sus actos.

b) Autorización: son reglas explícitas acerca de quién y de qué manera puede utilizar los recursos.

c) Mínimo privilegio: la gente debe estar autorizada única y exclusivamente para acceder a los recursos que necesita para hacer su trabajo.

d) Separación de obligaciones: las funciones deben estar divididas entre las diferentes personas relacionadas a la misma actividad o función, con el fin de que ninguna persona cometa un fraude o ataque sin ser detectado.

e) Auditoría: el trabajo y los resultados deben ser monitoreados durante su inicio y hasta después de ser terminado.

f) Redundancia: el principio de redundancia afecta al trabajo y a la información. Múltiples copias son guardadas con importantes registros y dichas copias son frecuentemente almacenadas en diferentes lugares.

g) Reducción de Riesgo: Esta estrategia debe reducir el riesgo a un nivel aceptable, haciendo que el costo de la aplicación sea proporcional al riesgo. (p. 67-68).

3.2. Conceptos de virtualización

La virtualización es una tecnología que para Martin. D, Marrero, M, Urbano, J, Barra, E y Moreiro J.A. (2011), permite "la extracción del software de una computadora, encapsulándolo en algo que llamaremos máquina virtual, que será ejecutada en una máquina física ajena a la anterior" (p. 349), cuya principal ventajas consiste en una optimización del aprovechamiento del hardware que se traduce en una reducción de los costos de mantenimiento y administración de la red interna de la organización, ya que la misma permite transformar una intranet conformada por varios servidores, que en la mayoría de los casas están subutilizados a una estructura que se encuentra conformada por un número reducido de servidores que ofrecen los mismos.

3.2.1. Historia de la virtualización

La virtualización es un tecnología que tienes sus orígenes a principio de la década de los 60 de siglo 20, y su principal objetivo era el de permitir el particionamiento de los mainframes de gran tamaño con el objetivo principal de lograr mejoras en su uso.

Entre los primeros proyectos de virtualización se encuentra el de la IBM 7044, el cual consistía en una máquina física llamada la M44, la cual se encontraba integrada por varias máquinas lógicas 44X que se utilizaban para los procesos), por otro lado se tiene el desarrollado por el instituto de Tecnología de Massachusetts (en inglés, Massachusetts Institute of Technology, MIT) conocido como Compatible Time Sharing System (CTSS) que fue desarrollado sobre IBM 7044.

Un proyecto bastante llamativo es el proyecto Atlas de la Manchester University. Este proyecto alcanzo una importancia especial por su carácter innovador que dio respuesta los problemas que se originaban por el uso de una computadora central por un gran número de usuarios que accedían a la misma por medio de terminales. Este proyecto implemento un mecanismo que permitió el reparto y el acceso de forma simultánea de los recursos del computador, esencialmente del procesador y disco al mismo tiempo permitiendo que aseguraba el trabajo de los diferentes empleados de ninguna manera interfiriera en el de demás.

Se puede decir que la IBM en los años 60 da comienzo a los procesos de virtualización por medio de la implementación de particiones lógicas diferentes que se encontraran en un solo equipo. En este sentido, el primer computador que fue diseñado para el proceso de virtualización fue el mainframe IBM S/360 Modelo 67. Este Sistema Operativo cuyo nombre inicial fue el de S.O. de Supervisor o Virtual Machine Monitor (VMM) comenzó a evolucionar hasta llegar a convertirse en lo que en la actualidad se conoce como el Hipervisor.

En los años 80 se comienzan a utilizar los sistemas de cliente-servidor como una forma de hacerle la competencia a los Hosts, aprovechando la plataforma x86 que para la época comenzaba a robustecerse y adquiría solidez. Pero la plataforma x86

presentaba el problema de no cumplir con los requerimientos de virtualización de Popek y Goldberg, que establecía cuales eran las condiciones que debía cumplir una arquitectura para dar soporte a un sistema de virtualización de forma eficiente, ya que mientras los system/370 de IBM eran "compliant" y que los célebres Motorola 68000 son "no compliant", la arquitectura x86 tiene 17 instrucciones que generan problemas a la hora de virtualizar.

Va a ser pera finales de la década en de 1990, gracias a la fundación de la empresa VMware que comienza a desarrollar el proceso de virtualización para la plataforma de arquitecturas x86 de 32bits, este proceso tenía como función principal el solventar los problemas de rigidez y la subutilización de los mainframes de la época, para logra el acometido de lograr que la arquitectura x86 fuera "compliant" y pudiera dar los fruto de eficiencia y eficacia requerido, VMware desarrolló una técnica que interfiere, adapta y convierte en instrucciones seguras, dejando el resto de instrucciones trabajar de forma original.

Para el año de 1999 que VMware va a presentar el primer Hipervisor, como una solución a los problemas que se originan de que un solo recurso físico funcione como una diversidad de recursos lógicos.

La virtualización asistida por hardware que se encontraban al alcance de la mano gracias a los mainframes de IBM, a los servidores Sun y otras máquinas, va a vivir un resurgimiento a partir del año 2004 con la presentación de la tecnología VT de Intel, y posteriormente, en el año 2006 con la aparición de la AMD-V de Advanced Micro Devices (AMD).

Técnicamente lo que hace la virtualización asistida por hardware es hacer uso de circuitería en la CPU y chips controladores a fin de lograr mejoras en la ejecución y rendimiento de múltiples sistemas operativos que se encuentran instalados en una o varias máquinas virtuales. La virtualización con soporte hardware específico suelen tratar con funcionalidades y funciones como el almacenamiento y recuperación del estado de la Central Processing Unit (CPU) en transiciones entre el sistema operativo invitado (que corre en la máquina virtual) y el VMM, capa de virtualización que actúa como intermedio entre estos y el sistema operativo anfitrión y el hardware real disponible, gestionando los recursos y llamadas.

El proceso de virtualización se ha centrado la virtualización de servidores, logrando la partición de este recurso en una serie de servidores virtuales que funcionan como recursos físicos independientes, todo esto por medio del Hipervisor, que funge como el administrador de la virtualización, interactuando como un enlace entre el software y el hardware, asignándole al sistema operativo recursos como procesadores, memoria y unidades de almacenamiento.

3.2.2. Tipos de Virtualización

Emulación o simulación del hardware a nivel de aplicación

Por medio de una aplicación se logra la simulación entera del hardware lo cual permite que se logre la ejecución del sistema operativo sin que esta sufra modificación alguna, realizándose toda la ejecución bajo la administración del emulador que controla y simula el sistema completo, incluyendo la ejecución de las instrucciones a nivel de CPU.

Para Talens-Oliag, S (2010), "El emulador simula la ejecución de código binario para una CPU concreta en un sistema real que usa un procesador y un juego de instrucciones diferente al del sistema emulado" (p. 2).

Este modelo de virtualización presenta como principal inconveniente que la simulación es muy lenta debido a que para cada instrucción del sistema que se está emulando es necesario realizar un número bastante alto de instrucciones a la CPU real.

Virtualización completa o nativa sin apoyo hardware

De igual forma para Talens-Oliag (ob. cit) "Este tipo de sistemas usan una máquina virtual que hace de intermediaria entre el sistema invitado y el hardware real" (p. 2).

El hiperviso o monitor de máquina virtual (VMM) o hipervisor (hypervisor), es el encargado de emular un sistema completo y analiza dinámicamente el código que quiere ejecutar el sistema invitado, reemplazando aquellas instrucciones que son necesarias para la virtualización por nuevas instrucciones que logran que hardware virtual funcione como se desea, al mismo tiempo que permite la ejecución de aquellas instrucciones que no presentan ningún tipo de problemas en la CPU real.

Virtualización completa o nativa con apoyo hardware

A diferencia de la Virtualización completa o nativa sin apoyo hardware, y aunque funciona de igual forma que ésta, esta virtualización se apoya en las tecnologías que han sido incorporadas en los microprocesadores de la última generación ejecutando el código del sistema operativo invitado sin modificarlo ejecutando el hipervisor, en el anillo, es decir, en el máximo nivel de acceso a la en procesadores AMD e Intel, y en el anillo 0 ejecuta los sistemas invitados.

Es este tipo de virtualización debido a la introducción de un nivel superior al que realmente utilizan sistemas reales se logra que no se necesite realizar cambio alguno de los sistemas invitados, pero ahora es y es el hipervisor el que se va a encargar de administrar el acceso tanto de los dispositivos virtuales como de los reales por medio del requerimiento para acceder a los dispositivos desde los sistemas invitados que le realiza la CPU.

Paravirtualización

La paravirtualización es semejante a la virtualización completa, ya que de igual forma ejecutan el sistema invitado por medio de la ayuda del hipervisor el cual se va a ejecuta sobre el sistema real. La diferencia va a estribar que en este tipo de virtualización si es necesaria la modificación de los sistemas operativos invitado en donde se deben incluir un conjunto de instrucciones que tienen que ver con la virtualización, para que en vez de que sea el hipervisor el que capture las instrucciones problemáticas, sea el sistema invitado el encargado de realizar el llamado de forma directa al hipervisor cuando esto se requerido, pero independientemente de las modificaciones que se le deben realizar al núcleo del sistema invitado, los programas de usuario se pueden ejecutar sin ningún tipo de modificación.

La gran limitación que presenta este modelo de virtualización es la necesidad de tener que realizar la modificación del sistema operativo invitado, actividad que resulta imposible de realizar los sistemas operativos privativos y de código cerrado.

Virtualización a nivel de sistema operativo

Esta forma de virtualización se caracteriza por la creación de entornos de ejecuciones que son vistos como máquinas virtuales por las diferentes aplicaciones y que son ejecutadas solamente en el núcleo del anfitrión que es el encargado de crear estos entornos de ejecución.

En este sentido, Talens-Oliag (ob. cit) sostiene que "en este tipo de sistemas no hace falta emular el hardware a bajo nivel, puesto que en realidad es el mismo sistema operativo quién controla los dispositivos físicos" (p. 3), pero si es necesario el tener que apoyarse en la utilización de dispositivos virtuales, entre los que se encuentran los discos o tarjetas de red que se deben encontrar dentro de cada entorno de ejecución.

Esta forma de virtualización es una de las más económicas debido al hecho de que no necesita apoyarse en ningún hardware ni es necesario la constante supervisión del código abajo nivel, pero debido a que se ejecuta en un solo núcleo va a presentar como la principal limitación el hecho de que solamente va permitir que los entornos virtuales solamente se lleven a cabo para la misma CPU y sistema operativo lo que trae consigo que si el núcleo presenta algún tipo de problema, este afectara a todas las máquinas virtuales.

Virtualización de aplicaciones

Este tipo de virtualización es ideal cundo existen aplicaciones que son incompatibles entre sí ya que son ejecutadas en el sistema operativo, pero independientemente del mismo, convirtiendo las aplicaciones en servicios virtualizados que se ejecutan bajo una administración centralizada y debido a que no se hayan instalados en el CPU no se presentan conflictos entre las aplicaciones.

3.2.3. Ventajas de la Virtualización

La Corporación Computer Discount Warehouse, citado por Martin. D, Marrero, M, Urbano, J, Barra, E y Moreiro J.A. (ob. cit), realizo un estudio en mayo del 2010 por medio de su división CDW-G, cuyo fin principal fue el de analizar el estado de virtualización de agencias federales, estatales y locales en Los Estados Unidos de Norteamérica, en el mismo se llevaron a cabo 600 encuestas a directivos de empresas de tecnologías de las TICs llegando a concluir que entre las ventajas de la virtualización se encuentran:

1. Ahorro de costos; para la VM Ware Inc (2010), el proceso de virtualización arroja una relación de ahorro en la adquisición de hardware en una relación de 10 a 1 servidores en el caso más optimista, y de 6 a 1 en el caso más pesimista.

2. La Reducción del número de computadoras se refleja en una baja en el consumo de energía eléctrica y del dióxido de carbono que es emitido a la atmósfera.

3. Mejora de Costo Total de posesión (total Cost of Ownership (TCO)) y el Retorno de la inversión (Return of Investment (ROI)) que se deriva de la reducción del número de máquinas.

4. Reducción de los costes de espacio; menos máquinas se traducen en más espacios físicos libres.

5. La utilización de un número menor de máquinas y de una administración global centralizada y simplificada conlleva a un número menor de máquinas a las que se deben administrar, aunado al hecho de que el software de virtualización ayuda a la gestión remota de las máquinas virtuales.

6. Tecnología de fácil crecimiento debido a que permite la rápida incorporación de nuevos recursos para los servidores virtualizados por medio de la agregación de nuevas máquinas virtuales en una máquina anfitriona.

7. Mejora en los procesos de clonación y copia de seguridad del sistema: mayor facilidad para la creación de entornos de prueba que permiten utilizar nuevas aplicaciones sin afectar a la producción en un entorno controlado agilizando el proceso.

8. Un fallo general de sistema de una máquina virtual no afecta al resto de máquinas virtuales gracias al aislamiento e independencia que existe entre sí y con el hipervisor. Por tanto, un fallo en una aplicación o en una máquina virtual afectará únicamente a esa máquina virtual mientras que el resto de ellas y el propio hipervisor continuaran con su funcionamiento regular.

9. La posibilidad de poder virtualizar cualquiera de los diferentes elementos que conforman la estructura informática.

Igualmente Martín I. (2008), en un artículo que escribe para el portal web TechWeek.es, agrega otras ventajas a la virtualización como son:

1. Mayor seguridad debido a que cada máquina tiene un acceso privilegiado que es independiente que en casos de un ataque de seguridad sobre una máquina virtual sólo afectará a esa máquina.

2. Mayor Flexibilidad para crear las máquinas virtuales con las características de CPU, memoria, disco y red que necesitemos en un solo anfitrión.

3. Facilidad de creación de las máquinas virtuales es un proceso muy rápido, básicamente la ejecución de un comando

4. Gran Portabilidad de las máquinas virtuales debido a que las configuraciones de la misma se encuentran en pocos ficheros que encapsulan la máquina virtual lo que facilita el proceso de clonación o de transportar la máquina virtual a otro servidor por el simple copiando y movimiento de esos ficheros.

5. Rápida recuperación cuando ocurren fallo por medio del arranque de la máquina virtual con los ficheros de configuración guardados sin la necesidad de tener que volver a reinstalarlas o verse en la urgencia de tener que llevar a cabo los procedimientos largos que se suelen aplicar a los entornos reales.

3.2.4. Desventajas de la virtualización

En este sentido en un estudio realizado por Network Instruments (2009), citado por Martin. D, Marrero, M, Urbano, J, Barra, E y Moreiro J.A. (ob. cit), titulado; "Interop snapshot: virtualization deployments and challenges top of mind for attendee" en donde se trabajo con una población de 160 profesionales del sector de las TIC, en donde se llego a la conclusión de que la virtualización también ofrece algunas desventajas, entre las que se encuentran:

1. Despliegue extensivo: el 55 % de los encuestados ha realizado virtualizaciones de servidores críticos, un 50 % ha virtualizado servidores no críticos como servidores de Domain Name Service (DNS) y Dynamic Host Configuration Protocol (DHCP). Sólo el 39 % realizan una virtualización de escritorio.

2. Solución de problemas poco claro: el 27 % de los encuestados identifica una falta de visibilidad en la solución de problemas en entornos virtuales.

3. Trampas de la virtualización: el 55 % experimenta más problemas que soluciones, mientras que el 45 % restante piensa que los beneficios superan a los problemas, si no se sabe implementar adecuadamente.

4. Problemas con los administradores de virtualización: el 59 % opina que carecen de experiencia para gestionar adecuadamente la tecnología.

5. Costes de despliegue demasiado altos, según la opinión del el 47 % de los encuestados. (p. 352)

De igual forma, el estudio del estudio de Network Instruments manifiesta que la virtualización de una intranet básicamente debe cumplir con dos condiciones para que se puedan considerar exitosas, en primer lugar debe existir el compromiso de la dirección haciéndose necesaria la implementación de programas de formación que se fundamente en una política que propicie una constante formación y actualización tecnológica y técnica de los gestores, además de promover, incentivar y premiar el liderazgo.

En este mismo orden de ideas, Santero, J. C. (2016), sostiene que la virtualización puede presentar como desventajas las siguientes:

1. Disminución del rendimiento del hardware real debido a la ejecución de la máquina virtual en la capa intermedia del mismo y al hecho de que las aplicaciones se ejecutan de forma más lenta en las maquinas virtuales que si lo hicieran un servidor físico.

2. Mala compartición del servidor debido a una mala distribución de los recursos ya que en muchas ocasiones se suelen colocar servidores virtuales que consumen muchos recursos en el servidor real.

3. La única posibilidad de utilizar los hardwares que solamente son utilizados por el hipervisor debido a las restricciones que imponen los softwares virtualizados que solamente permiten hacer uso de los dispositivos que se encuentran disponibles en las máquinas virtuales.

4. No se puede realizar aceleración de videos por hardware ya que no se disponen de los efectos 3D del hardware anfitrión.

5. Necesidad de disponer de recursos suficiente de para los servidores virtuales.

6. La elección e instalación de dos servidores que consuman mucho ancho de banda suele producir problema de congestión de la red ocasionada por el servidor, teniendo sé que crear un bound en el servidor que permita aumentar al doble el ancho de banda.

3.2.5. Infraestructura de la Virtualización

Infraestructura Son los recursos necesarios Para conseguir un entorno virtual. Separando los distintos elementos se logra conseguir; Disponibilidad de recurso y del ambiente físico, flexibilidad, movilidad, escalabilidad, creación, y automatización del entorno.

Servidores (hosts) Junto con el hipervisor, los servidores conforman parte fundamental de la virtualización, ya que en ellos es en donde se va a ubicar el hipervisor, de igual forma los servidores son los encargados de ofrecer los recursos para la máquinas virtuales.

Normalmente, los servidores deben reunir unos requisitos que deben cumplirse para poder aplicar la tecnología de virtualización entre las que se pueden encontrar muchas gigas de memoria Random Access Memory (RAM) y suficientes tarjetas de red para la gestión de las máquinas virtuales y el almacenamiento.

Almacenamiento El almacenamiento compartido entre los servidores es una parte fundamental, nos va a permitir almacenar las máquinas virtuales en una ubicación central, para así obtener alta disponibilidad, live migration, balanceo de carga, snapshots, backups/restore, etc.

Se puede utilizar casi cualquier tipo de almacenamiento, SAN, NAS, ISCSI /NFS /FC /FCOE, lo importante es tener en cuanta siempre es el tipo y ancho de banda de la red para de esta forma evitar la aparición de un cuello de botella, o atascamiento del flujo de datos.

Red El diseño de la red para una infraestructura virtual es primordial, es necesario planear y personalizar los accesos de red para las diferentes máquinas virtuales que funcionan dentro de un hosts. Se hacen necesarios el uso de Virtual Local Access Networks (VLANs) y configuraciones personalizadas a nivel de red.

3.2.6. El Monitor de máquina Virtual (VMM o Hipervisor)

Para poder aplicar virtualización a una computadora o a un conjunto de ellas es necesario apoyarse en una plataforma conocida como hipervisor (hypervisor) o VMM, ésta plataforma es la que va a posibilitar el desarrollo de todo el conjunto de técnicas y procedimientos de control que van a permitir que en una sola computadora se pueda trabajar con sistemas operativos diferente de forma simultánea y al mismo tiempo.

El Hipervisor es la figura encargada de coordinar el trabajo entre estos sistemas operativos para que estos sistemas dentro del entorno de la máquina real que sirve de anfitriona compartan el hardware, el CPU, la memoria y los diferentes recursos que estén disponibles en la computadora.

3.2.7. Tipos de Hipervisor

García Garrido, J. C. (2010), afirma que existen dos tipos de hipervisores:

Hipervisor tipo 1

También denominado nativo, unhosted; que se ejecuta directamente sobre la máquina anfitriona, se encarga de repartir los recursos de memoria y dispositivos entre las diferentes máquinas huéspedes, este hipervisor pone en práctica una tecnología que se encarga de subdividir las tareas que realiza el procesador para que de esta forma gestione los diferentes sistemas operativos y aplicaciones en particiones que son independientes del propio chip.

Para que el procesador que sirve de anfitrión instale este tipo de hipervisor es necesario que cumpla los requisitos de instalación del mismo.

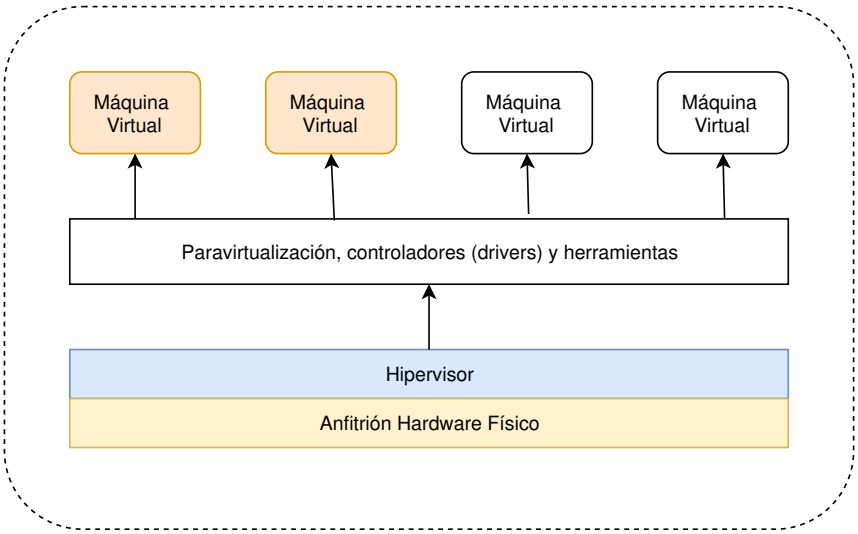

Figura 3.1: Hipervisor Tipo 1: Nativo

Hipervisor tipo 2

Llamados hosted que es un programa que se ejecuta sobre un sistema operativo y se ejecuta como una aplicación más dentro de un sistema operativo y da soporte a una máquina virtual que corren como procesos individuales.

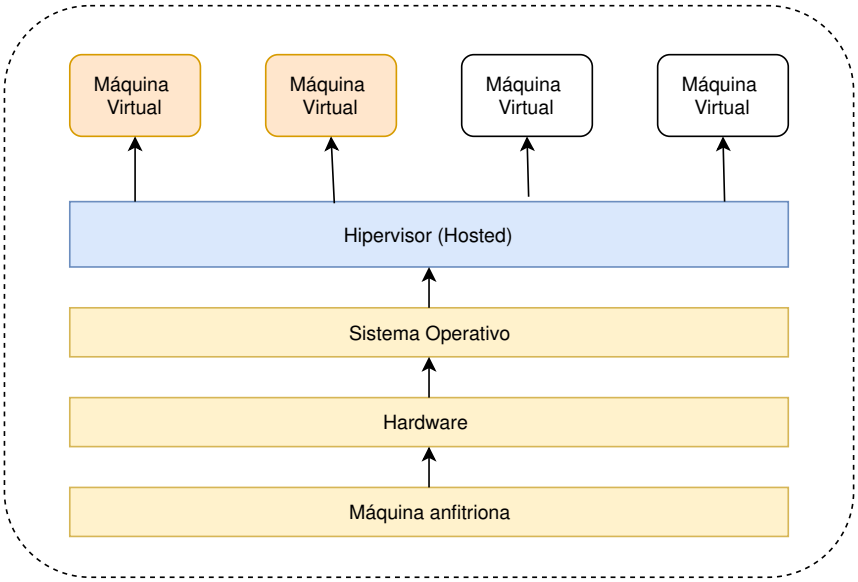

Figura 3.2: Hipervisor Tipo 2: Hosted

3.2.8. Retos de Seguridad del proceso de virtualización

En este orden de ideas, Campos, M. (2010), en un artículo publicado en internet en el portal de cso.computerworld.es, titulado Los seis riesgos de la seguridad en los entornos virtuales, sostiene que partiendo de los datos publicados por la consultora Gartner los principales riesgos a que presentan los entornos virtuales son:

a) No tener en cuenta la seguridad en los proyectos de virtualización

   En este sentido sostiene que el tema de la seguridad del entorno debe comenzar a realizarse previamente al proceso de virtualización basado en un plan de acción que contemple la arquitectura inicial al proceso ya que dar este paso significa realizar una serie de cambios que conlleva a una adecuación de los conocimientos y técnicas para poder brindarle una protección adecuada al flujos de trabajo, a los sistemas operativos y a los equipos es necesario la implementación de nueva tecnología que sea compatible con las maquinas virtuales no olvidando que las maquinas virtuales genera nuevas capas de software que no son contempladas por los sistemas y software de seguridad convencionales.

b) Las amenazas de la capa de virtualización afectaría a todas las cargas de trabajo dependientes

   Cómo la capa de virtualización es un software es sensible como cualquier software a presentar vulnerabilidades que son las tenidas en cuentas por los posibles atacantes para centrar sus ataques a este tipo de tecnología para afectar negativamente las cargas de trabajo y de esta forma afectar todas las operaciones que dependen.

c) Falta de visibilidad y control de las redes internas virtuales

   En este sentido Campos, M. (ob. cit), manifiesta que Gartner recomienda que, como mínimo, las organizaciones busquen el mismo tipo de control en las redes

virtuales que en las físicas, para no perder visibilidad y capacidad de gestión al dar el salto a la virtualización, ... pretendiendo reducir la posibilidad de una mala configuración"

Nuevamente centra su atención de que las herramientas de seguridad deben ser compatibles con las maquinas virtuales para que permita protegerlo desde dentro porque la administración de los sistemas virtualizados es una función exclusiva del hipervisor, herramienta que se encuentra sometida a los mismos riesgos que los demás componentes de los equipos clásicos , pero que al mismo tiempo se convierte en un nuevo vector de ataque, que si se le suma el hecho que las propias herramientas de gestión del proceso de virtualización generan nuevos vectores de ataques, sin importar como opere la tecnología virtualizadora, los riesgos se encuentran siempre presenta y aunque están de forma latentes, cabe destacar que lo importante es comprender que prioridad perenne es la de enfrenta as amenazas antes de que aparezcan y si aparecen deben ser enfrentadas atendiendo las condiciones propias del entorno.

d) Las cargas de trabajo de los distintos niveles de seguridad se consolidan en un único servidor físico sin la suficiente separación.

e) Un control inadecuado de acceso administrativo a la capa Hipervisor VMM y a las herramientas administrativas.

f) Pérdida potencial por la separación de las funciones de red y los controles de seguridad.

4 Seguridad en IaaS Cloud

En el Capitulo 1 se ha realizado una breve introducción sobre los servicios que ofrecen el cloud computing. Servicios como el SaaS, PaaS e IaaS han sido descritos. Este capitulo específicamente describe los diferentes factores a considerar en la seguridad en el IaaS, asi como los problemas a tratar.

La IaaS es una forma de hosting que incluye acceso de red, servicios de ruteo y almacenamiento. Los proveedores de servicios IaaS generalmente proveen el hardware y los servicios administrativos necesarios para guardar aplicaciones y plataformas para alojar y ejecutar aplicaciones, en resumen, un IaaS provee un ambiente para ejecutar sistemas virtuales en el cloud. Gracias a esta técnica, servidores virtuales son instalados con todo el software necesario que eventualmente se ejecutará en el cloud. El proveedor de IaaS tiene como responsabilidad asegurar la operatividad y el mantenimiento de la infraestructura virtual, sin embargo es responsabilidad del cliente el monitoreo de la operatividad del software y los servicios instalados en el servidor virtual.

Un ejemplo de proveedores de esta tecnología es Amazon Web Services (AWS) el cual ha tenido una gran aceptación la cual atrae un alto número clientes debido a la habilidad de ejecutar servidores virtuales con el más alto nivel de escalabilidad y flexibilidad.

4.1. El problema en Iaas Clouds

Uno de los actuales desafíos en la implementación de IaaS es determinar la ubicación de la máquina virtual, por ejemplo asignar cada máquina virtual a un equipo físico en la infraestructura del proveedor de IaaS Cloud.

Algunas estrategias han sido implantadas para IaaS, estas estrategias son basadas en varios criterios. Un ejemplo de esta estrategia es "network-aware placement"[7], [8]. Esta estrategia se basa en implantar varias maquinas virtuales con altos requerimientos de comunicación en una junto a otra con el fin de optimizar el consumo de energía eléctrica. Por otra parte la técnica "energy-aware VM placement "pretende optimizar la implantación y ubicación las máquinas virtuales con el fin de minimizar el consumo energético en el cloud [9], [10].

Existen pocos esfuerzos que incorporan el manejo de riesgos y seguridad en la implantación de maquinas virtuales. Los riesgos de seguridad es uno de los factores más importantes a considerar que influencian el desarrollo y la aceptación de de IaaS clouds en aplicaciones prácticas, pero lamentablemente en realidad prevalecen las vulnerabilidades mas comunes en máquinas virtuales públicas que los proveedores proveen [15] [16].

En [16] los autores mostraron que al escanear un cierto número de imágenes de máquinas virtuales, se encontró que las imágenes poseían información privada como claves, llaves y otras credenciales.

Esta información delicada que por negligencia existe en varias imágenes de máquinas virtuales, puede encadenar un considerable número de ataques hacia los otros servidores virtuales que se encuentran alojados en un IaaS Cloud.

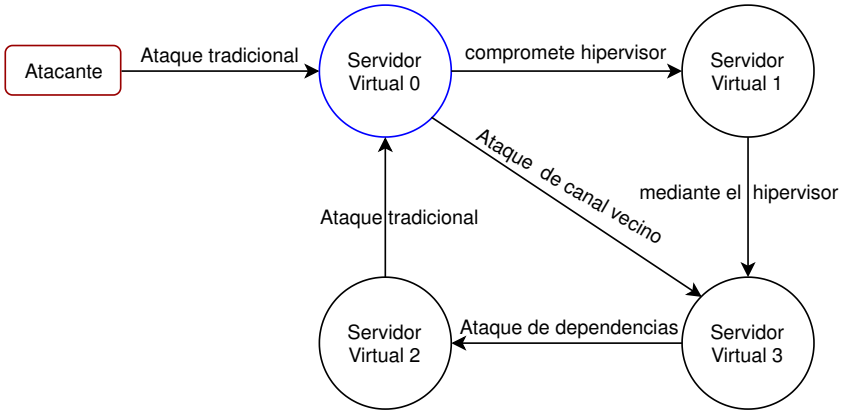

Figura 4.1: Ejemplo de grafo de ataque a maquinas virtuales

La Figura 4.1 muestra como cuando se introduce una nueva imagen de una máquina virtual en un servidor físico, existe un alto riesgo de vulnerabilidad hacia las imágenes de máquinas virtuales ya instaladas en dicho servidor físico.

Esto se debe al hecho del la relación 1 a n entre el servidor físico y las máquinas virtuales, lo cual hace que las vulnerabilidades se propaguen rápidamente en la infraestructura del IaaS. Inclusive el servidor físico que contiene todas las imágenes de las máquinas virtuales podría ser tomado por el atacante si la máquina virtual del hipervisor (Servidor virtual 1) se encuentra comprometida con las mismas vulnerabilidades que las otras máquinas virtuales.

Por ejemplo, uno de los ataques mas comunes en una infraestructura IaaS son los ataques de canal lateral a través del servidor virtual 1 por medio de la co-ubicación de los servidores virtuales. Los atacantes pueden mapear la ubicación de las maquinas virtuales internas en el cloud y realizar ataques de canal lateral instalando servidores virtuales maliciosos en la máquina física de la víctima.

En resumen, con el nuevo modelo de cloud público, es fácil para los atacantes lanzar ataques a través de vulnerabilidades predominantes.

Obviamente estos ataques son basados en la ubicación de los servidores virtuales y sus éxito netamente depende de las estrategias de ubicación del cloud. Por lo tanto, la ubicación de un servidor virtual puede causar un impacto en el las condiciones de seguridad del cloud.

Para minimizar los riesgos de seguridad en el cloud y poder aliviar la seguridad de servicios los clientes es necesario desarrollar una estrategia segura de ubicación de servidores virtuales en el cloud donde las máquinas virtuales con alto riesgo pueden ser separadas de las máquinas virtuales de bajo riesgo. De igual manera la

probabilidad de ubicar o instalar una máquina virtual vulnerable en un servidor físico con un alto nivel de seguridad debe ser minimizado.

4.2. Evaluación de la seguridad de servidores virtuales en IaaS Clouds

La evaluación de seguridad consiste en evaluar los riesgos de los servidores tanto físicos como virtuales en el cloud.

Existe una base de datos de vulnerabilidades pública y periódicamente actualizada por un entidad gubernamental de los Estados Unidos de Norte América [17], esta base de datos se llama "US National Vulnerability Database (NVD)". En esta base de datos las vulnerabilidades son marcadas o clasificadas dependiendo de su Sistema de puntuación de vulnerabilidad común (Common Vulnerability Scoring System (CVSS)) [18].

Basados en estos datos se puede calcular la probabilidad de riesgo de cada servidor virtual explorando las relaciones de dependencia entre las maquinas virtuales en el cloud. De igual manera se puede inferir en una calificación o clasificación de cada servidor físico dependiendo en el nivel de riesgo de seguridad de las máquinas virtuales alojadas en este.

4.2.1. Identificación de vulnerabilidades en servidores virtuales

Como previamente mencionado, este trabajo se basará en el uso de NVD para identificar las vulnerabilidades en las servidores virtuales.

Para comprender de mejor manera el uso de la base de datos NVD en el calculo de riesgos, es necesario entender los conceptos de Sistema de puntuación de vulnerabilidad común CVSS y las Vulnerabilidades y exposiciones comunes Common Vulnerabilities and Exposures (CVE) detalladas en [18].

Los CVSS proveen un framework abierto que estima y cuantifica las vulnerabilidades de software de varios proveedores. Los CVSS son usados por organizaciones gubernamentales como Computer Emergency Response Team s (CERTs) [1], Computer Security Incident Response Team s (CSIRTs) [2] para dar prioridad de respuesta a las vulnerabilidades que se encuentran a diario en sus dominios. Los CVSS son actualizados a diario por el Forum of Incident Response and Security Teams (FIRST) [3].

El CVE es un diccionario que asigna un identificador único a cada vulnerabilidad de seguridad de conocimiento público. Los CVEs son usados como un estándar industrial de nombres de vulnerabilidades; cada vez que una nueva vulnerabilidad es encontrada, se le asigna un identificador de CVE único, (ejemplo CVE-2018-0034522), una breve descripción y las referencias sobre dicha vulnerabilidad.

El NVD es el repositorio que provee la clasificación de los CVSSs para todas las vulnerabilidades de CVE. Estas vulnerabilidades incluyen los últimos ataques

[1] Equipo de Respuesta ante Emergencias Informáticas, término usado en EE.UU

[2] Equipo de Respuesta ante Incidencias de Seguridad Informáticas, término usado en Europa

[3] El padre de todos los CERTs y CSIRTs

en el cloud. La Figura 4.2 muestra un ejemplo de un reporte de vulnerabilidad en maquinas virtuales en el cloud.

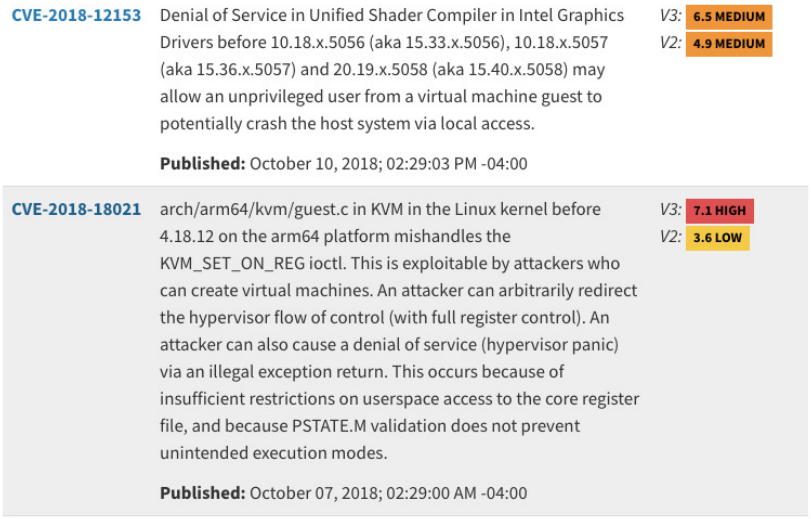

Figura 4.2: Ejemplo de un CVE

El sitio de NVD provee archivos XML on sus respectivas métricas para todos los CVE c encontrados hasta la actualidad desde el año 2002.

Este trabajo usa los datos obtenidos del NVD para identificar las vulnerabilidades encontradas ralacionada a los servidores virtuales en el cloud incluyendo sistemas operativos y servicios instalados ene ste.

Estas métricas de CVSS obtenidas del NVD serán utilizadas para calcular los riesgos en los servidores virtuales, algunos atributos describen cuan severa es la vulnerabilidad. De igual manera información sobre los exploits usados, el proveedor, el nombre del producto, las versiones afectadas por dicha vulnerabilidad entre otras es otorgada por el NVD.

5 Propuesta

En el capitulo 4 se ha tratado el problema de seguridad en Iaas Cloud. Adicionalmente se ha calculado la probabilidad del índice de vulnerabilidad tanto para servidores virtuales como para servidores físicos.

En este capítulo se presenta una propuesta de solución al problema de la seguridad en IaaS cloud. Este capitulo se divide en dos partes: la primera trata sobre un método de asignación de nuevas máquinas virtuales en servidores físicos y la segunda es un manual de políticas a seguir para maximizar la seguridad en los servidores virtuales instalados.

5.1. Evaluación de la seguridad del Servidor Virtual

La clasificación de los CVSS es la métrica principal para poder ponderar el nivel de peligro de la vulnerabilidad. Esta clasificación se encuentra en una escala del 1 al 10 la cual corresponde al nivel de severidad ***nula***, ***bajo***, ***medio***, ***alto***. y ***crítica*** como se muestra en el cuadro 5.1. Los detalles se encuentran en [17].

Cuadro 5.1: Grados de vulnerabilidad otorgados por la NVD

Gravedad	Ponderación
nula	0.0
baja	entre 0.1 y 3.9
media	entre 4.0 y 6.9
alta	entre 7.0 y 8.9
crítica	entre 9.0 y 10.0

1. En este proceso primeramente se verifica la NVD para recolectar eventuales vulnerabilidades tanto del Sistema Operativo como del Software que presta servicios específicos (ej. File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP) en los servidores virtuales.

2. Luego se procede a realizar un escaneo de vulnerabilidades con herramientas como Nessus y Qualys [1].

3. Es muy probable que existan varias vulnerabilidades en un servidor virtual virgen, por lo que hay que asignar una ponderación a cada vulnerabilidad encontrada en cada servidor virtual [19].

[1] herramientas para la detección de vulnerabilidades actuales en sistemas de información

4. Se escoge la vulnerabilidad más critica encontrada (Clasificación basada en el CVSS) de cada servidor virtual. Se asume que el nivel de vulnerabilidad no es más alto que la vulnerabilidad más débil de este servidor virtual.

5. Una vez que se cuantificado el nivel de vulnerabilidad de cada servidor virtual, se procede a mapear la vulnerabilidad cuantificada a la probabilidad de que las otras máquinas virtuales que se encuentran instaladas en el mismo servidor o infraestructura puedan verse comprometidas con dicha vulnerabilidad. En este mapeo se usa información topológica básica como la dirección Internet Protocol (IP) y de red, números de puertos, etc, generadas por herramientas de red como netstat.

Una vez obtenida todas las relaciones de dependencia, se puede construir un grafo de dependencia de maquinas virtuales como se muestra en la Figura 5.1.

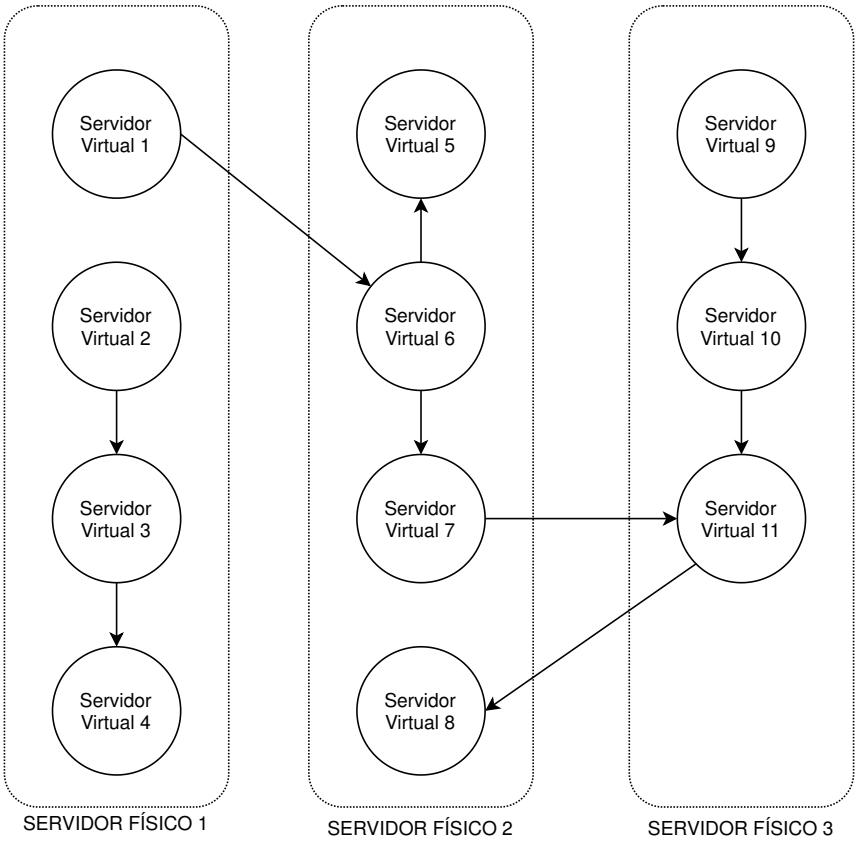

Figura 5.1: Mapeo de servidores virtuales

Para mapear las vulnerabilidades cuantificadas que podrían comprometer o afectar otras máquinas virtuales según las relaciones de dependencia se calcula un índice de vulnerabilidad de todas las MVs instaladas en el servidor físico.

Asumir un servidor virtual (maquina virtual) como MV_a cuyo índice de vulnerabilidad es IV_{MV_a}, el indice de vulnerabilidad de las otras maquinas virtuales conectadas a esta es $\{IV_{MV_1}, IV_{MV_2}, IV_{MV_3}, \ldots, IV_{MV_n}\}$

El índice de vulnerabilidad del servidor físico IV_{SF} es calculado con la Ecuación 5.1.

$$IV_{SF} = \frac{\sum_{i=1}^{n} IV_{MV_i}}{n} \tag{5.1}$$

La ecuación 5.1 da como resultado un índice entre cero y diez. Este índice es muestra el riesgo seguridad del servidor físico tomando en cuenta cada índice de seguridad de que cada máquina virtual que este aloja. El índice de riesgo es el mismo que el descrito en el cuadro 5.1.

Para calcular el índice de compatibilidad IC entre el servidor físico SF y la maquina virtual MV_a a ser ubicada en ese servidor se usa la ecuación 5.2.

$$IC = |(IV_{SF} - IV_{MV_a}) \times 0{,}1| \tag{5.2}$$

Mientras el valor de IC tienda a cero mas compatible es la máquina con el servidor físico, por lo contrario, mientras el valor de IC tiende a 1 la máquina virtual a ser instalada no es compatible con el servidor físico

Ejemplo (caso 1): Según la NVD, la maquina virtual nueva a ser ubicada en un servidor físico posee un índice de vulnerabilidad IV=9. El servidor físico posee 5 máquinas virtuales instaladas (MV_1, MV_2, MV_3, MV_4 y MV_5) con índices de vulnerabilidad IV_{MV_i},de (9, 10, 7, 5 y 8) respectivamente.

Según la ecuación 5.1, el índice de vulnerabilidad del servidor es $IV_{SF} = 7{,}8$.

Aplicando la ecuación 5.2, el índice de compatibilidad entre la máquina virtual y las otras máquinas virtuales instaladas en el servidor físico es $IC = 0{,}12$.

Esto significa que todas las maquinas virtuales del servidor físico poseen un índice de vulnerabilidad muy aproximado al de la maquina virtual a instalarse en el servidor físico.

Ejemplo (caso 2): Según la NVD, la maquina virtual nueva a ser ubicada en un servidor físico posee un índice de vulnerabilidad IV=1. El servidor físico posee 5 máquinas virtuales instaladas (MV_1, MV_2, MV_3, MV_4 y MV_5) con índices de vulnerabilidad IV_{MV_i},de (9, 10, 7, 5 y 8) respectivamente.

Según la ecuación 5.1, el índice de vulnerabilidad del servidor es $IV_{SF} = 7{,}8$.

Aplicando la ecuación 5.2, el índice de compatibilidad entre la máquina virtual y las otras máquinas virtuales instaladas en el servidor físico es $IC = 0{,}68$.

Esto significa que todas las maquinas virtuales del servidor físico poseen un índice de vulnerabilidad muy alejado al de la maquina virtual a instalarse en el servidor físico, lo cual significa que existe un gran riesgo de contagio de vulnerabilidad si comparten servidor físico.

5.2. Método de asignación de nuevas máquinas virtuales en una máquina física

El objetivo de este método es minimizar la probabilidad de vulnerabilidades tanto en un servidor virtual como en el servidor físico que alberga las máquinas virtuales.

En el capitulo anterior se ha estudiado el impacto de la vulnerabilidad y se mencionó que un ataque exitoso depende de la estrategia de ubicación de las maquinas virtuales en el cloud.

Este método propuesto se enfoca en minimizar el riesgo tanto para el servidor virtual como para el servidor físico.

Para una maquina virtual cuya probabilidad de riesgo es baja, no debería ser ubicada en una maquina física cuyo índice de supervivencia es bajo. Esto aumentaría la probabilidad de riesgo de una maquina virtual.

Por otra parte, en el caso de un servidor físico con alta probabilidad de supervivencia, no debería alojar maquinas virtuales con alta probabilidad de riesgo, pues esto causaría un considerable impacto en el nivel de supervivencia de la máquina física.

Por lo tanto, un método inteligente debe minimizar el riesgo y maximizar la supervivencia del servidor físico simultáneamente. Por ejemplo, es lógico y razonable que una máquina virtual con baja probabilidad de riesgo sea instalada en un servidor físico con alta probabilidad de supervivencia.

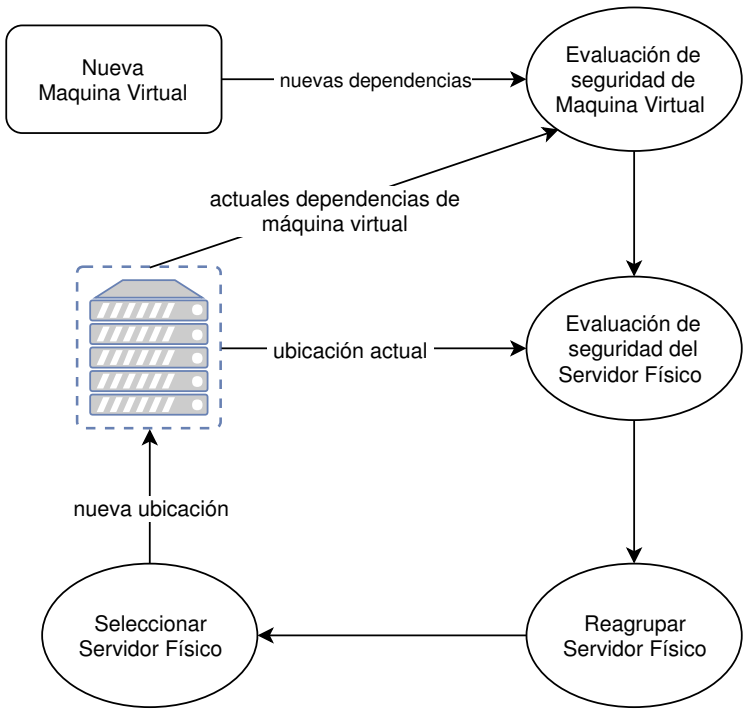

Figura 5.2: Esquema general de ubicación de máquinas virtuales

La Figura 5.2 representa el esquema propuesto para la asignación de maquinas virtuales a servidores físicos. Cuando una nueva máquina virtual necesita ser instalada

se debe actualizar el índice de riesgo de todas las máquinas virtuales instaladas según lo muestra la ecuación 5.1 basado en las relaciones de dependencia introducidas por la nueva máquina virtual.

El siguiente paso es reagrupar las maquinas virtuales en diferentes servidores físicos basadas en su índice de riesgo.

A continuación se describe este proceso en el Algoritmo 1.

Algoritmo 1 Ubicación de servidores virtuales (mv, SF, MV)

1: **Datos de entrada**: mv: nueva maquina virtual a ser ubicada
   SF: Lista de servidores físicos disponibles en el cloud
   MV: Lista de máquinas virtuales presentes en cada servidor físico
2: **repeat** (para cada $sf_i \in SF$)
3: **repeat** (para cada $mv_j \in sf_i$)
4: Calcular IC según ecuación 5.2
5: Agrupar o reagrupar la mv_j en un sf_i dependiendo de su CI
6: **until** no existan más máquinas virtuales
7: **until** no existan más servidores físicos

5.3. Políticas de seguridad para servidores virtuales

El mecanismo presentado previamente, a mi criterio debe ser complementado con un conjunto de buenas prácticas a ser implementadas relacionadas al IaaS. En esta sección se describe las políticas mínimas a seguir, lo cual es la segunda parte de este trabajo.

5.3.1. Seguridad Básica para los Sistemas Virtualizados

El Hipervisor corazón de los sistemas virtualizados tienen los mismos riesgos que el resto de los equipos, su seguridad comienza por asegurar primeramente los componentes físicos del computador que lo alberga. Mientras que los sistemas físicos cuentan con bastantes herramientas informáticas (software) y políticas para su protección lo mismo no ocurre con los entornos virtualizados que no reaccionan adecuadamente frente a los recursos de los sistemas físicos.

En la actualidad se han comenzado a dar pasos importantes en este sentido, Vmware al comenzado a diseñar programas antivirus para su tecnología de virtualización la desventaja que presenta es que no son compatibles para virtualizaciones realizadas con otros programas de virtualización, aunado al hecho de la existencia casi nulas de programas como antimalwares y spybots.

De igual forma las políticas de seguridad para entornos virtualizados que existente en la actualidad son muy vagas, generales y en la mayoría de los casos solos aplicables a tecnologías de virtualización específicas.

Los retos de seguridad a las que deben enfrentar las organizaciones como son los que tienen que ver con la agilidad, el cumplimiento normativo y los retos técnicos de seguridad pueden ser comunes a todos los entornos virtualizados sin importar la tecnología de virtualización, pero no así sus soluciones.

En este sentido Reis, D. (2013), mantiene que frente a la ventaja de la agilidad existen un conjunto de cuestiones que son necesarias tener en cuenta:

1. Haber utilizado el perfil de seguridad aprobado y de acuerdo con las directivas.

2. Constatar que se instalado la versión adecuada de SO y se le han realizado las revisiones correctas, que la maquina anfitriona cuenta con la capacidad y los recursos necesarios.

3. Verificar cómo afecta una nueva MV al rendimiento y a la seguridad de otras MV que se instalan y actualizan las revisiones de seguridad para las MV inactivas y que estas son analizadas con regularidad en busca de vulnerabilidades conocidas, son eliminadas correctamente la infraestructura virtual de las MV retiradas y verificar que el tratamiento que reciben los datos previamente asociados a una MV retirada.

4. Lo anterior debe ser atendido en función de la tecnología de virtualización utilizada para ello es necesario darse a la tarea de conocer, analizar y comprender cuáles son las características de la virtualización seleccionada.

En el Anexo 7.1 se presenta un conjunto de normas a seguir para maximizar la seguridad en sistemas virtualizados.

5.3.2. La Seguridad Básica a Nivel de Cloud Computing

El Cloud Computing ofrece a personas y organizaciones un conjunto de recursos informáticos bien mantenido, de fácil acceso, proporcionando una mayor flexibilidad con los datos y la información, a los que es posible acceder en cualquier momento y desde cualquier lugar que tenga acceso a internet.

Aunque cloudsecurityalliance.org sostiene que los diferentes servicios de cloud son bastantes seguros debidos a los cuantiosos recursos que las empresas que prestan este servicio realizan para mejorar la seguridad de sus servicios, además de contar con los recursos especializados para ello las empresas contratantes deben de poner en prácticas ciertas recomendaciones adjuntas en el Anexo 7.2.

Estas normas fueron recopiladas de varios trabajos sobre el tema [20] [3] y [21].

6 Conclusión

La seguridad relacionada a los servidores virtuales es altamente general, por lo que este estudio se enfoca netamente en la seguridad de IaaS en los servidores virtuales.

Aunque las tecnologías de virtualización han adquirido una velocidad impresionante de adopción, y que al momento de realizar un balance entre los beneficios de la virtualización versus sus retos y los riesgos que se deben asumir cuando se decide optar por la virtualización, virtualizar gana el reto; no significa que aquellas personas u organizaciones que se decidan a implementar Ésta tecnología deban darse por satisfechas por el simple hecho de haber ganado ventajas en su sistema informático.

Toda persona u organización que se decida por la virtualización debe tener bien claro que la tecnología de seguridad tradicional estructurada para los sistemas de hardware no tiene el mismo funcionamiento en los entornos virtuales.

Por otro lado, todo entorno virtualizado a la larga es un sistema híbrido en algún sentido, en toda organización existe una mezcla de los sistemas virtuales y sistemas físicos y los sistemas virtuales dependen de los sistemas físicos para poder existir y poder realizar su función, lo anterior indica que para querer implementar medidas de seguridad de lo sistema virtualizados se debe dar inicio por ofrecerle seguridad en primera instancia al entorno físico para continuar con el del entorno virtualizado, pero este proceso no debe verse como partes separadas por el contrario debe verse como un todo holísticos.

Para evitar la aparición de los agujeros normativos de seguridad, y más cuando estos se relacionan con los entornos virtualizados lo recomendable es que las organizaciones que utilizan estas tecnologías se mantengan informadas y actualizadas sobre las disposiciones que emanan de los organismos especializados en normalizar y estandarizar la gestión de la seguridad a nivel mundial. Organismos como los CERTs o CSIRTs, NVD o el FIRST deben ser usados como una fuente de información actualizada para poder obtener datos reales sobre las nuevas vulnerabilidades encontradas recientemente.

Los métodos de seguridad al instalar una maquina virtual deben tomar en cuenta tanto el servidor virtual como el servidor físico. Por su parte el proveedor debería entregar al cliente, un manual de actualización del Sistema Operativo y servicios alojados en la maquina virtual. Por su parte el cliente debe actualizar su Sistema Operativo de manera periódica.

Trabajos futuros deberían enfocarse en soluciones de isolación de maquinas virtuales para evitar ataques en cadena en el mismo servidor físico.

Bibliografía

[1] Inc John Wiley & Sons. Seguridad para la nube y la virtualización for dummies. *Nueva Jersey*, 2013.

[2] Hernández Sampieri and R y otros. Metodología de la investigación. In *McGRAW-HILL INTERAMERICANA EDITORES S.A.*, 2014.

[3] Galmés Hernández. Sobre la seguridad del almacenamiento en la nube. *Catalunya*, 2016.

[4] J. Cropper, J. Ullrich, P. Frühwirt, and E. Weippl. The role and security of firewalls in iaas cloud computing. In *2015 10th International Conference on Availability, Reliability and Security*, pages 70–79, Aug 2015.

[5] G. B. Singh, F. Jaafar, and S. Butakov. Analysis of overhead caused by security mechanisms in iaas cloud. In *2018 5th International Conference on Control, Decision and Information Technologies (CoDIT)*, pages 952–958, April 2018.

[6] E. Bauer, O. Schluga, S. Maksuti, A. Bicaku, D. Hofbauer, I. Ivkic, M. G. Tauber, and A. Wöhrer. Towards a security baseline for iaas-cloud back-ends in industry 4.0. In *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 427–432, Dec 2017.

[7] M. Alicherry and T.V. Lakshman. Optimizing data access latencies in cloud systems by intelligent virtual machine placement. In *Proceedings of the 32th IEEE Conference on Information Communications (INFOCOM'13)*, pages 647 – 655, April 2013.

[8] P. T. Fung, G. Hamilton, and D. P. Pezaros. Implementing scalable, network-aware vm migration for cloud data centers. In *Proceedings of the 6th IEEE International Conference on Cloud Computing*, pages 557–564, June 2013.

[9] A. Hameed, A. Khoshkbarforoushha, R. Ranjan, P. P. Jayaraman, J. Kolodziej, P. Balaji, S. Zeadally, Q. M. Malluhi, N. Tziritas, A. Vishnu, S. U. Khan, and A. Zomaya. A survey and taxonomy on energy efficient resource allocation techniques for cloud computing systems. In *Computing Journal*, pages 1–24, June 2014.

[10] D. Hatzopoulos, I. Koutsopoulos, G. Koutitas, and W. Van Heddeghem. Dynamic vm allocation in cloud server facility systems with renewable energy sources. In *Proceedings of the IEEE International Conference on Communications*, pages 4217–4221, June 2013.

[11] Z. Afoulki, A. Bousquet, and J. Rouzaud-Cornabas. A security-aware scheduler for virtual machines on iaas clouds. In *Report*, 2012.

[12] M.Li, Y.L.Zhang, K.Bai, W.Y.Zang, M.Yu, and X.B.He. Improving cloud survivability through dependency based virtual machine placement. In *Proceedings of the International Conference on Security and Cryptography*, pages 321–326, July 2013.

[13] E. Caron, A. D. Le, A. Lefray, and C. Toinard. Definition of security metrics for the cloud computing and security-aware virtual machine placement algorithms. In *Proceedings of International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, pages 125–131, October 2013.

[14] S. Al-Haj, E. Al-Shaer, and H. V. Ramasamy. Security-aware resource allocation in clouds. In *Proceedings of IEEE 10th International Conference on Services Computing*, pages 400–407, June 2013.

[15] S. Zhang, X. Zhang, and X. Ou. After we knew it: empirical study and modeling of cost-effectiveness of exploiting prevalent known vulnerabilities across iaas cloud. In *Proceedings of the 9th ACM symposium on Information, Computer and Communications Security*, pages 317–328, June 2014.

[16] S. Bugiel, S. Nurnberge, T. Poppelmann, A. Sadeghi, and T. Schneider. Amazonia: when elasticity snaps back. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, pages 389–400, October 2011.

[17] NVD. US National Vulnerability Database. In *https://nvd.nist.gov*.

[18] FIRST. Common vulnerability scoring system. In *http://www.first.org/cvss*.

[19] M. Ekstedt H. Holm and D. Andersson. Empirical analysis of system-level vulnerability metrics through actual attacks. *IEEE Transactions on Dependable and Secure Computing*, 9(6):825–837, August 2012.

[20] González Hernández. Aspectos de seguridad informática en la utilización de cloud computing. universidad nacional abierta y a distancia (unad). 2016.

[21] Chahin Noreña and Juan Antonio. Metodologia acrd para la gestión de seguridad en entornos virtuales. In *Universidad Nacional de la Rioja*, Septiembre 2015.

7 Anexos

7.1. Anexo 1: Normas de seguridad de los entornos virtualizados

1. Debe existir una política de autentificación robusta de usuario para restringir el acceso al (los) huésped(es), solamente a aquellos usuarios autorizados.

2. Se debe implementar la Seguridad del Server HOST o del Storage a través de la aplicación de permisos de acceso a las máquinas virtuales.

3. Se debe implementar una normativa de encriptación de datos para evitar que la información que se encuentra en la máquina virtual o que fluye por medio de la red pública puedan ser leídos por personas no autorizadas.

4. Las llaves de llaves de encriptación para el cliente y el servidor se deben generar y renovar de forma periódica según patrones establecidos.

5. Se deben mantener actualizados los soportes para los protocolos más comunes o usuales utilizados en las redes públicas.

6. Para asegurar que la interconexión entre redes virtuales se debe implementar Protocolo de Túneles (PPTP, LTTP, IPSEC); encapsulación y encriptación de las tramas emulando un enlace punto a punto privado seguro sobre la infraestructura pública usada; de las conexiones VPN, con la finalidad de cumplir las necesidades de seguridad de los datos transmitidos. Se pueden combinar los protocolos LTTP, IPSEC.

7. Se deben siempre herramientas de seguridad que hayan sido diseñadas para trabajar con los aspectos dinámicos del entorno virtual y puedan detectar los problemas automáticamente y proteger las maquinas virtuales.

8. Deshabilite las Funciones Innecesarias o Superfluas

9. Se deben utilizarse los mecanismos de seguridad específicos de las máquinas virtuales que se encuentran incorporados en las APIs del hipervisor para proporcionar una monitorización granular del tráfico que pasa por las backplanes de estas máquinas.

10. Los sistemas operativos virtualizados deben incluir firewall (entrante/saliente), sistema de prevención de intrusiones en host (HIPS), sistema de prevención de intrusiones en red (NIPS), protección de aplicaciones web, antivirus, monitorización de integridad de archivos, monitorización de logs, etc.

11. Se deben diseñar una política de eliminación de las copias de seguridad y sistema de respaldo cuando elimine y borre las imágenes de la máquina virtual.

12. Se deben diseñar una política para el continuo mantenimiento y actualización de las imágenes de máquinas virtuales en reposo y de protección de las nuevas VM hasta que sean parchear.

13. Las máquinas virtuales no utilizadas deben ser cifradas mientras no estén en uso.

14. Se debe definir claramente los roles y acceso de los usuarios del sistema.

15. Se debe separar físicamente, al menos, las redes de almacenamiento, gestión y máquinas virtuales.

16. Se debe utilizar los programas Monitores de máquinas virtuales (VMMs) que tengan acceso a todos los estados de una VM, incluyendo el estado del CPU, de la memoria y de los dispositivos y con capacidades de inspección que propicien checkpoints, rollbacks y replays.

17. Se debe aplicar una política de aislamiento de máquinas virtuales, por medio de la instalación las VM en particiones o volúmenes diferentes que cuente con un mecanismo de reporte que ofrezca pruebas del aislamiento y active alertas si hay una violación del aislamiento.

18. Las VM's deben tener asignados recursos fijos para su funcionamiento.

19. Implementar mecanismos para lograr un control de detección del tráfico por medio de la generación de reportes tales como: los horarios de accesos al entorno virtual, el registro de tráfico entre maquina virtuales, el flujo de datos valorizado entre VM, cuales son las maquinas conectadas y los accesos externos, reporte de host activos y tiempo de actividad, análisis de protocolos y rendimiento de comunicación y de alertas por detección de tráfico malicioso y accesos no permitidos.

20. Establecer controles de seguridad en cada capa dentro de la arquitectura virtual, incluidos los controles de la red de la organización. Las capas virtuales primarias que proteger son la del hipervisor, los sistemas operativos hospedados, la red virtual entre máquinas virtuales, la red física, el sistema de gestión de la virtualización y el almacenamiento físico de las imágenes virtuales.

21. Utilizar la consola de gestión de Trend Micro a fin de supervisar y notificar de cambios importantes en los sistemas críticos.

22. Utilizar los switches virtuales para asegurar la red virtual contra ataques potenciales del tipo man-in-the-middle.

23. Implementar un aparato virtual con acceso a comunicación con sitios externos que le permitan descargar información actualizada sobre amenazas para que desempeñe todas las funciones de una solución de seguridad como si fuera una sola máquina virtual que se encargara de supervisar a todas las máquinas virtuales por medio hipervisor.

24. Maximizar el aislamiento de las instancias que se ejecutan en la misma máquina.

7.2. Anexo 2: Normas de seguridad a nivel de Cloud Computing

1. Se debe firmar un contrato de servicio que como mínimo contemple que el proveedor de servicios firme un acuerdo de confidencialidad y no divulgación de datos a los que pudiera tener acceso durante la provisión del servicio. DE igual forma se deben contemplar en el mismo: Retención de datos, Service Level Agreement, Responsabilidades, Jurisdicción, Privacidad, Leyes sobre Seguridad, Pedidos de información y Cumplimiento de regulaciones y auditorias

2. Se debe constatar que el proveedor cuente con políticas muy estrictas para la destrucción de información que pudiera encontrarse en hardware que se retira de servicio activo.

3. Implementar el uso de servidor proxy inverso (reverse proxy), que proporcione un punto de acceso único a la red interna y el mismo debe estar habilitado como componente de autenticación y de control de acceso a las aplicaciones WEB.

4. Hacer uso de certificados digitales emitidos por autoridades de confianza, que permitan a las aplicaciones cliente verificar que realmente está conectado con el proveedor de servicio correcto

5. Utilizar el Protocolo ligero de acceso a directorios (LDAP, Lightweight Directory Access Protocol), los más usados son; Oracle directory server, IBM Tivoli Directory Server y OpenLDAP.

6. Utilizar un dispositivo de seguridad IPS (Intrusion Prevention System) para prevenir posibles intrusiones a partir de la identificación y bloqueo de patrones específicos de ataque en su flujo por la red, más utilizados: Snort, CISCO Firepower, Checkpoint y Suricata.

7. Implementar mecanismos de Intrusion Detection System (IDS) integrados al cortafuego que funcionen en tiempo real para detectar actividades inapropiadas, incorrectas o anómalas en la red de una organización

8. El uso de Secure Sockets Layer (SSL) y Transport Layer Security (TLS) para el cifrado de la información.

9. Utilizar herramientas de escaneo de vulnerabilidades, los más usadas son; Nessus, Nmap, OpenVAS.

10. Solicitarle al proveedor que nuestras máquinas virtuales sean ubicadas en una zona desmilitarizada (DMZ), y si es necesario requerir equipos de red independientes como Switches dedicados por los cuales sólo fluya el trafico destinados solamente a las máquinas virtuales de la organización.

11. Solicitar al prestador de servicios que utilice VLAN Tagging o Truking para las máquinas virtuales a fin de asegurar que todos los paquetes que entran o salen de las máquinas virtuales de la organización tengan un ID de VLAN que sólo las interfaces de red en la misma VLAN reciban y procesen esos paquetes.

12. Es recomendable, Si se puede, alquilar el servidor físico completo para el uso exclusivo de las máquinas virtuales de la organización evitando tener que compartirlo con otros inquilinos.

13. Programar la realización de copias de seguridad a un tiempo definido.

14. Elija almacenamiento con dispersión de los datos cuando esté disponible.

15. Utilice el ciclo de vida de seguridad de los datos para identificar riesgos de seguridad y determinar los controles más adecuados.

16. Monitorice las bases de datos clave internas y los repositorios de archivos con DAM y FAM para identificar grandes migraciones de datos, que podrían indicar que se están migrando datos al Cloud.

17. Monitorice el acceso de los empleados a Internet con filtrado de URL y/o herramientas DLP para identificar datos delicados que se estén migrando al Cloud.